Request for Proposal
for
Selection of Master System Integrator (MSI) for Technology Implementation, Operationalization and Maintenance of State-wide NexGen UP112 Project

Tender No. **ITECCS** Date: 16-07-2022

UP POLICE

GOVERNMENT OF UTTAR PRADESH

1 INTRODUCTION

1.1 Project background

The Uttar Pradesh Police Emergency Response Support System (UP112) has been established to provide prompt integrated emergency response for public safety and security to all citizens, at any time, across the entire state. The system has been designed to optimize and function to serve citizens within average response times of 15 minutes in urban and 20 minutes in rural areas. To serve to the needs of more than 22 crore citizens, the project boasts an infrastructure consisting of a high-tech centralized contact and dispatch centre at Lucknow, with dedicated lease lines to connect Data Centre and Command Centre at Lucknow, OMC Centres at Prayagraj and Ghaziabad, 126 District Control Rooms, 18 Zones, 8 ranges, 4 Commissionerate's, Fire Service and GRP.

Over 32,000 trained and sensitized police personnel are deployed and dispersed throughout the state to serve citizens.

The UP112 headquarters (centralized contact centre) is a state-of-the-art facility with 600 outsourced professional lady officers (civilians), centralized dispatch officers, served by 300 police officers.

At the ground level, 4800 modern Police Response Vehicles (PRVs), fitted with GPS-enabled Mobile Data Terminals, Radio-Over-Internet-Protocol (RoIP) wireless sets, mobile phones, dashboard cameras and first aid kits are deployed for 24*7 and 365 days to serve the citizens of UP state.

1.2 NexGen UP112

Vision of NexGen UP112

"To provide ***prompt integrated emergency response for public safety and security to all persons anytime, anywhere*** in Uttar Pradesh"

Aim of NexGen UP112

NexGen UP112 aims to enhance the services provided to citizens of UP in terms of

a) Smooth call landing at 112 system, by dealing with all present challenges of call connectivity
b) Improve overall response time
c) Increase in the role of UP112, by integrating with other government agencies for the coordinated response to citizens of Uttar Pradesh.

It is proposed that in NexGen UP112, ITECCS would be able to handle more calls landing through multiple channels such as PSTN, mobile, SMS, emails, social media channels, web portal, and mobile app and provide better services using updated solutions and technologies.

In NexGen UP112, we expect the system to receive 1 lakh 50 thousand calls per day (on the higher side). The increase in calls count is expected due to changes in the call landing protocol of the system, increasing awareness, approachability/ reachability of the UP112 system by

citizens, population growth, and integration with other government agencies. Accordingly, the manpower has been estimated for a large call volume to be addressed with the aim of **no call unanswered at ITECCS**.

For calls dropped due to any reason, a call back would be made to ensure that services are provided timely to the citizens. This is to ensure that the citizens perceive ITECCS not as a Call Centre, but as a Contact Centre with skilled and trained manpower dedicated to providing them a prompt, efficient and coordinated response.

2 INSTRUCTIONS TO THE BIDDERS

2.1 Instructions for online bid submission

2.1.1 Instructions to the Bidders to submit the bids online through the GeM Portal

2.1.2 Enrolment/registration of the Bidders on the GeM Portal is a prerequisite for e-tendering.

2.1.3 Bidders need to log in to the GeM Portal through their user ID/ password chosen during enrolment/ registration.

2.1.4 Bidder may go through the tenders published on the GeM Portal and download the required tender documents/ Annexures for the tenders they are interested in.

2.1.5 After downloading/ getting the tender document/ Annexures/ Appendices, the Bidder should go through them carefully and then submit them as asked; otherwise, the bid will be rejected.

2.1.6 If there are any clarifications, this may be obtained online through the tender site or the contact details. Bidder should take into account the corrigendum/ Addendum published before submitting the bids on GeM Portal.

2.1.7 It is construed that the bidder has read all the terms and conditions before submitting their offer. Bidder should go through the tender Annexures and appendices carefully and upload the documents as called for; otherwise, the bid will be rejected.

2.1.8 Bidder, in advance, should get ready the bid documents to be submitted as indicated in the tender document/ Annexure, and generally, they can be in PDF/Xls/rar/zip/dwf formats. In addition, the bidder should consider the corrigendum/ Addendum published from time to time before submitting the online bids.

2.1.9 Bidder should submit the Tender Fee/ EMD as specified in the tender. The original should be posted/ couriered/ given in person to the Tender Inviting Authority.

2.1.10 If the price bid format is provided in a RFP document, the rates offered should be entered in the allotted space only and uploaded after filling the relevant columns. The Price Bid template must not be modified/ replaced by the bidder; otherwise, the bid submitted will be rejected for this tender.

2.1.11 Buyer shall not have any liability to bidders for any interruption or delay in access to the GeM site / Reverse Auction link etc., irrespective of the cause and all queries related to such impediments should be raised to GeM technical team

2.1.12 For any queries regarding the e-tendering process, the bidders are requested to contact GeM.

2.2 General instruction to bidders

2.2.1 The Bidder must carefully read all the terms, conditions, and specifications before filling up the tender proposal and financial bid. The Bidder shall be bound by all terms, conditions, and specifications detailed in this tender document. The Bidders who are confident of executing the contract in time by employing the required resources, manpower, and materials need only participate in this tender.

2.2.2 Regarding the matters pertaining to this contract, Bidder shall not directly or indirectly bring or attempt to bring any political or outside influences or intervention through any association, union, or organization. All disputes, differences, clarifications, etc., arising out of this contract will be represented by Bidder himself or by his legal representative.

2.2.3 It may be noted that the tender notice is only for fixing a contract and shall not be construed as an invitation to bid for providing the job, i.e., there is no guarantee for the award of work without assigning any reason whatsoever may be.

2.2.4 It is implied that the Bidder has obtained all necessary information directly or indirectly affecting the contract, such as a legal stipulation, possible delays, and hindrance or interference in executing the contract, and has satisfied them before making the offer. Unexpected difficulties or expenses shall NOT be considered excuses for difficulties in performing the contract. The rate quoted should consider all factors.

2.2.5 The Bidder acknowledges that he assumes all risks contingent upon the nature of the contract to be encountered by him in executing the contract, even though such actual conditions may result in the Bidder performing more or less work than that originally anticipated.

2.2.6 The tender shall contain the name, address of residence, and place of Bidder's business and shall be signed by the Bidder's authorised signatory. Consortium Partner firms shall furnish full names and addresses. In case of the authorized representative signs, "Power of Attorney" duly attested by a public notary must be submitted. In the case of the Consortium partnership, a Self-Attested true copy of the Consortium agreement must be submitted along with the bid. Similarly, the Self Attested copy of the Memorandum of Article & Association must be submitted along with the tender in the company's case.

2.2.7 Interest shall NOT be payable on the Earnest Money deposit

2.3 Cost to bid

2.3.1 The Bidder shall bear all costs associated with submitting its bid, including the cost of purposes of clarification of the bid if so desired by the Buyer. The Buyer shall in no case be responsible for those costs, regardless of the conduct or outcome of the Tendering process

2.4 Clarification on RFP

2.4.1 When deemed necessary, during the tendering process, ITECCS may seek clarifications on any aspect from any or all the Bidders. However, that would not entitle the Bidder to change or cause any change in the substance of the bid submitted or price quoted.

2.5 Pre-bid Meeting & Clarifications

2.5.1 A Bidder requiring any clarification on the RFP Document may submit the queries, in writing, at the Buyer's email ID as per schedule indicated in 'Bid details of GEM' of this RFP. The queries must be submitted in the following format in editable form (Excel format):

Bidder's request for clarification		
Name and Address of the Organization submitting request	Name and Designation of Person submitting request	Contact Detail of the Organization or Authorized Representative
		Tel:
		Fax:

				Email:
S.No	RFP Reference Section	RFP Reference Page	Content of RFP requiring clarification	Points of clarification required
1.				
2.				

2.5.2 Only authorized representatives (maximum two persons) of the Bidder(s) are invited to attend the Pre-bid meeting at their own cost which would take place at the venue mentioned in the Bid details of GEM.

2.5.3 The purpose of the pre-bid meeting is to provide basic information and to clarify any concerns, Bidder may have, related to this tender.

2.5.4 Bidder are encouraged to participate in the pre-bid meeting. However, not attending the pre-bid meeting will not be a cause for disqualification.

2.5.5 Buyer shall not be responsible for ensuring that the Bidder's queries have been received by them. Any request for clarifications, post the indicated date and time stipulated in Bid details of GEM, may not be entertained by the Buyer.

2.6 Responses to Pre-Bid Queries and Issue of Corrigendum

2.6.1 At any time prior to the deadline for submission of Bids, the Buyer may, for any reason, whether at its own initiative or in response to a clarification requested by the Bidder, amend the Bid document by issuing an addendum/corrigendum.

2.6.2 In order to provide Bidder reasonable time to take the amendment into account in preparing their bids, the Buyer may, at its discretion, extend the last date for the receipt of Bids.

2.6.3 The corrigendum (if any) and clarifications to the queries from all Bidder will be posted on GeM Portal and emailed to all participants of the pre-bid meeting at the email ID provided by the Bidder in pre-bid format.

2.7 Amendment of RFP

2.7.1 At any time prior to the last date for receipt of bids, the Buyer may, for any reason, whether at its initiative or in response to a clarification requested by a prospective Bidder, modify the RFP by an amendment. The amendment shall be notified on the GeM portal and should be considered by the prospective agencies while preparing their bids.

2.7.2 To provide prospective Bidders reasonable time in which to take the amendment into account in preparing their bids, the Buyer may, at its discretion, extend the last date for the receipt of Bids

2.7.3 Buyer may at any time during the tendering process request the Bidder to submit revised Technical/ Commercial Bids and/ or Supplementary commercial bids without thereby incurring any liability to the affected Bidder or Bidders

2.8 Language of bids

2.8.1 The Bids prepared by the Bidder and all correspondence and documents relating to the bids exchanged by the Bidder and the Buyer shall be written in the English language, however, provided that any printed literature furnished by the Bidder may be written in another language so long the same is accompanied by its English

translation in which case, for purposes of interpretation of the bid, the English translation shall govern. As the bid is being initiated by an organization working under government of Uttar Pradesh therefore Hindi and Urdu language will be encouraged but for comparison English translation of the bid must be available as per provided format through GeM.

2.9 Procedure for submission of bids

2.9.1 The bid prepared by the Bidder shall be submitted online on GeM Portal only.

Note: Prices should not be indicated/ mentioned in Technical Bid but should only be mentioned in the Commercial Bid.

2.9.2 The Bidder shall submit only one (1) bid in response to the RFP. If the Bidder submits more than one bid, it shall be subject to disqualification of the bidder and shall also cause the rejection of all the bids which such Bidder has submitted

2.10 Bid prices

2.10.1 The Bidder shall indicate in the proforma prescribed at Section 7 of this RFP, the unit rates of the services/components it proposes to provide under the Contract. Prices should be shown separately for each item as detailed in Section 7 of the RFP.

2.10.2 In the absence of information as requested above, a bid shall be considered incomplete and summarily rejected.

2.10.3 The Bidder shall prepare the bid based on details provided in the RFP documents. The Bidder shall carry out all the tasks in accordance with the requirement of the RFP documents and it shall be the responsibility of the Bidder to fully meet all the requirements of the RFP documents.

2.10.4 The Bidder as part of its Financial Bid should account for all out of pocket, taxes, levies, and other expenses that the Bidder shall incur during the contract period.

2.11 Firm prices

2.11.1 Prices quoted must be firm and final and shall remain constant throughout the period of the contract and shall not be subject to any upward modifications, on any account whatsoever. The Bidder shall, therefore, indicate the prices in Section 7 of this RFP. The Bid Prices shall be indicated in Indian Rupees (INR) only.

2.11.2 The Financial Bid should clearly indicate the price to be charged without any qualifications whatsoever and should include all taxes, duties, fees, levies, works contract tax and other charges as may be applicable in relation to the activities proposed to be carried out.

2.11.3 A financial bid submitted with an adjustable price quotation or conditional bid shall be treated as non-responsive and the bid shall be rejected summarily.

2.12 Discount

2.12.1 The Bidder is advised not to indicate any separate discount. Discount, if any, should be merged with the quoted prices. Discount of any type, indicated separately, will not be taken into account for evaluation purpose.

2.13 Bidder qualification

2.13.1 The “Bidder” or "Prime Bidder" in case of Consortium as used in the RFP documents shall mean the Organisation on whose behalf the RFP response has been

submitted. The Bidder may be either the Principal Officer (MD or Company Secretary) or his or her duly Authorized Representative, in which case he or she shall submit a power of attorney as mentioned in Annexure 18 and 19 of Section 9 of this RFP. All certificates and documents (including any clarifications sought and any subsequent correspondences) received hereby, shall be furnished, and signed by the representative or the principal.

2.13.2 It is further clarified that the individual signing the RFP or other documents in connection with the RFP must certify whether he or she signs as:
Constituted attorney of the firm if it is a company

OR

The Principal officer or his or her duly Authorized Representative of the Bidder or Prime Bidder in case of the Consortium, in which case he or she shall submit a certificate of authority on behalf of the Prime Bidder of the consortium

2.13.3 The authorization shall be indicated by power-of-attorney accompanying the bid as per Annexure 18 and 19 of Section 9 of this RFP.

2.14 Earnest Money Deposit (EMD)

2.14.1 As part of this bid, the Bidder shall furnish an Earnest Money Deposit (EMD) of the amount mentioned in the Bid details of GEM of this RFP through Bank Guarantee.

2.14.2 Bidder shall upload a scanned copy of the same in the online bid, and a hard copy of the same will have to be submitted directly to the Buyer before the last date of bid submission.

2.14.3 Bidders can also submit the EMD with Account Payee Demand Draft issued by any Scheduled Commercial Bank/ Nationalized Bank drawn in favour of ADG UP112 payable at LUCKNOW.

2.14.4 Bidder has to upload scanned copy / proof of the DD along with bid and has to ensure delivery of hardcopy to the Buyer before the last date of bid submission

2.14.5 The EMD should be valid for 45 days beyond the bid validity

2.14.6 The EMD is required to protect the Buyer against the risk of Bidder's conduct which would warrant the security's forfeiture pursuant to Scope of Work

2.14.7 Unsuccessful Bidder's EMD shall be discharged/ returned within 30 days after the award of contract to the successful Bidder or expiry of bid validity, whichever is earlier. Earnest money of successful bidder shall be returned within 30 days after receipt of Performance Security / e-PBG.

2.14.8 The Buyer shall pay no interest on the EMD

2.14.9 The EMD may be forfeited:

a. if the bidder withdraws or modifies or derogates its bid during the period of bid validity specified by the Bidder in the Bid.
b. If it comes to notice that the information/documents furnished in its bid are false, misleading, or forged; or
c. In the case of a successful Bidder, if the Bidder fails.
   i. To sign the Contract in accordance with Clause 2.29: Award of Contract; or
   ii. To furnish Bank Guarantee for contract performance in accordance with clause 2.15 Performance Bank Guarantee

2.15 Performance Bank Guarantee

2.15.1 Performance Bank Guarantee has to be made in the form of Refundable & Irrevocable Bank Guarantee from any Scheduled Commercial Bank/ Nationalized Bank drawn in favour of the Beneficiary payable at Lucknow before signing of the Contract

2.15.2 The bidder has to deposit 06 (six) Bank Guarantees as per below manner:

a. First Bank Guarantee of the amount equivalent to 3% of the Contract value of the contract would be submitted to the Buyer within 15 (fifteen) days from the date of notification of award of contract on GeM. The same would be returned by the Buyer after acceptance of the system as defined in Clause 4.18 of this RFP.

b. Second Bank Guarantee of the amount equivalent to 3% of the Opex value of the contract would be submitted to the Buyer within 15 (fifteen) days from the date of starting of O&M phase. The same would be returned by the Buyer within 15 days after completion of 1st year of O&M phase and completion of all contractual obligations of this phase.

c. Third Bank Guarantee of the amount equivalent to 3% of the Opex value of the contract would be submitted to the Buyer within 15 (fifteen) days from the date of starting of 2nd year of O&M phase. The same would be returned by the Buyer within 15 days after completion of 2nd year of O&M phase and completion of all contractual obligations of this phase.

d. Fourth Bank Guarantee of the amount equivalent to 3% of the Opex value of the contract would be submitted to the Buyer within 15 (fifteen) days from the date of starting of 3rd year of O&M phase. The same would be returned by the Buyer within 15 days after completion of 3rd year of O&M phase and completion of all contractual obligations of this phase.

e. Fifth Bank Guarantee of the amount equivalent to 3% of the Opex value of the contract would be submitted to the Buyer within 15 (fifteen) days from the date of starting of 4th year of O&M phase. The same would be returned by the Buyer within 15 days after completion of 4th year of O&M phase and completion of all contractual obligations of this phase.

f. Sixth Bank Guarantee of the amount equivalent to 3% of the Opex value of the contract would be submitted to the Buyer within 15 (fifteen) days from the date of starting of 5th year of O&M phase. The same would be returned by the Buyer within 15 days after completion of 5th year of O&M phase and completion of all contractual obligations of this phase.

2.15.3 In the event of termination, Buyer may Invoke the Performance Bank Guarantee, recover such other direct costs and other amounts towards direct damages from the Agency that may have resulted from such default and pursue such other rights and/ or remedies that may be available to the Buyer under law.

2.15.4 The payments to the Bidder shall become due only after receipt of Performance Bank Guarantee by the Buyer and verification of its genuineness.

2.15.5 If the Bidder fails or neglects to observe or perform any of his obligations under the contract, it shall be lawful for the Buyer to forfeit either in whole or in part, the Performance Security furnished by the Bidder.

2.15.6 If the Bidder duly performs and completes the contract in all respects, the Buyer

shall refund the Performance Security to the Bidder within 30 days of completing all contractual obligations by the Bidder.

2.15.7 Failure of the successful Bidder to comply with the requirement of the above Clause shall constitute sufficient grounds for the annulment of the award and forfeiture of the EMD

2.15.8 Bidders can also submit the same in favour of ADG UP112 Lucknow payable at LUCKNOW.

2.16 Period of validity of Bids

2.16.1 Bids shall remain valid for a period of 180 days from the bid end date. A bid valid for a shorter period may be rejected by the Buyer as non-responsive.

2.16.2 In exceptional circumstances, the Buyer may request the Bidder(s) to extend the period of validity. The request and the responses thereto shall be made in writing (or through e-mail). The validity of EMD provided under the above Clause may also be extended if required.

2.17 Format and signing of bid

2.17.1 The documents of the bid submitted online shall be clear and readable. The documents shall be signed by the Bidder or a person or persons duly authorized to bind the Bidder to the Contract. All pages of the bid, except for unamended printed literature, shall be initialled and stamped by the person(s) signing the bid.

2.17.2 The response to the bid should be submitted along with legible, appropriately indexed, duly filled Information sheets and sufficient documentary evidence. Responses with illegible, incomplete Information sheets or insufficient documentary evidence shall be rejected.

2.17.3 The bid shall contain no interlineations, erasures, or overwriting except as necessary to correct errors made by the Bidder, in which case such corrections shall be initialled by the person(s) signing the bid

2.18 Code of integrity

2.18.1 No official of a procuring entity or a Bidder shall act in contravention of the codes which includes:

a. Prohibition of

i. Making offer, solicitation or acceptance of bribe, reward or gift or any material benefit, either directly or indirectly, in exchange for an unfair advantage in the procurement process or to otherwise influence the procurement process.

ii. Any omission, or misrepresentation that may mislead or attempt to mislead so that financial or other benefit may be obtained, or an obligation avoided.

iii. Any collusion bid rigging or anticompetitive behaviour that may impair the transparency, fairness, and the progress of the procurement process.

iv. Improper use of information provided by the procuring entity to the Bidder with an intent to gain unfair advantage in the procurement process or for personal gain.

v. Any financial or business transactions between the Bidder and any official of the procuring entity related to tender or execution process of Contract, which can affect the decision of the procuring entity directly or indirectly.

vi. Any coercion or any threat to impair or harm, directly or indirectly, any party or

its property to influence the procurement process.

vii. Obstruction of any investigation or auditing of a procurement process.

viii. making false declaration or providing false information for participation in a bid process or to secure a Contract.

b. Disclosure of conflict of interest

In case of any reported violations, the procuring entity, after giving a reasonable opportunity of being heard, comes to the conclusion that a Bidder, as the case may be, has contravened the code of integrity, may take appropriate measures.

2.18.2 **Integrity Pact**

The pact essentially envisages an agreement between the Bidder and the Buyer, committing the persons/ officials of both sides, not to resort to any corrupt practices in an aspect/ stage of the Contract. Bidder are required to sign an Integrity pact as provided in Annexure 22 in original and should be submitted along with bid.

2.19 Revelation of prices

2.19.1 Prices in any form or by any reason before opening the Commercial Bid should not be revealed, failing which the offer shall be liable to be rejected

2.20 Terms and conditions of bidders

2.20.1 Any terms and conditions of the Bidders shall not be considered as forming part of their Bids

2.21 Consortium

2.21.1.1 The Bidder may be a single entity or a group of at maximum of 3 (three) entities(the "**Consortium**"), coming together to implement the Project. However, no Bidder applying individually or as a member of a Consortium, as the case may be, can be member of another Bidder for the Project. In the event of such an occurrence (i.e., if the Bidder is part of Consortium of more than 1 bid), all such bids, shall be summarily rejected. The term 'Bidder'used herein would apply to both a single entity and a Consortium.

2.21.1.2 In case the Bidder is a Consortium, it shall comply with the following requirements:

a. The maximum number of members that shall be allowed to form a Consortium for the purpose of this RFP must not exceed 3 (three). In the event of such an occurrence (i.e., if the consortium members are more than 3), the bid, shall be summarily rejected.

b. The Proposal should include a description of the roles and responsibilities of individual Members of the Consortium, particularly with reference to technical, financial, operational and maintenance obligations. The Proposal should contain the required information for each Member of the Consortium.

c. The lead bidder and the consortium partners should fulfil eligibility criterion as applicable as defined in Section 3 of the RFP and one of them would be considered as Lead bidder as decided by them through a Joint Bidding Agreement, to whom the Project would be given for execution and the Lead Bidder would be responsible for execution of the complete project and comply with all terms & conditions of RFP. The nomination(s) shall be supported by a power of attorney, substantially in the form specified at Annexure 18 and 19 of Section 9 of the RFP, executed on non-

judicial stamp paper of appropriate value and duly notarized by a notary public, signed by Member of the Consortium.

d. The Consortium member, other than the Lead Member of the Consortium should hold at least 10% (Ten percent) of the share in the Consortium for the entire duration of the Project. This would ensure that member with small equity holdings are not included with the sole purpose of achieving pre-qualification. In other words, only the experience and net worth of consortium member who shall have a substantial stake in implementation of the project is to be counted.

e. The Member of the Consortium shall enter into a binding joint bidding agreement, substantially in the form specified at Annexure 17 of section 9 of the RFP (the "Joint Bidding Agreement"), for the purpose of submitting a Proposal. The Joint Bidding Agreement, to be submitted along with the Proposal, shall, inter alia:

   i. convey the details of shareholding/ ownership equity commitment(s) of the Member of the Consortium, which would enter into the Contract with ITECCS and subsequently perform all the obligations of the Selected Bidder in terms of the Contract, in case the Project is awarded to the Consortium in accordance with this RFP; and,

   ii. clearly outline the proposed roles and responsibilities, if any, of each Member; and,

   iii. commit the minimum equity stake to be held by each Member; and

   iv. undertake that the Consortium member, other than the Lead Member of the Consortium; whose technical and/or financial capacity is considered for the purpose of qualification and shortlisting herein; should hold at least 10% (10 percent) of the paid up and subscribed equity in the Consortium for the entire duration of the Project; and

   v. include a statement to the effect that all Members of the Consortium shall be liable jointly and severally for all obligations in relation to the Project for the entire Contract Period or such extended term as may be mutually agreed; and

   vi. except as provided under this RFP and the Bidding Documents, there shall not be any amendment to the Joint Bidding Agreement without the prior written consent of UP Police.

2.22 Last date for receipt of bids

2.22.1 Bids shall be submitted by the Bidder no later than the time and date specified in GeM Portal

2.22.2 Bids shall be submitted online in GeM Portal

2.22.3 The Buyer may, at its discretion, extend the last date for the receipt of bids by amending the RFP, in which case all rights and obligations of the Buyer and Bidders previously subject to the last date shall thereafter be subject to the last date as extended

2.23 Modification and withdrawal of bids

2.23.1 No bid may be altered/ modified subsequent to the closing time and date for receipt of bids. Unsolicited correspondences from Bidders shall not be considered

2.23.2 No bid may be withdrawn in the interval between the last date for receipt of bids and the expiry of the bid validity period specified by the Bidder in the Bid. Withdrawal of a bid during this interval may result in the Bidder's forfeiture of its EMD and be

declared a “defaulting bidder.” In such a situation, the tendering process shall be continued with the remaining bidders as per their ranking.

2.23.3 If the bidder relents after being declared a selected bidder, it shall be reported as defaulting bidder, and EMD of such defaulting bidder shall be forfeited, and the Buyer reserves the right to blacklist/ debarred bidder for the next 03 years from participating in any such tender. In such a situation, the tendering process shall be continued with the 2nd rank bidder based on evaluation of the bid as defined in section 3.

2.24 Contacting the Buyer

2.24.1 No Bidder shall contact the Buyer on any matter relating to its bid, from the time of the bid opening to the time the contract is awarded

2.24.2 Any effort by a Bidder to influence the Buyer’s bid evaluation, bid comparison, or contract award decisions may result in the rejection of the Bidder’s bid

2.25 Evaluation of bid

2.25.1 Evaluation of the received bids will be carried out as per Section 3.

2.26 Buyer's right to vary scope of contract

2.26.1 The Buyer may at any time, by a written order given to the Bidder, make changes to the scope of the Contract as specified with effect of +-10

2.26.2 If any such change causes an increase or decrease in the cost of, or the time required for the Bidder’s performance of any part of the work under the Contract, whether changed or not changed by the order, an equitable adjustment shall be made in the Contract Value or schedule, or both, as decided by the committee and the Contract shall accordingly be amended. Any claims by the Bidder for adjustment under this Clause must be asserted within thirty (30) days from the date of the Bidder’s receipt of the Buyer’s changed order.

2.27 Buyer's right to accept any bid and to reject any or all bids

2.27.1 The Buyer reserves the right to accept any or all bid and to annul the Tender process or reject all bids at any time prior to award of contract, without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for the Buyer's action.

2.28 Notification of award

2.28.1 Prior to the expiry of the period of bid validity, pursuant to Clause 2.16 of this Section - Period of Validity of Bid, the Buyer shall notify the successful Bidder in writing by registered letter/ courier/ E mail to be confirmed in writing by registered letter, that its bid has been accepted

2.28.2 The notification of award shall constitute the formation of the Contract

2.28.3 Upon the successful Bidder's furnishing of Performance Bank Guarantee for Contract Performance, the Buyer may notify each unsuccessful Bidder and shall discharge their EMD

2.29 Award of contract

2.29.1 There shall be only one successful bidder

2.29.2 At the same time as the Buyer notifies the successful Bidder that its bid has been

accepted, the Buyer shall send the Bidder the Proforma for Contract, incorporating all agreements between the parties

2.29.3 Within 15 days of receipt of the Contract, the successful Bidder shall sign and date the Contract and return it to the Buyer

2.29.4 Bidder has to agree to honour all RFP conditions and adherence to all aspects of fair-trade practices in executing the work orders placed by the Buyer

2.29.5 In the case of Bidder whose bids are accepted, Bidder shall be required to give Performance Bank Guarantee as mentioned in Clause 2.15 of this section.

2.29.6 Buyer may, at any time, terminate the contract by giving written notice to the Bidder without any compensation, if the Bidder becomes bankrupt or otherwise insolvent, provided that such termination shall not prejudice or affect any right of action or remedy which has accrued or shall accrue thereafter to Buyer

2.29.7 If at any point during the contract, if the Bidder fails to deliver as per the RFP terms and conditions or any other reason amounting to disruption in service, the Termination, and Exit Management clause shall be invoked

2.30 Tender related condition

2.30.1 The Bidder should conform to the unconditional acceptance of full responsibility of completing the job and executing the 'Scope of Work' of this RFP. This confirmation should be submitted as part of the Technical Bid. The Bidder shall also be the sole point of contact for all purposes of the Contract.

2.30.2 The Bidder should not be involved in any litigation that may affect or compromise the delivery of services as required under this contract. If at any stage of Tendering process or during the Contract, any suppression/ falsification of such information is brought to the knowledge of the Buyer, the Buyer shall have the right to reject the bid or terminate the contract, as the case may be, without any compensation to the Bidder.

2.31 Rejection criteria

2.31.1 Besides other conditions and terms highlighted in the RFP, bids may be rejected under the following circumstances:

a. Pre-qualification Rejection Criteria
   i. Bids submitted without or improper EMD
   ii. Pre-qualification Bid containing commercial details
   iii. Bids received through Telex/ Telegraphic/ Fax/ E-Mail except, wherever required, shall not be considered for evaluation
   iv. Bids that do not conform unconditional validity of the bid as prescribed in the RFP
   v. If the information provided by the Bidder is found to be incorrect/ misleading at any stage/ time during the Tendering Process
   vi. Any effort on the part of a Bidder to influence the Buyer's bid evaluation, bid comparison, or contract award decisions
   vii. Bids submitted by the Bidder after the last date and time of bid submission of bids prescribed by the Buyer
   viii. Bids without the power of authorization and any other document consisting of adequate proof of the ability of the signatory to bind the Bidder

b. Technical Rejection Criteria
   i. Technical Bid containing commercial details
   ii. The revelation of Prices in any form or by any reason before opening the Commercial Bid
   iii. Failure to furnish all information required by the RFP or submission of a bid not substantially responsive to the RFP in every respect
   iv. Bidders not quoting for the complete scope of Work as indicated in the RFP, addendum (if any), and any subsequent information given to the Bidders
   v. Bidders not complying with the services, functionality, specifications, and other terms and Conditions as stated in the RFP
   vi. The Bidder not conforming unconditional acceptance of full responsibility of providing Services in accordance with the Scope of Work and General Conditions of Contract
   vii. If the bid does not conform to the timelines indicated in the bid
   viii. Bidder not scoring minimum marks as mentioned in RFP
c. Commercial Rejection Criteria
   i. Incomplete Commercial Bid
   ii. Commercial Bids that do not conform to the RFP's Commercial Bid format
   iii. The total price quoted by the Bidder does not include all statutory taxes and levies applicable
   iv. If there is an arithmetic discrepancy in the commercial bid calculations, the Buyer shall rectify the same. If the Bidder does not accept the correction of the errors, its bid may be rejected.

2.31.2 If bidder quotes NIL charges/ consideration, the bid shall be treated as unresponsive and shall not be considered

2.32 Fraud and corrupt practices

2.32.1 The Bidders and their respective officers, employees, agents, and advisers shall observe the highest standard of ethics during the Selection Process. Notwithstanding anything to the contrary contained in this RFP, the Buyer shall reject a Proposal without being liable in any manner whatsoever to the Bidder and blacklist for further participation in any bidding process, if it determines that the Bidder has, directly or indirectly or through an agent, engaged in corrupt practice, fraudulent practice, coercive practice, undesirable practice, or restrictive practice (collectively the "Prohibited Practices") in the Selection Process. In such an event, the Buyer shall, without prejudice to its any other rights or remedies, forfeit and appropriate the Bid Security or Performance Security as mutually agreed genuine pre-estimated compensation and damages payable to the Authority for, inter alia, time, cost, and effort of the Authority, regarding the RFP, including consideration and evaluation of such Bidder's Proposal.

2.32.2 Without prejudice to the rights of the Buyer and the rights and remedies which the Buyer may have under the LOI or the Agreement, if an Bidder or Systems Bidder, as the case may be, is found by the Authority to have directly or indirectly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice during the Selection Process, or after the issue of the LOI or the execution of the Agreement, such Bidder or Systems Bidder shall not be eligible to participate in any tender or RFP issued by

the Buyer during a period of 2 (two) years from the date such Bidder or Systems Bidder, as the case may be, is found by the Buyer to have directly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice, as the case may be.

2.32.3 For the purposes of this RFP, the following terms shall have the meaning hereinafter respectively assigned to them:

a. "corrupt practice" means the offering, giving, receiving, or soliciting, directly or indirectly, anything of value to influence the action of any person connected with the Selection Process or in contract execution (for avoidance of doubt, offering of employment to or employing or engaging in any manner whatsoever, directly or indirectly, any official of the Buyer who is or has been associated in any manner, directly or indirectly with the Selection Process or the LOI or has dealt with matters concerning the Agreement or arising there from, before or after the execution thereof, at any time prior to the expiry of one year from the date such official resigns or retires from or otherwise ceases to be in the service of the Buyer, shall be deemed to constitute influencing the actions of a person connected with the Selection Process); or save as provided herein, engaging in any manner whatsoever, whether during the Selection Process or after the issue of the LOA or after the execution of the Agreement, as the case may be, any person in respect of any matter relating to the Project or the LOA or the Agreement, who at any time has been or is a legal, financial or technical consultant/ adviser of the Buyer in relation to any matter concerning the Project;

b. "fraudulent practice" means a misrepresentation or omission of facts or disclosure of incomplete facts, to influence the Selection Process or the execution of a contract to the detriment of the Procurement Entity and includes collusive practice among the tenderers/bidders either prior to or after tender submission, designed to establish tender prices at artificial non-competitive levels and to deprive the Procurement Entity of the benefits of free and open competition.

c. "coercive practice" means impairing or harming or threatening to impair or harm, directly or indirectly, any persons or property to influence any person's participation or action in the Selection Process.

d. "undesirable practice" means establishing contact with any person connected with or employed or engaged by Buyer with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the Selection Process; or having a Conflict of Interest; and

2.32.4 "Restrictive practice" means forming a cartel or arriving at any understanding or arrangement among Bidders with the objective of restricting or manipulating a full and fair competition in the Selection Process.

3 EVALUATION OF BID

3.1 Evaluation Process

3.1.1 The Technical Evaluation Committee constituted by the ITECCS shall evaluate the responses to the RFP and all supporting documents / documentary evidence.

3.1.2 The decision of the TEC in the evaluation of responses to the RFP shall be final. No correspondence will be entertained outside the process of discussion with the Technical Evaluation Committee.

3.1.3 The TEC may, at its discretion, ask for meetings with the Bidders to seek clarifications on their proposals or ask to submit additional documents on their proposal for completing bid evaluation process. The Bidders are required to respond within the prescribed time frame.

3.1.4 The TEC reserves the right to reject any or all Proposals on the basis of any deviations contained in them.

3.1.5 Each of the responses shall be evaluated as per the criterions and requirements specified in this RFP.

3.1.6 The TEC may seek inputs from their professional and technical experts in the evaluation process.

3.1.7 The ITECCS reserves the right to do a reference check of the past experience stated by the Bidder. Any feedback received during the reference check shall be taken into account during the Technical evaluation process.

3.1.8 All responsive Bids will be considered for further processing as below:

a. ITECCS will prepare a list of responsive Bidders, who comply with all the Terms and Conditions of the RFP.
b. All eligible bids will be considered for further evaluation by a Technical Evaluation Committee according to the Evaluation process define in this RFP document.
c. The decision of the Committee will be final in this regard.

3.2 Pre-qualification criteria

Sr. No.	Organizational Strength/Capability	Supporting evidence to be provided
1.	Prime bidder / consortium member of the consortium shall not at the same time be an applicant/ member of any other bid for this RFP	Undertaking by all the bidders as per Annexure 13 (Anti-Collusion Certificate) of Section 9 of this RFP
2.	Prime bidder and all the consortium members must be a legal entity registered in India under the Companies registered under the Indian Companies Act, 2013 or any other earlier Companies Act OR	Copy of Certificate of Incorporation / Registration Certificate

Sr. No.	Organizational Strength/Capability	Supporting evidence to be provided
	Partnership firms registered under the Limited Liability Partnerships (registered under LLP Act, 2008)	
3.	Prime bidder and all the consortium members (in case of consortium) should have GST and valid PAN number	Copy of GST registration certificate issued by GST authorities Copy of PAN card
4.	Prime bidder should have an average annual turnover of INR 1000 crores in last three financial years (ending 31st March 2022)	Copies of audited accounts/ certificate from auditors. The provisional copy of the balance sheet for FY2021-22 may be considered for evaluation purpose only.
5.	Consortium members should have an average annual turnover of INR 100 crores in last three financial years (ending 31st March 2022)	Copies of audited accounts/ certificate from auditors. The provisional copy of the balance sheet for FY2021-22 may be considered for evaluation purpose only.
6.	Prime Bidder should have a current net worth of INR 80 crore as of 31 March 2022	Copies of audited accounts/ certificate along with certified copies of company balance sheet and Profit and Loss Account duly audited from auditors
7.	Prime Bidder should have an experience of handling assignments in India as System Integrator / Master Service Integrator/ Implementation agency/ Technology Solution Provider over the last 5 years for experience as below: 1 project with value 650 crore OR 2 projects with value 500 crore each OR 3 projects with value 300 crore each	Copy of LoI/ Contract/ Client Certificate / Work Order/ Experience certificate
8.	Prime Bidder or consortium members should have an experience of minimum one running project in the last 5 years of Call Centre as below: 1 project with 200 seats OR 2 projects with 160 seats	Copy of LOI/ Contract/ Client Certificate / Work Order/ Experience certificate

Sr. No.	Organizational Strength/Capability	Supporting evidence to be provided
	OR 3 projects with 120 seats OR Emergency Response (Medical or Police or Fire or Disaster management) with Contact Centre solution for at least one year in last 5 years with Central/State Govt. or PSU	
9.	Prime bidder or consortium member (if applicable) should have direct or subcontracting experience in providing training in at least 3 projects having cumulative 1,000 trainees as on bid submission date.	Copy of LOI/Contract/Client Certificate / Work Order/Experience certificate
10.	Prime bidder and consortium members (if applicable) should have all the following valid certifications: 1. CMMI Level 3 or above 2. ISO 9001 3. ISO 27001 4. ISO 2000 With the condition that each Prime Bidder and consortium members should have at least one of the above certificates	Copy of Valid Certificate to be furnished
11.	Prime bidder should have a local office in Lucknow OR If the bidder has no local presence, it should open a local office within 30 days from the issuance the of LOI or contract.	List of offices in India to be duly authorised by bidder OR Undertaking by the prime bidder on firm's letter head committing that office will be setup in Lucknow within 30 days of issuance of LoI/ Signing of the Contract
12.	Prime Bidder and consortium member should not have been blacklisted/ debarred to provide similar services to any State or Central Government Department or Ministry or Public Sector Unit as on bid submission date	Undertaking on firm's letter head in format as per Annexure 2 of Section 9 of this RFP

Sr. No.	Organizational Strength/Capability	Supporting evidence to be provided
13.	Special Power of Attorney for the Bidder who shall sign the Contract Agreement	Special Power of Attorney to sign the Contract Agreement on Non – judicial stamp paper of INR 100/- or such equivalent amount and document duly notarized in format as per Annexure 18/19 of Section 9 of this RFP

Qualification criteria for Cloud Service Provider (CSP)

Sr. No.	Organizational Strength/Capability	Supporting evidence to be provided
1.	The CSP must be incorporated and registered in India under the Indian Companies Act 1956 and should have been in operation in India for more than 5 years.	Copy of Certificate of Incorporation and GST Registration Certificate
2.	The CSP (or its affiliates) must have started offering cloud services (IaaS/PaaS/SaaS) in India or Globally for more than 5 years	Self-Certificate
3.	The CSP must have been empaneled by Ministry of Electronics and Information Technology (MeitY) and the data center should have been audited by STQC	Empanelment certificate needs to be submitted
4.	The CSP should be certified for ISO 27001 (latest version), ISO 27017:2015, ISO 27018:2015	ISO Certificate
5.	The CSP should Conform to at least Tier III standard, certified under TIA 942-b or Uptime Institute certifications by a 3rd party/self-declaration, link to public website	Data Centre Tier III certificate, certified under TIA942-b or Uptime Institute certifications by a 3rd party/self-declaration, link to public website
6.	The CSP is compliant with IT Act 2000 (including 43A) and amendments	Letter from authorized signatory on the letter head of CSP mentioning the compliance
7.	The CSP must offer 99.99% Uptime SLA on compute service from the India region	Letter from authorized signatory on the letter head of CSP confirming the same

Note

1. The period of project experience will be considered as on last date of bid submission.

2. Parent company average annual turnover would be considered for only 100% subsidiary or division or subdivision or branch business unit

3.3 Evaluation of technical bids

3.3.1 **Bidders who meet the pre-qualifications/eligibility requirements would be considered as qualified to move to the next stage of Technical and Financial evaluations.**

Sl. No	Technical Evaluation criteria	Max Marks	Documentary Evidence
1	**Company Profile**	**150**	
1.1	Prime bidder should have an average annual turnover of at least INR 10**00** crores of last three financial years (ending 31st March 2022)	**150**	Copies of audited accounts/ certificate from auditors. The provisional copy of the balance sheet for FY2021-22 may be considered for evaluation purpose only.
1.1.1	> = INR 1200 Crores	150	
1.1.2	> = INR 1100 Crores and < INR 1200	128	
1.1.3	> = INR 1000 Crores and < INR 1100	105	
2	**Company Experience**	**550**	
2.1	Prime Bidder should have experience in handling assignments related to the implementation of Data Centre/Command and Control Centre for State /Central Government / PSU in India in the last 5 years. The bidder to provide a valid completion/commissioning /Go-live certificate	**150**	Copy of LOI/Contract/Client Certificate/Work Order/Experience certificate/ completion/commissioning /Go-live certificate
2.1.1	1 project with the value of INR 150 Crores or above	150	
2.1.2	2 or more projects with the value of INR 100 Crores each	135	
2.1.3	3 or more projects with the value of INR 75 Crores each	120	
2.2	Prime Bidder or consortium member should have an experience of projects related to Emergency Response System (Police/ Medical/Fire/ Disaster management) OR Security, Surveillance, and command centres	**100**	Copy of LOI/Contract/Client Certificate/Work Order/Experience certificate
2.2.1	1 project of value more than or equal to INR 100 Cr.	90	

Sl. No	Technical Evaluation criteria	Max Marks	Documentary Evidence
2.2.2	2 projects of value more than or equal to INR 75 Cr. each	77	
2.2.3	3 projects of value more than or equal to INR 50 Cr. each	63	
2.2.4	Additional marks if any of the projects for Emergency Response system (Police/ Fire/ Medical/ Disaster Management) for Central/State Govt. or PSU	10	
2.3	Prime Bidder or consortium members (if applicable) should have an experience of running Call Centre for the period of at least one year during the last 5 years in India	**100**	Copy of LOI/Contract/Client Certificate / Work Order/Experience certificate
2.3.1	> = 200 Seats	90	
2.3.2	> = 150 Seats and < 200 Seats	77	
2.3.3	> = 100 Seats and < 150 Seats	63	
2.3.4	Additional marks for call centre projects as mentioned above related to Emergency Response (Police or Fire or Medical or Disaster) for Central/State Govt. or PSU	10	Copy of LOI/Contract/Client Certificate / Work Order/Experience certificate
2.4	Prime bidder or consortium members (if applicable) should have an experience of minimum 20,000 trainees/ 50,000 man-days in any State /Central Government for the courses like technology courses and behavioural development in the last 5 years in India.	**100**	Copy of LOI/Contract/Client Certificate / Work Order/Experience certificate
2.4.1	25,000 trainees/ 62,000 man-days	100	
2.4.2	22,000 trainees/ 55,000 man-days	85	
2.4.3	20,000 trainees/ 50,000 man-days	70	
2.5	Prime bidder or consortium partner bidder should have experience of at least 3 out of the 6 below migration/transition activities: 1. Migration of technology of age-old platforms or legacy applications to new platforms 2. Datacentre migration 3. Network migration 4. Transition of manpower 5. Induction of new hardware with replacement of old ones	**100**	Copy of LOI/Contract/Client Certificate / Work Order/Experience certificate

Sl. No	Technical Evaluation criteria	Max Marks	Documentary Evidence
	6. Capacity building of employees for new technology and processes		
2.5.1	3 or more projects	100	
2.5.2	2 projects	85	
2.5.3	1 project	70	
3	**Solution Proposed**	**200**	
3.1	**Technical Presentation**	**100**	
3.1.1	Plan of Risk Management	20	Presentation
3.1.2	Plan for Migration related activities	20	Presentation
3.1.3	Plan for Business continuity and Adequacy of the Work plan	20	Presentation
3.1.4	• Project implementation approach and maintenance plan including comprehensiveness of fallback. • Strategy and planning during the transition to NexGen112	20	Presentation
3.1.5	Assessment of Manpower Deployment, Training, and Handholding plan: • Deployment strategy of Manpower in the migration, implementation, and operations phase • Contingency management • Mobilization of existing resources and additional resources as required • Employee welfare	20	Presentation
3.2	**Demonstration of the following components is required**	**100**	
3.2.1	Voice recording system	20	Demonstration
3.2.2	MDT	15	Demonstration
3.2.3	Mobile	15	Demonstration
3.2.4	ELS/ALS	20	Demonstration
3.2.5	RoIP system	15	Demonstration
3.2.6	AVLS/ GPS solution	15	Demonstration
4	**Proposed resources for the project (As per the criterion mentioned below)**	**100**	**CV in format as per Annexure 10 of Section 9 of this RFP**

Note:

1. *The period of project experience will be considered as on date of publish of RFP.*
2. *The MSI is liable to deliver the same equipment/ hardware which was demonstrated by the MSI during demonstration.*
3. *To ensure this all the hardware shall be available with department thus deposited post demonstration*
4. *The deposited hardware will be returned to the unsuccessful bidders after awarding the contract to successful bidder.*
5. *In case any hardware/software, demonstrated by the MSI, is rejected by the buyer, MSI will be given another chance for the demonstration with different model.*

3.3.2 Marks on proposed key resources:

S.No	Profile for evaluation	Max Marks	Required criteria
a.	Project Director/Manager	10	Overall professional Experience: 2 marks • 15 to 17 years of overall experience: 1 mark OR • Above 17 years of overall experience: 2 marks Experience of project management in govt. sector for implementation of IT with 5 years of experience: 2 marks • 5 to 10 years of experience: 1 mark OR • Above 10 years of experience: 2 marks Emergency Response Experience: 2 marks • 1 project: 1 mark OR • 2 or more projects: 2 marks Experience of project management role leading a team with minimum 40 member in IT implementation projects.: 4 marks • 40 to 80 members 1 project: 1 mark OR • 2 or more projects: 2 marks

S.No	Profile for evaluation	Max Marks	Required criteria
			Certifications: 2 marks • PMP: 2 marks OR • Prince2: 1 mark
b.	Solution Architect (DC, DR)	8	Experience: 2 marks • 10 to 12 years: 1 mark OR • More than 12 years: 2 marks Emergency Response Experience: 2 marks • 1 project: 1 mark OR • 2 or more projects: 2 marks Experience of Tier 3 or above level Data Centre: 2 mark • 1 project: 1 mark OR • 2 or more projects: 2 marks Certifications: 2 marks • MCSE/ MCSA/CCIE (Data Centre) Note: Lab attempted Applicable) / CCNA / TOGAF: 1 mark AND • CCNP: 1 mark
c.	Solution Architect (Applications)	6	Experience: 2 marks • 10 to 12 years: 1 mark OR • More than 12 years: 2 marks

S.No	Profile for evaluation	Max Marks	Required criteria
			Emergency Response Experience: 2 marks • 1 project: 1 mark OR • 2 or more projects: 2 marks Certifications: 2 marks • TOGAF: 1 mark AND • Certified System Architect (CSA): 1 mark
d.	Solution Architect (Network)	5	Experience: 3 marks • 10 to 12 years: 2 marks OR • More than 12 years: 3 marks Certifications: 2 marks • CCNA/CCNP (R&S or Voice)/CWNA: 1 mark And • TOGAF/ CCIE (R&S or Voice): 1 mark Note: For CCIE certificate Lab attempted Applicable
e.	Solution Architect (Information Security)	5	Experience: 2 marks • 10 to 12 years: 1 mark OR • More than 12 years: 2 marks Info security Experience in Government sector: 2 marks • 1 project: 1 mark

S.No	Profile for evaluation	Max Marks	Required criteria
			OR • 2 or more projects: 2 marks Certifications: 1 mark • ISO27001: 0.5 mark AND • TOGAF/ CISA/ CCIE (Security): 0.5 mark Note: Lab attempted Applicable
f.	Database Architect or Modeler	5 (2.5 marks for each resource)	Experience: 3 marks • 10 to 12 years: 2 marks OR • More than 12 years: 3 marks Certifications: 2 marks • DBA Architect level Certification: 2 marks Note: Database certificate should be of proposed database
g.	Database Administrator	10 (2.5 marks for each resource)	Experience: 6 marks • 6 to 8 years: 4 marks OR • More than 8 years: 6 marks Certifications: 4 marks • DBA Architect level Certification: 4 marks Note: Database certificate should be of proposed database

S.No	Profile for evaluation	Max Marks	Required criteria
h.	Business Analyst	2.5	Experience: 1.5 marks • 6 to 8 years: 1 mark OR • More than 8 years: 1.5 marks Experience in Command and control Centre project: 1 mark • 1 project: 0.5 mark OR • 2 or more projects: 1 mark
i.	CAD Expert (from OEM)	6 (2 marks for each resource)	Experience: 3 marks • 10 to 12 years: 1.5 marks OR • More than 12 years: 3 marks Experience in ERSS projects: 1.5 marks • 1 project: 1.2 marks OR • 2 or more projects: 1.5 marks Certifications: 1.5 marks • OEM Certifications: 1.5 marks Note: Certificate should be of proposed OEM
j.	GIS Expert (from OEM)	2.5	Experience: 1 mark • 8 to 10 years: 0.5 marks OR • More than 10 years: 1 mark

S.No	Profile for evaluation	Max Marks	Required criteria
			Experience in ERSS/ Smart City projects: 1 mark • 1 project: 0.5 marks OR • 2 or more projects: 1 mark Certifications: 0.5 mark • OEM Certifications: 0.5 mark Note: Certificate should be of proposed OEM
k.	Telephony & ACD expert (from OEM)	3 (1 mark for each resource)	Experience: 1.5 marks • 10 to 12 years: 0.5 marks OR • More than 12 years: 1.5 marks Experience in command and control projects: 1.5 marks • 1 project: 0.9 mark OR • 2 or more projects: 1.5 marks
l.	Radio over IP specialist (from OEM)	4	Experience: 2 marks • 10 to 12 years: 1 mark OR • More than 12 years: 2 marks Emergency Response Experience: 2 marks • 1 project: 1 mark OR • 2 or more projects: 2 marks
m.	Master Trainer	5	Experience: 2 marks

S.No	Profile for evaluation	Max Marks	Required criteria
			• Minimum 8 years: 1 mark OR • 8 years and above: 2 marks Emergency Response Experience: 2 marks • 1 project: 1 mark OR • 2 or more projects: 2 marks Work experience for disaster framework such as Hyogo Framework /Sendai Framework • 1 or more projects: 1 mark
n.	Documentation Specialist	4 (1 marks for each resource)	Experience: 4 marks • 7 to 10 years: 2 marks OR • More than 10 years: 4 marks
o.	SOC Expert	4 (1 mark for each resource)	Experience: 2 marks • 7 to 10 years: 1 mark OR • More than 10 years: 2 marks Experience in Government projects: 2 marks • 1 project: 1 mark OR • 2 or more projects: 2 marks
p.	VAPT Expert	4 (1 mark for each resource)	Experience: 2 marks • 7 to 10 years: 1 mark OR • More than 10 years: 2 marks

S.No	Profile for evaluation	Max Marks	Required criteria
			Experience in Government projects: 2 marks • 1 project: 1 mark OR • 2 or more projects: 2 marks
q.	Data Migration Expert	4 (2 marks for each resource)	Experience: 2 marks • 10 to 12 years: 1 mark OR • More than 12 years: 2 marks Experience in Government projects for Data Migration: 2 marks • 1 project: 1 mark OR • 2 or more projects: 2 marks
r.	IT Security & asset Manager	4 (0.5 marks for each resource)	Experience: 4 marks • 8 to 10 years: 2 marks OR • 10 years and above: 4 marks
s.	ERSS Domain Expert	2	Experience: 1.5 marks • 5 to 7 years: 1 mark OR • More than 7 years: 1.5 marks International experience of emergency response: • 1 or more projects: 0.5 marks
t.	Project Head Contact Centre	2	Experience: 1.5 marks • 15 to 17 years: 0.5 mark OR

S.No	Profile for evaluation	Max Marks	Required criteria
			• More than 17 years: 1 mark Certification of Project Management: 0.5 marks • PMP: 0.5 marks
u.	Communication Officer Manager (CO Manager)	4 (1 mark for each resource)	Experience: 4 marks • 10 to 12 years: 2 marks OR • More than 12 years: 4 marks

3.3.3 The technical presentation should be delivered by the bidder before the Technical Evaluation Committee as a part of Technical evaluation process.

3.3.4 The presentation should be delivered by the proposed project manager of the bidder's along with key resources of the proposed team.

3.3.5 Wherever there is problem in providing name or cost of project due to Non-disclosure agreements with the clients, the bidder can provide a certificate from an independent auditor or Company Secretary. The bidder has to provide an undertaking that to this effect.

3.3.6 Minimum passing marks in technical evaluation is 700 out of 1000.

3.3.7 Parent company project experience, financial capabilities and certifications would be considered for only 100% subsidiary or division or subdivision or branch business unit which is registered in India. Bidder to provide necessary proof for subsidiary of the parent company.

3.4 Evaluation of commercial bids

3.4.1 The Financial Bids of technically qualified Bidders will be opened on the prescribed date in the presence of Bidder representatives.

3.4.2 If a firm quotes NIL charges / consideration, the bid shall be treated as unresponsive and will not be considered.

3.4.3 The Lowest Quoting Bidder will be selected as per the lowest Gross Total Value (GTV), designated as L1, for awarding of the contract.

3.4.4 The bid price will exclude all taxes and levies and shall be in Indian Rupees and mentioned separately.

3.4.5 Any conditional bid would be rejected

3.4.6 Errors & Rectification: Arithmetical errors will be rectified on the following basis: "If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail, and the total price shall be corrected. If there is a discrepancy between words and figures, the amount in words will prevail".

3.4.7 Predatory Pricing

The buyer may, in case of predatory pricing/ abnormally price low bid or any line item in BoQ, seek written clarifications from the bidder, including detailed price analysis of its bid price in relation to scope, schedule, allocation of risks and responsibilities, and any other requirements of the bid document. If after evaluating the price analysis, the buyer determine that the bidder has substantially failed to demonstrate its capability to deliver the contract at the offer price, the Purchase may reject the bid.

4 SCOPE OF WORK

The NexGen UP112 project will be a geographically spread initiative involving multiple stakeholders. Its implementation will be complex, and its ultimate success depends on all the stakeholders; the role of MSI is very critical and hence MSI is required to design and implement a comprehensive and effective project planning and management methodology together with efficient & reliable tools.

The MSI shall address the following but not limited to:

i. Create an organized set of activities for the project
ii. Coordinate and collaborate with various stakeholders including the police department, Home department, District Police offices and Commissionerate, etc.
iii. Establish and measure resource assignments and responsibilities
iv. Construct a project plan schedule including milestones
v. Measure project deadlines, budget figures, and performance objectives
vi. Communicate the project plan to stakeholders with meaningful reports
vii. Provide facility for detecting problems and inconsistencies in the plan

During the project implementation the MSI shall report on following items:

i. Results accomplished during the period.
ii. Cumulative deviations to date from schedule of progress on milestones as specified in this RFP read with the agreed and finalized Project Plan.
iii. Corrective actions to be taken to return to planned schedule of progress.
iv. Proposed revision to planned schedule provided such revision is necessitated by reasons beyond the control of the MSI.

As part of the project management activities, the MSI shall also undertake:

i. Issue Management to identify and track the issues that need attention and resolution from the State.
ii. Scope Management to manage the scope and changes through a formal management and approval process
iii. Risk Management to identify and manage the risks that can hinder the project progress

The detailed project plan shall clearly specify the various project milestones and project deliverable schedules. It shall also include the following:

i. Project Organization and Management plan
ii. Software Design and Development plan
iii. Implementation plan
iv. Pre-commissioning, Operational and User Acceptance Testing Plan
v. Design, Delivery and Installation Plan for Hardware and Network
vi. Training Plan
vii. Support Service Plan

viii. Task, Time, and Resource Schedules (List of tasks, the dependency among the tasks, the duration to perform the tasks, the resources allocated to perform the tasks, the scheduled start and finish dates for the task)
ix. Post-support Service Plan
x. Technical Support Plan
xi. Quality Assurance and Control Process details which must include (but not limited to) detailing on Metrics, Reviews, Problem Reporting and Corrective action etc.
xii. Technical and Operational Process which must include (but not limited to) detailing on Methods, Tools, Techniques etc.

MSI shall hold weekly/fortnightly review meetings with the department providing detailed report on the progress of the project (Project Progress Report) clearly highlighting the activities completed in the reporting period, activities planned for the next reporting period, deviations from the planned dates, issues or concerns affecting the project progress, impact on the overall project timelines, project related risks with their mitigation plans.

MSI shall allow or support the department or the nominated agencies of the department to conduct the review of the project as and when required.

4.1 Approach

The MSI (Master System Integrator) shall be responsible for the operation and maintenance of the existing UP112 project while catering to all the additional requirements of the NexGen UP112.

The successful MSI has to use some the existing infrastructure, hardware and software solution(including those added before the date of signing of contract) by extending the AMC and licenses. Activities will be largely but not limited to upgradation or replacement of existing IT/Non-IT Infrastructure, integrations, ensuring compatibility of protocols, addition of hardware and software etc. In case any new components are required to fulfil the functional requirements of the published RFP and meet the SLA requirements, the successful MSI will be responsible for performing all the associated activities to comply with same.

Details of required new procurements or upgradation for hardware and software are detailed under section 4.27.7 (applications) and 4.27.8 (Hardware)

NexGen UP112 has focused on migration of system on cloud as a principal. SI to have DRC set up on cloud from Day 1 i.e., from the beginning of NexGen 112.

At the time of launch/go-live DC shall be on in-premise model. It shall be migrated to cloud in a phase wise manner during course of the project.

Note:

i. The proposed Hardware and Software solutions of MSI must be stable and functioning for entire tenure of the project. Considered Hardware and Software should not have end of life/ end of support during the tenure of project.

ii. MSI shall ensure the smooth functioning of NexGen UP112 project in the existing premises. MSI need to make suitable provisions for hardware/ software etc. for smooth execution of project.
iii. All the proposed applications shall be compatible to the cloud environment
iv. The details of all the existing components have been comprehensively specified in 4.27.7 (applications) and 4.27.8 (Hardware) of this RFP.
v. MSI has to ensure that the existing data, databases, reports, and recordings are migrated the way it is available/ hosted in the current system.

4.2 Project Timeline

This project consists of a series of activities like transition from the TSP (Technology Service Provider), design and development of the new system, maintaining the existing UP112 system till acceptance followed by operations and maintenance NexGen UP112 system.

In this context, the project implementation timelines for the design of the NexGen UP112 have been formulated to ensure service continuity of UP112 system while the new solution is being developed and implemented.

During the contract period, the MSI is expected to complete the design and implementation of the envisaged application and solution enhancements of NexGen UP112.

1. Contract signing (T)

The contract will be signed on T date, after which the Knowledge Transfer stage will be initiated.

2. Phase-0: Knowledge transfer (T+1 Month) - 1st month

This stage will start from the day of contract signing with the MSI or date of issue of LoI, whichever is earlier.

i. Scope of work: The MSI will take the knowledge transfer of UP112 from TSP.
ii. SLA related to performance of UP112 system shall not be applicable on MSI in this month
iii. TSP will assist MSI with the complete audit of the system including licenses and physical assets.
iv. MSI to comply with all the deliverables for this stage as detailed under section “Deliverables” section 4.4

3. Phase-1: Transition and O&M of existing UP112 (from start of T+2 month till the end of T+5 month) - Duration: 4 months

3.1. Phase-1a: Transition (T+2 month) – 2nd Month

i. **Scope of work:** The MSI will shadow the TSP to run the UP112 system, including all the infrastructure, network, and other responsibilities of the system.
ii. **Change request:** Any change requests by ITECCS during this stage will be implemented by the TSP

iii. **SLA applicability:** No SLA will be applicable on MSI in this duration
iv. **Asset transfer:** Complete asset handover shall be executed by the end of this stage.
v. MSI to comply with all the deliverables for this stage as detailed under section "Deliverables" section number 4.4

3.2. Phase-1b: Operations and maintenance of existing UP112 system (T+3 month – T+5 month) – 3rd, 4th, and 5th Month

i. **Scope of work:** The MSI shall be responsible to operate and manage the existing UP112 system till the NexGen UP112 system is commissioned. Shadow support shall be provided by the TSP in this duration.
ii. **Change request:** Any change requests generated on UP112 will be implemented by the MSI.
iii. **SLA applicability:** Existing Service levels of NexGen UP112 will be owned by the TSP.
iv. MSI to complete the procurement of software and hardware and deliver all hardware (client end infrastructure, DC-DR, end-user infrastructure) required for the project, activity to be completed till 3rd month (T – T+3)
Note: The MSI is liable to deliver the same equipment/ hardware which was demonstrated by the MSI during demonstration. To ensure this all the hardware shall be available with department thus deposited post demonstration.
v. MSI to comply with all the deliverables for this stage as detailed under section "Deliverables" section 4.4

4. Phase-2: Design & Implementation of NexGen UP112 system (T+3 to T+5 months or System Acceptance) – Duration: 3 months

This stage will begin after the completion of the stage-1a. The MSI will design, develop, and implement the NexGen UP112 system. The MSI will also procure, configure, commission, and integrate the listed key components to build the desired NexGen UP112 system.

Phase-2 can be further sub-divided into 3 sub-phases:

4.1. Phase - 2a (T + 3 month), 3rd Month

i. Procurement and delivery of all ICT hardware (client end infrastructure, DC-DR, end-user infrastructure) required for the project
ii. SITC of equipment – Supply of Installation Testing and Commissioning of all S/W and H/W required for making the system fully functional
iii. Design and development of the modules as listed under section 7.5
iv. MSI to comply with all the deliverables for this stage as detailed under section "Deliverables" section 4.4

4.2. Phase - 2b (T + 4 month), 4th Month

i. /Designing and development of other project components related to software solutions and systems required to operationalize the NexGen UP112 system.
ii. The hardware will be commissioned in this stage (till T + 4 months), along-with setting up of the software environments.
iii. All the other requirements for implementation, as per the detailed scope of work, need to be completed.
iv. The MSI needs to demonstrate the capability of NexGen UP112 system to take over from UP112
v. MSI to comply with all the deliverables for this stage as detailed under section “Deliverables” section number 4.4

4.3. UAT and System Acceptance (T + 5 month), 5th Month

i. System Acceptance shall mean that from this point onwards, the newly designed, developed, deployed, and installed NexGen UP112 system is accepted by the ITECCS as per the criteria defined in section 4.4. UP112 has an option to provide Provisional system acceptance certificate for successful transition of UP112 as NexGen UP112. The provisional system acceptance shall not be considered as acceptance of Functional and Integration testing **of entire system** including Hardware, Software, Network, and other components. This certificate shall be provided for successfully Installing, Testing and Commissioning of the critical software and hardware. Based on provisional acceptance certificate payment for **respective** and live applications and services can be commenced as those defined for O&M phase. UP112 reserves the right to evaluate and consider the readiness of system for issuing of Provisional System Acceptance Certificate.
ii. MSI to comply with all the deliverables for this stage as detailed under section “Deliverables” section number 4.4

5. Phase-3: Operations and maintenance of the NexGen UP112 system (start of T+6 month till the end of T+65 month) – Duration: 60 months

i. The MSI shall be responsible to operate and maintain the NexGen UP112 system, as per the requirements of the RFP
ii. The SLAs, as detailed in Service Levels for NexGen UP112, shall be complied by the MSI
iii. MSI to comply with all the deliverables for this stage as detailed under section “Deliverables” section number 4.4

4.3 Phases of Project

The whole project is divided into two stages:

i. Implementation stage - 5 Months (from start of T+1 till end of T+5)
ii. Operations and maintenance stage - 60 Months (from start of T+6 till end of T+65)

Note: The proposed timeline for the project includes 5 months of knowledge transfer, implementation and UAT followed by 5 years (60 months) of O&M stage that may be extended by 2 optional years at the discretion of ITECCS, at same cost of 5th year. During extension stage no additional cost can be charged by MSI until and unless new equipment is purchased due to EoI or EoS. Also, MSI cannot quote the cost of new equipment for extension stage more than the cost quoted before in the financial bid.

The decision on extension will be taken by ITECCS, while considering the following:

i. Circumstances inescapably requiring taking recourse to this option
ii. Time constraints or other serious impediments in selection of replacement MSI
iii. Satisfactory performance of the MSI
iv. Technological reasons

Also, in case implementation stage is delayed then:

i. MSI would continue the UP112 operations post taking it over from MSI as defined in stage 1.b.
ii. The extra time elapsed in implementation stage shall be reduced from O&M stage. Thus, no extra cost shall be charged from department for implementation also cost deduction will be made O&M stage.

4.4 Project Milestones and Deliverables

Project timelines and deliverables are provided below. MSI needs to adhere to these timelines throughout the project period.

Note: Deliverable means the products, infrastructure and services agreed to be delivered by the MSI in pursuance of the agreement as defined more elaborately in the RFP and includes all documents related to NexGen UP112, user manual, business designs, the process documentations, the artifacts, the training materials, technical manual, design, process and operating manuals, service mechanisms, policies and guidelines (such as security related, data migration related), inter alia payment and/or process related etc., source code and all its modifications for any bespoke development done as a part of this project.

S. No	Module/ Activity	Milestone	Timeline (In month)	Deliverable/ Documents
1	LoI issue or contract signing	Letter of Signing of contract or issuance of LoI by ITECCS and submission of PBG	T day	Submission of PBG
Knowledge transfer (Phase 0) (1st Month Onwards)				
2.1	Manpower deployment	50% of Technical resources (including all key resources) of Implementation stage	(T+1 Month) - 1st month	1. Letter of deployment with all details of resource 2. NDA with MSI on behalf of team members

S. No	Module/ Activity	Milestone	Timeline (In month)	Deliverable/ Documents
				3. Deployment checklist approval
2.2	Planning	Submission of detail project plan for all locations like DC, DR, UP112 HQ, Field Locations and PRV including network plan, IT security plan and other components to ITECCS		4. Detailed project plan document tagged with timelines 5. Test plan document
2.3	Handshaking between MSI and TSP	Knowledge Transfer Completion Certificate		1. Existing inventory, assets list (with details of functional and non-functional items) and acceptance certificate by MSI 2. Weekly work progress status report (as per template defined by ITECCS) 3. A detailed plan of the Knowledge Transfer 4. Knowledge Transfer certificate to TSP by MSI
2.4	Knowledge Transfer	Understanding of UP112 by MSI		1. Weekly status report on the progress of KT activity 2. Report on detailed understanding of UP112 system and operations
Transition and O&M of existing UP112 (Phase 1) (from T+2 Month to T+5 Month)				
3.1	Manpower deployment	100% of Technical resources of Implementation stage	(T+2 month – T+5 month) – 2nd, 3rd, 4th, and 5th Month	1. Letter of deployment with all details of resource 2. NDA with MSI on behalf of remaining team members 3. Deployment checklist approval
3.2	Capacity Building	1. Training need analysis for all stakeholders 2. Capacity building planning		1. Training Resource Plan 2. Training Calendar
3.3	Go ahead for Procurement	Approval letter from department for procurement of the products	T to T+3 months	1. Complied Technical Specification on OEM letter head
3.4	Procurement and delivery of hardware and Software	Procurement and delivery of all software and hardware (at all project locations such as DC, DRC, UP112 HQ, Filed Locations and PRVs) required for the project		1. Specification of OEM component 2. Copy of purchase order of MSI issued to OEM 3. Warranty and AMC Support Document

S. No	Module/ Activity	Milestone	Timeline (In month)	Deliverable/ Documents
Design & Implementation of NexGen UP112 system (Phase 2a) (T+3 Months onwards)				
4.1	Network and Software Design	Acceptance of documents such as system requirement specification, design documents by ITECCS	T + 3-month, 3rd Month	1. SRS document including system design, Network Design document (NDD), High Level Design Document (HDD), DB design, application arch etc. 2. FRS document 3. High level design document 4. Low level design document 5. Deployment document in development, QA, and Production environment 6. Deployment checklist 7. Test cases 8. Data Migration Approach (For complete historical data from all applications) 9. Data Storage Policy
4.2		Initiation of applications development and acceptance of compliance document by ITECCS		1. Technical compliance documents for all the application 2. Release Plan and Release Note
Design & Implementation of NexGen UP112 system (Phase 2b) (T+4 Month onwards)				
5.1	Capacity Building	1. Modules and training content finalization 2. Facilitation of training centres in the field	T + 4-month, 4th Month	1. Stakeholder wise course content and Training plan 2. Deployment checklist approval
5.2	Contact centre Manpower at UP112 HQ and OMCs	Hiring and training of all contact centre resources		1. Letter of deployment with all details of resource 2. NDA with firm on behalf of team members 3. Deployment checklist approval 4. Training Plan 5. Module wise rollout plan 6. Business continuity plan
5.3	Upgrade and Installation of Hardware	Upgrade, Installation, and setup of Hardware at Data centre (DC), OMCs, Field and PRVS. Cloud environment setup for DRC		1. PDI report from site supervisor 2. POST (Power-On Self-Test) diagnostic report

S. No	Module/ Activity	Milestone	Timeline (In month)	Deliverable/ Documents
5.4	Upgrade and development of software and applications	1. Development of software and applications as per approved FRS and SRS with integrations within applications. 2. Upgrade of existing software (wherever required) as per RFP requirements		1. Software design document
5.5	Data Migration	Sign off from department for complete re-processing and validation of historical data		1. Migration of historical data as per approved plan
5.6	Network and security components commissioning	1. Setup of network connectivity and requisites security components at UP112 HQ, OMC, and another field location 2. Setup of network and security		1. PDI report from site supervisor
5.7	Exit	Exit Plan		1. Exit Management Plan
NexGen UP112 UAT and System Acceptance stage (T+5 Month)				
6.1	User Accepting Testing (UAT)	1. Acceptance of all applications, and hardware, at UP112 HQ, OMC, and other field location as per EMS reports	T+5 Month, 5th Month	1. UAT Test report including test cases and result Report on Closure of Audit issues (if any) 2. Bugs or issues report with status like resolved, pending etc. 3. System acceptance as per Test Plan Document
6.2	System Acceptance	UAT for DC, DRC, UP112 HQ and OMC for all equipment such as MDT and Radio devices configured in vehicles		1. Sign off from department for complete re-processing and validation of historical data 2. Bugs or issues report with status like resolved, pending etc.
NexGen UP112 O&M stage (T+6 to T+65 months – Duration: 60 months)				
7.1	Manpower deployment	100% of Trained O&M resources	T+5+ 1 day	1. Letter of deployment with all details of resource 2. NDA with MSI on behalf of team members 3. Deployment checklist approval

S. No	Module/ Activity	Milestone	Timeline (In month)	Deliverable/ Documents
7.2	Compliance	Maintenance of operations at defined standard	Quarterly	1. Change management plans 2. Defect or Bugs log with resolution 3. Change Request logs 4. Services procedures for the SOC report 5. Fortnightly status reports 6. T&A every year for course correction 7. Upgradation Plan
			Half Yearly	1. Preventive Maintenance Report 2. Corrective Measure Report
7.3	Issue Resolution	Any issue related to technology failure or down or corrective measures to be opted for upgrade or correction or proper functioning of the project	As and when requested by ITECCS - delivery within 24 hrs	1. Root cause analysis reports (RCA)
7.4			As and when requested by ITECCS - delivery within 30 days	1. Technical and Financial Bid
7.5	Technology refresh	System upgradation and betterment	Every 2 year (From System Acceptance)	1. Quality Audit report 2. Closure report for identified issues 3. Proof of renewal of support for all IT infrastructure products and other system software 4. Technology refresh including SLA review and reduction of TCO plan
7.6	DC Movement to Cloud	DC migration and Setup to Cloud	T+24toT+60	1. DC Migration Plan 2. Application UAT report on cloud 3. System Acceptance report
7.7	Audits	Safety and security of system	Every quarter after initiation of O&M stage (from 6th month in ideal case)	4. Penetration Test Report 5. Vulnerability Test Report 6. Penetration Testing and Vulnerability Closure Report 7. 3rd Party assessment reports

S. No	Module/ Activity	Milestone	Timeline (In month)	Deliverable/ Documents
7.8	Update management	This would include OEM patches/OEM version/upgrades/ customizations of software/ applications, Database, and operating systems as and when required during project period. The MSI has to take necessary approval with the fallback strategy before such updates.	Hal yearly	1. Meeting with OEM 2. Version Control Document 3. Application Assurance Certificate from OEM 4. Business continuity plan
7.9	Capacity Building	1. Training need analysis for all stakeholders 2. Capacity building planning 3. Training feedback	As and when required	T&A Report
7.10	Capex Purchase	Capex such as EoS products during the course of project should be supplied and installed 6 months before the EOS	Yearly	1. Training Resource Plan 2. Training Calendar 3. Training feedback report
			As and when required	1. Specification of OEM component 2. Copy of purchase order of MSI issued to OEM 3. Warranty and AMC Support Document
7.11	Inventory	Stock check list	Half yearly	1. Inventory audit report
7.12	Integration	Submission of integration plan with other government agencies	As per request by ITECCS	1. Detailed integration plan document with approach, level, list, and timelines of integration

4.5 Implementation stage

4.5.1 Work Stream 1: Knowledge Transfer, Transition Management and O&M of UP112

MSI will perform all the functions and services necessary to accomplish the Transition of the entire suite of applications, infrastructure, and services under UP112 from the current MSI on or before the specified completion dates. MSI will be responsible for the overall management of the transition in accordance with the transition plan and will work to ensure the transition is completed on schedule and to identify and resolve any problems encountered. The MSI will demonstrate to ITECCS reasonable satisfaction, prior to the completion of Transition stage, that it is ready to take over the O&M UP112 without the support of the TSP. For removal of all doubts, it is clearly stated that all activities that are part of scope of work for UP112 as performed by the TSP, shall be within the scope of work for the MSI during the implementation stage of NexGen UP112 i.e., till T + 5 months or until acceptance of NexGen UP112, whichever is later.

a. Responsibilities of the MSI during the Knowledge Transfer (T + 1) shall include the following:

i. The MSI will be required to submit a detailed Knowledge Transfer plan at the start of the KT stage, listing all the activities from their end, including the expectations from TSP. A checklist (as part of knowledge transfer plan) needs to be prepared by the MSI for ensuring proper knowledge transfer. This shall be reviewed and subject to approval by ITECCS.

ii. The TSP shall provide all knowledge transfer of the system to the MSI to the satisfaction of ITECCS as per the specified timelines and as per detailed Exit Management Plan.

iii. The knowledge transfer shall include initial and ongoing training on UP112, training materials, operations manuals, procedure manuals and deployment/ installation guide.

iv. The TSP shall conduct detailed Knowledge Transfer sessions for the MSI (such sessions should be recorded by the MSI for future playback) and shall concentrate on the following:

1. Study of the functional specification documents, documentation of business processes, presentations to ITECCS to confirm understanding
2. Identification and deep dive into all documents (like High Level design document, Low Level Design Document, User Manual, SRS etc.)
3. Details of integration with other systems
4. Details and access to the codes, scripts, jobs, etc. for study and assist in understanding the documentation of UP112 and its various components, understanding of development, support processes, configuration management processes, etc.
5. Understanding of various environments (development, UAT, Production etc.), and obtain training on all the existing tools used, processes followed, and activities performed
6. Understanding of existing infrastructure and network management
7. Walkthrough of the helpdesk setup and NOC and SOC solution.
8. Understanding of all existing issues in the IT landscape and their impact; of the issues faced by the TSP while implementing and managing the existing solutions and the resolutions for the same; and of any special behaviour (if any) exhibited by the overall solution or the individual applications.

v. It is clarified that the MSI is required to deploy technically competent resources, in the specific solution areas deployed in UP112, during the Knowledge Transfer (KT) stage and Transition stage. The TSP shall not be responsible for imparting any basic technical skillset to the resources of the MSI, which would be deemed as a pre-requisite.

vi. The MSI is required to utilize this time period in the most efficient and

effective manner, to ensure that they are able to take-over the operations of UP112. The MSI should deploy its project management, domain as well as technical manpower to absorb the KT sessions. They should conduct site visits to each of the client locations to get an understanding of the requirements at each of the locations.

vii. The MSI will be required to submit a weekly status report on the progress of KT activities.

viii. During this stage, the MSI shall be required to submit a report on the detailed understanding of UP112 system and operations, which will be reviewed by ITECCS and this will form the basis of start of the next stage, i.e., Transition stage.

ix. MSI needs to submit the all the deliverables to ITECCS as stipulated in the RFP during this stage, as these shall be a critical input for the success of subsequent stages of the project.

x. Assistance from TSP to MSI will be ensured by ITECCS such as in terms of the complete audit of the system including licenses and physical assets.

b. Exit management responsibilities of the TSP:

i. ITECCS will ensure scheduling of session for knowledge transfer as per contract of TSP and ITECCS during 1st month of project.

ii. Exit Management Plan: TSP will initiate the knowledge transfer as per submitted plan and schedule.

iii. Transfer of Assets: Transfer both IT and non-IT Assets acquired for the UP112 project to the MSI. The list of assets shall cover those under the purview of current operator as well as its subcontractors

iv. Testing: The TSP shall ensure that the system being handed over is tested rigorously before being handed over to the MSI

v. Close critical issues: The TSP shall close all critical open issues as on date of exit. All other open issues as on date of Exit shall be listed and provided to UP112.

vi. Risks: All the risks during transition stage shall be properly documented by the TSP and mitigation measures be planned in advance along with the MSI and recorded in the Exit Management Plan so as to ensure smooth transition without any service disruption.

vii. Transfer of Agreements: Arrange or provide support for Assignment / Transfer of Agreements with all the OEMs / contractors / sub-contractors who are being used by the current operator in the execution of the UP112 project.

viii. Provision of Information: Provide access to information reasonably required to define the current mode of operation associated with the provision of services and access and copies of all information / data / documentation, prepared, or maintained, pertaining to UP112, services rendered including but not limited to applications, Business and IT Operations, and other performance data.

ix. Access Rights: Provide reasonable rights of access to UP112 Project Location and premises where assets are located. Provide access to

TSP's employees and facilities as reasonably required to understand the methods of delivery of the services employed by the TSP and to assist appropriate knowledge transfer.

x. Personnel: Provide a list of all employees (with job titles) of the TSP dedicated to providing the services. To the extent that any Transfer Regulation does not apply to any employee of the TSP, the TSP shall not enforce or impose any contractual provision that would prevent any such employee from being hired by ITECCS or MSI in case an offer of employment or contract for services is made to such employee.

c. Responsibilities of the TSP during UP112 Transition and O&M stage (Phase 1(a) and 1(b)) i.e., from start of T+2 to the end of T + 5 month: 2nd, 3rd, 4th, and 5th Month

During the Transition stage (Phase 1(a) and 1(b)), the MSI will be provided a hands-on exposure to the UP112 system. During the first month, the MSI will shadow the entire team of the TSP, at all the client locations. During the next 1 month, the MSI shall be managing the entire responsibilities of UP112, however the TSP shall deploy its team as a shadow support and will be responsible for supervising and reviewing all the activities of the MSI.

1. Phase-1a: Transition (T+2 months) – Duration: 2nd month

i. The MSI shall detail the transition plan and transition risk management plan (submitted at the proposal stage), at the start of this stage. These plans shall build on the already submitted plans (submitted at the bidding stage) and should not entail any deviation from the principles laid down in the proposal made. ITECCS team will finalize the scope of the activities that will be taken over by the MSI from the TSP

ii. TSP will take the lead in this stage and continue with the usual operations of maintaining and managing the UP112 system

iii. MSI will shadow the TSP with the purpose of understanding the existing system and preparing for takeover in the next stage

iv. The MSI would need to create a separate team to align with the resources deployed by TSP during the transition stage. Each team member observes the activities done by the TSP. Process and application knowledge is built, and hands-on application and infrastructure know-how is acquired. This knowledge will be documented for future use by the MSI.

v. Study of existing Operations (As-Is Architecture): The MSI shall study and document the current operations of existing UP112 system. After the study of as–Is Architecture, MSI will work out a plan for the To-Be architecture, with any changes or improvements required in the existing operations after the transition

vi. Old SLAs of UP112 will be applicable to the TSP during this stage

vii. Success criteria for the transition will be defined in this stage by ITECCS, and only upon meeting the success criteria, the project will

move to stage 1(b), where the MSI will be in lead for managing UP112 independently.

viii. Transfer and handover of all assets from old to MSI and everything that is a part of UP112 project to the MSI

ix. AMC: The TSP shall handover all AMC support related documents, credentials etc. for all OEM products supplied / maintained in the system. It will also handover MoUs signed for taking services taken from any of the sub-contracted agencies

x. The MSI shall examine and document or cause it to be documented by the TSP any process, code, software which is either not documented or is operated in an ad-hoc manner in consultation with the TSP to avoid any surprises once the MSI takes over operations.

xi. Considerations during requirement gathering stage: For the requirement gathering exercise, certain methodologies which shall be followed are:

- Workshop mode will be used for requirement gathering, to ensure group participation by ITECCS users for eliciting requirements
- Design thinking and other interactive methodologies should be used for understanding user expectations
- UI/UX designers should be involved during requirement gathering and design stage, to design the most personalized user experience
- Study on the global practices for baselining the requirements

a. The requirement gathering shall be done at ITECCS office premises in Lucknow, as well as any other ITECCS office locations as stated above in this RFP. ITECCS will designate the individuals who would be responsible for providing an overview of user requirements to the MSI. The MSI shall cover all the stakeholders approved by ITECCS in the requirement gathering process.

b. On gathering the requirements, MSI shall analyse these requirements to ensure the requirements are complete, accurate, consistent, and unambiguous.

c. Weekly review meetings shall be organized to keep ITECCS abreast of the work progress. MSI will be required to present a summary of all the requirements gathered during the week, and ITECCS representatives may provide their feedback or suggestions. Minutes of these meetings should be prepared by the MSI within 2 working days and circulated to ITECCS for agreement.

d. The requirement gathering stage shall culminate in documentation of the requirements in form of technical and functional requirement documents. ITECCS will only approve any incremental requirements / modifications gathered on existing modules, or requirements gathered for any new modules.

2. Phase-1b: Transition (from start of T+3 month to T+5) – Duration: 3rd, 4th, and 5th Month

i. The MSI will take the lead in this stage, in managing the UP112 system and the TSP will provide shadow support to the MSI but exit of TSP will subject to the approval of ITECCS
ii. The MSI will carry out the activities under the supervision of the TSP
iii. The MSI shall continue the business on the UP112 system and deliver the services to the stakeholders. The MSI shall also manage the existing operations including the applications, facility management, etc.
iv. Any change requests generated on UP112 hereafter will be implemented by the MSI as per the Change Control procedures defined in UP112 RFP (and any amendments thereafter) but the payment for change requests generated in the stage-1b shall be deferred and paid to the MSI.
v. SLA applicability: During this period, the MSI shall be responsible for maintaining the old SLAs for UP112. The TSP shall be paid their monthly invoices (decided as part of the UP112 RFP) less any deductions basis the average performance of the UP112 system on SLAs. Any further degradation in performance of the UP112 system (measured on the SLAs of UP112) will be deductible from the invoice of the TSP.
vi. MSI's must initiate hiring and training of communication officer to be deployed.
vii. As part of the transition process, the MSI will perform the following activities (including but not limited to) to continue to meet ITECCS business requirements without any disruption to UP112's services.

1. Validate the inventory of all project related assets (H/w & S/w) as submitted by the TSP
2. Facilitate the effective and smooth transfer of assets from the TSP
3. Assume operational ownership (including commercials if any) of the software licenses to the MSI and renewal of Third-Party Contracts. However, DNS Domain ownership shall remain to be of UP112
4. Complete DC-DR shifting (if any) and implement the agreed upon physical security requirement
5. Implement the required governance model
6. Develop and implement the required plans, as well as the operational change management processes required to implement the transition plan
7. Prepare the functional, system, technical and process documentation of the existing applications and processes necessary for continued operation and maintenance of the services
8. Provide the program and project management services associated with the above activities

At the end of transition stage, MSI shall be required to submit compliance report with respect to transition responsibilities to UP112.

d. MSI Exit Management

An Exit Management plan shall be furnished by MSI in writing to the GoUP within 90 days from the date of signing the Contract, which shall deal with at least the following aspects of exit management in relation to the contract as a whole and in relation to the Project Implementation, and Service Level monitoring.

i. A detailed program of the transfer process that could be used in conjunction with a Replacement Service Provider including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer.
ii. Plans for provision of contingent support to Project and Replacement Service Provider for a reasonable period after transfer.
iii. Exit Management plan in case of normal termination of Contract period
iv. Exit Management plan in case of any eventuality due to which Project is terminated before the contract period.
v. Exit Management plan in case of termination of the MSI
vi. Exit Management plan at the minimum adhere to the following:
    a. Three (3) months of the support to Replacement Service Provider post termination of the Contract
    b. Complete handover of the Planning documents, bill of materials, functional requirements specification, technical specifications of all equipment, change requests if any, sources codes, reports, documents, and other relevant items to the Replacement Service Provider/GoUP
    c. Certificate of Acceptance from authorized representative of Replacement Service
    d. Provider issued to the MSI on successful completion of handover and knowledge transfer
vii. In the event of termination or expiry of the contract, Project Implementation, or Service level monitoring, both MSI and GoUP shall comply with the Exit Management Plan.
viii. During the exit management period, the MSI shall use its best efforts to deliver the services.
ix. Provide a recommended Exit Management Plan, which shall include following documents:
    1. Project Organization and Management plan
    2. Software Design and Development plan
    3. Implementation plan
    4. Pre-commissioning, Operational and User Acceptance Testing Plan
    5. Design, Delivery and Installation Plan for Hardware and Network
    6. Training Plan
    7. Support Service Plan
    8. Task, Time, and Resource Schedules (List of tasks, the dependency among the tasks, the duration to perform the tasks, the resources

allocated to perform the tasks, the scheduled start and finish dates for the task)
9. Post-support Service Plan
10. Technical Support Plan
11. Quality Assurance and Control Process details which must include (but not limited to) detailing on Metrics, Reviews, Problem Reporting and Corrective action etc.
12. Technical and Operational Process which must include (but not limited to) detailing on Methods, Tools, Techniques etc.

x. Provide inventory details with Serial Number, Asset tagging for complete hardware and software parts.

xi. Provide steps for Information technology handover both hardware and software this includes license policy, support mechanism and status of hardware.

xii. Provide current technical manpower and their support mechanism in transition stage and as well as under Operation and Maintenance of new MSI.

xiii. Current contact centre manpower supplied till your contract and provide any support thereafter.

xiv. Provide training and capacity building documents including
1. Training Calendar
2. Course Curriculum Modules
3. Training Need Assessment

xv. Provide details of critical issues and challenges that you would like to highlight.

xvi. The exit management plan may be suitably modified by the MSI to cover all the aspects during the transition period and upon acceptance by ITECCS, will be implemented by the next MSI.

xvii. Transfer of Assets: Transfer both IT and non-IT Assets acquired for the UP112 project to the new MSI. The list of assets shall cover those under the purview of current operator as well as its subcontractors

xviii. Testing: The MSI shall ensure that the system being handed over is tested rigorously before being handed over to the new MSI

xix. Close critical issues: The MSI shall close all critical open issues as on date of exit. All other open issues as on date of Exit shall be listed and provided to UP112.

xx. Risks: All the risks during transition stage shall be properly documented by the MSI and mitigation measures be planned along with the new MSI and recorded in the Exit Management Plan so as to ensure smooth transition without any service disruption.

xxi. Transfer of Agreements: Arrange or provide support for Assignment / Transfer of Agreements with all the OEMs / contractors / sub-contractors who are being used by the current operator in the execution of the UP112 project.

xxii. Provision of Information: Provide access to information reasonably required to define the current mode of operation associated with the

provision of services and access and copies of all information / data / documentation, prepared, or maintained, pertaining to UP112, services rendered including but not limited to applications, Business and IT Operations, and other performance data.

xxiii. Access Rights: Provide reasonable rights of access to UP112 Project Location and premises where assets are located. Provide access to new MSI's employees and facilities as reasonably required to understand the methods of delivery of the services employed by the new MSI and to assist appropriate knowledge transfer.

xxiv. Personnel: Provide a list of all employees (with job titles) of the MSI dedicated to providing the services. To the extent that any Transfer Regulation does not apply to any employee of the MSI, the MSI shall not enforce or impose any contractual provision that would prevent any such employee from being hired by ITECCS or new MSI in case an offer of employment or contract for services is made to such employee.

e. Responsibilities of the MSI during the O&M stage of UP112 (Phase 1(b)) shall include the following:

The MSI shall be responsible for end-to-end provision of O&M services including planning, delivery, and execution of services for UP112, as per the requirements stated in UP112 RFP or any subsequent amendments, change orders, etc. To remove any doubt, it is reiterated that, the MSI shall operate the UP112 solution, without any recourse to the TSP. The MSI shall be responsible for taking all necessary steps required, including replacement, enhancement or upgradation of any hardware, software, network, or infrastructure components to efficiently manage the UP112 system, at no additional cost to ITECCS. Some of the key responsibilities of the MSI in this stage will include (but not limited to):

i. Complete end to end management of UP112 application and all its components
ii. Helpdesk support
iii. Handholding support at the client sites (UP112 locations)
iv. Network service and support
v. DC & DR services
vi. Data Transfer from DC to Government Secured Repository (near DR)
vii. Application maintenance and functional support services
viii. Warranty/ AMC support for software / infrastructure
ix. Asset management services
x. Support to 3rd party acceptance testing, audit, and certification
xi. UP112 Portal maintenance
xii. Peak filing support
xiii. Change requests in UP112
xiv. Generation of all reports as per UP112 RFP (from Q2 onwards till acceptance of system stabilization)

4.5.2 Work Stream 2: Implementation of NexGen UP112 (from start of T+4 to end of T+5 month) 4th and 5th Months

During the implementation stage, beginning from start of T+4 month till end of T + 5 month (or the actual date of acceptance of UAT), MSI shall be responsible for design, development, and deployment of the NexGen UP112 system including commissioning of all hardware, software, network, and manpower components. MSI shall be responsible for building the NexGen UP112 system from grounds-up and software / hardware reuse from UP112 shall not be permitted (other than business rules which shall be allowed to be ported from the present system to the new system).

Key considerations to be followed during the system implementation are as under:

a) The MSI needs to ensure that all the existing features, functionalities, capabilities, business rules of UP112 (as on date of migration of the system from UP112 to NexGen UP112) are included in NexGen UP112 by default and there should not be any functionality of UP112 that is left out while developing NexGen UP112, unless explicitly approved by UP112.
b) The design of solution and technology architecture should be done in consultation with UP112. Further, MSI shall ensure creation and updation of all the required design documents required as part of software development at defined intervals.
c) The strategic control and ownership of all the assets will remain with ITECCS, however, MSI shall procure, implement, and operate NexGen UP112 on its behalf and procure all the licenses in the name of ITECCS. Further, MSI shall be required to maintain required insurance for the assets as per provisions given in section 5 clause 5.11
d) Given that there are frequent changes in the acts / rules / policies, MSI shall ensure that system design and architecture is such that the changes to the NexGen UP112 system are implemented within minimum turnaround time.
e) MSI shall ensure thorough and systematic testing including (but not limited to) unit testing, integration testing, functional testing, and user acceptance testing, in line with industry standards and best practices. Proper documentation and signoffs should be obtained for all these tests.
f) Mandatory monthly project progress report shall be submitted by MSI throughout the duration of the contract. This would be discussed in the monthly project review committee meetings, which would be constituted by UP112.

Any changes that are required to be implemented in UP112 to integrate the abovementioned modules with the system shall be in the scope of MSI and need to be implemented in the given timeline itself.

MSI shall ensure that all modules are passed through appropriate quality assurance and audit mechanisms before actual deployment (as per the requirements in section on system acceptance and testing). Post their deployment, the performance of these modules would be measured on UP112 SLAs till T+4 months, post which new SLAs would be applicable.

The details of scope of activities various stages are given in the section below.

a. **Planning stage**

All the MSIs are required to submit a detailed implementation plan for the implementation stage. The plan should cover:

i. Timelines of various stages of implementation
ii. Quality assurance and audit plan and methodology
iii. Resource deployment plan
iv. Infrastructure deployment plan
v. Module wise rollout plan
vi. Capacity building plan
vii. Milestones and associated risks

This plan shall be evaluated at the time of bid evaluation and would be evaluated as per the scoring criteria mentioned in section 3 – "Evaluation of Bid" of the RFP. Further, the plan shall be the basis for measuring the progress of MSI at the time of actual execution, in addition to the requirements mentioned in the RFP.

MSI will create its own module-wise implementation plan and include it as part of the technical proposal. The plan should be robust, modular, and flexible, allow for stepwise implementation than a big bang approach. This plan may be revised by the MSI after gaining better understanding of the UP112 system, during the knowledge transfer stage, subject to the approval of UP112. ITECCS reserves the right to ask the MSI to make any changes to the timelines and phasing of the implementation plan.

b. Requirement Gathering

The MSI is required to carry out an exhaustive requirement gathering exercise with the ITECCS team and the teams designated by ITECCS for understanding the requirements. The MSI is expected to do the following activities (including but not limited to):

i. Study the SRS, user manuals, and any other documents of UP112 to understand all the current functionalities of UP112 system.
ii. Study the requirements of new modules as well as enhancements to existing modules as mentioned in this RFP. These are the basic minimum enhancements which need to be implemented by MSI.
iii. Conduct detailed requirement gathering exercise (both with internal and external stakeholders of UP112) to validate the functional requirements of existing modules and gather any new requirements to be developed as part of NexGen UP112 system. These shall be documented and agreed upon with UP112.
iv. Detailed assessment of the networking requirements and network systems are also to be carried out for NexGen UP112 with respect to the scope of work and all requirements set out in the RFP.
v. MSI shall carry out a detailed assessment of infrastructure, network, hardware requirements for NexGen UP112 and shall validate its BOM designed as part of the technical proposal. Any additional infrastructure

requirements must be provisioned by MSI, to ensure smooth operations of NexGen UP112 system, at no additional cost to UP112.

vi. Given the dynamic nature of UP112, some of the requirements from NexGen UP112 system may undergo changes during the Implementation stage. The MSI will be required to incorporate all such requirements identified up-till 5 months before the system acceptance of NexGen UP112. No extra cost shall be paid for such changes and these need to be incorporated in the overall costing of the project. All major changes post this stage shall be handled through change control process.

vii. Any product found not meeting the Technical/Functional Specification as per RFP during implementation stage shall need to be replaced by MSI with complied product at no additional cost.

c. Development and Integration

The MSI shall be responsible for creating the new application afresh (including existing functionalities and proposed enhancements) and migrating the data available in the existing system to the new application. Development of all the existing functionalities and envisaged enhancements to the system shall be detailed in the form of SRS / design documents. The MSI should adhere to the following guidelines for software development for the application:

i. The solution design shall be based on SOA framework and shall include, but not be limited to, the design of the -
    1. Application architecture
    2. User interface (web portals)
    3. Database structures
    4. Security architecture
    5. Integration architectures
    6. Network architecture

ii. MSI shall submit the solution design documents to ITECCS and get those reviewed by ITECCS (a detailed walk through should be carried out by MSI as part of review before commencing the development of the solution.

iii. MSI shall perform the software development based on the functional, system requirement specifications and designs finalized for the services.

iv. MSI shall be responsible for enabling all the functional, technical, infrastructure and operational requirements as have been envisaged under this RFP.

v. All the existing integrations of UP112 will be implemented by the MSI. Further additional integrations shall be implemented as per the requirements of ITECCS

d. UAT

The following will be the testing practices for NexGen UP112:

i. MSI shall carry out comprehensive testing of the entire application suite prior to the release of NexGen UP112. MSI is responsible for making all necessary arrangements for testing (including unit, functional, integration, system, user acceptance and system acceptance testing) including the preparation of test

data, scripts where necessary and deployment of the same. The test data shall be comprehensive and address all scenarios identified in the test cases. The MSI shall create test reports from testing activities and submit to ITECCS on request and at defined intervals

ii. ITECCS will also engage third party agency for testing the entire solution prior to release. Timelines for the same shall be as defined in the proposal submitted by the MSI and as agreed with UP112.

iii. MSI to perform unit, integration and system testing in its own premises where the development work is being executed. Testing tools for these to be provided by MSI. ITECCS doesn't intend to own these tools

iv. After successful unit testing of all components, the MSI should conduct full-fledged functional testing and integration testing in accordance with the approved Test Plans. Integration testing shall cover both cross-functional integration points, as well as end-to-end processes. The test plans should be provided to ITECCS in advance for approval. In addition to the above, the testing should cover performance testing (including load, scalability, and stress) and security testing.

v. MSI shall also conduct an internal Vulnerability Assessment and Penetration Testing (VAPT) on a periodic basis

vi. The MSI shall ensure coordination with the external agencies/bodies like CERT-In to ensure compliance with Government guidelines

vii. MSI shall conduct the load tests with an objective to determine the response times of various time critical transactions and business processes and ensure that they are within documented SLAs.

viii. MSI shall conduct the stress tests with an objective to determine the system's behaviour when its resources are limited and to check whether the behaviour is well within the defined parameters.

ix. Load, scalability, and stress testing would be finalized by the MSI in the implementation plan conducted prior to submitting the application for User Acceptance Test (UAT) once the system integration testing has been conducted successfully.

x. MSI shall submit internal QA report to ITECCS before moving for UAT. In case there is less than 95% pass rate out of the total set of test cases or there are blockers which need remediation, in that scenario MSI shall not be allowed to proceed to UAT. It would be binding on MSI to remove all blockers and to have a reasonable pass rate (more than 95% at-least) and before being allowed to proceed to UAT.

xi. MSI should use suitable simulation tools in accordance with the agreed test procedures keeping in view UP112's projected future load of transactional users as proposed by MSI and agreed by UP112.

xii. Test Plans for UAT would be prepared / updated by the MSI in collaboration with the UP112. MSI will plan all aspects of UAT (including the preparation of test data) and obtain required assistance from ITECCS to ensure its success. ITECCS would facilitate UAT. MSI would make the necessary changes to the application to ensure that the application successfully goes through UAT.

xiii. Since modular approach to development is proposed, the testing shall also be conducted in modular fashion. For example, there could be several stages of UATs (for each completed functionality)

xiv. At least 4 weeks shall be provisioned for every stage of UAT

xv. Sufficient bandwidth, processing power, storage space shall be made available for UAT to make it effective.

xvi. MSI shall ensure execution of system acceptance testing (post UAT and before go-live) in production environment. MSI shall submit a self-certificate to ITECCS detailing out how all the requirements targeted for the release are met prior to the release to the production.

1. ITECCS will review the details, conduct the necessary tests, and may request any clarifications. MSI shall clarify with additional details to the satisfaction of ITECCS and fix any open items that are discovered during the tests / audits conducted by ITECCS to the satisfaction of UP112. The same has to be approved by UP112.

2. Post release in production environment (in case of application) or deployment at the sites (in case of infrastructure), systems should be running for a continuous period of 2 weeks with no Priority Level – 1 (Critical), or Priority Level – 2 (High) incidents reported on the application and infrastructure. The incidents of business nature (for example, refund yet to be processed by UP112) will not be considered for this criterion. In case any such (priority Level- 1 or priority level – 2) incidents are reported in production, the same will have to be fixed and the fixes should be released into production. System acceptance test will be treated as successful when the application and / or infrastructure is running for a continuous period of 2 weeks with no Priority Level – 1 (Critical), or Priority Level – 2 (high) incidents reported on the application and infrastructure after such release(s).

3. The MSI, in case requested by UP112, should make provision to release the NexGen UP112 to a select set of users / geography before the full launch of the application to all the users / across all geographies. Provisions should also be made to release certain modules of application in advance to certain set of user groups before the entire system is made live. The limited release will be tested in production by the select set of users for a period up to 2 weeks or as decided by ITECCS before the full application launch. ITECCS shall facilitate the selection of user groups for testing which shall include back-office users, or the users registered on the portal.

4. During the system acceptance testing, although the controlled user groups would be allowed to make changes in the production server, those changes would not be considered material for business aspect. For example, even though user would be carrying out the entire process related to company incorporation on production server, the company

would not be considered as incorporated. That would only happen through the live system (which at that time would be the operational v2 system).

xvii. Further any changes to the application suite during the operations and maintenance stage will be released to production only after successful regression testing, including automated testing where necessary, of the application. The regression test plans shall be provided in advance to ITECCS for approval.

xviii. The MSI is expected to lay down a robust Quality Assurance (QA) program for testing of the developed application for its functionalities, performance, and security before porting it to the production environment. The program must include an overall plan for testing and acceptance of system, in which specific methods and steps should be clearly indicated and approved by UP112. The MSI shall share the QA management plan with ITECCS

e. Deployment

It shall be the responsibility of MSI to procure, install, configure, and commission the infrastructure for NexGen UP112 both at client side and server side. MSI shall also be responsible for sizing of necessary hardware and determining the specifications of the same in order to meet the service levels and requirements of UP112.

In the technical proposal, the MSI needs to elaborate on the proposed approach for commissioning, configuration & implementation of the entire system. The requirements for the infrastructure deployment are (but not limited to the following):

i. The MSI shall assess the sizing requirements for various products / tools / software required to fulfil the functional, technical, and operational requirements of the solution.
ii. The ownership of all software developed / customized / configured / procured for NexGen UP112 would lie with UP112. The ownership of any hardware and any other equipment purchased for the project would lie with UP112. All licenses related to these would be in the name of UP112.
iii. The MSI shall provide the hosting services for both the Data Centre and Disaster Recovery Centre. The MSI may either choose to continue in the current hosting facilities or move to a different hosting facility. However, it is clarified that a different infrastructure setup will need to be created for NexGen UP112, and the same infrastructure setup for UP112 cannot be reused.
iv. DC should be located within the Uttar Pradesh Region and the DR in a different seismic zone.
v. Sizing of the hardware should be done to support the scalability and performance requirements of the solution (particularly during the peak filing season) - MSI shall be required to augment the infrastructure without any additional cost to the ITECCS to ensure that the SLAs are maintained even during the peak periods. There should not be any constraints on the services

(for example, limit on sessions, blocking the VPD services) during the Peak Filing Period

vi. MSI should procure and deliver all client-side as well as server-side equipment / devices / infrastructure within first 5 months after T at the identified locations (within ITECCS and other locations). A delivery certificate from the authorized signatory of the MSI would be required in this regard.

vii. All the hardware components shall be commissioned within T + 3 months.

viii. The MSI is responsible for management and maintenance of all the client end hardware installed at ITECCS offices. ITECCS will be responsible for providing basic utilities viz. office area, electricity, water, earthing, sanitation at no cost to the MSI. However, the MSI shall provision for all other requirements such as basic site preparation (if needed, including wiring, LAN cabling, electric fitments, etc.). MSI shall also maintain UPS for uninterrupted power as well as air conditioners in the server room.

ix. There are certain tools / systems that are required from the very beginning of the project (within Knowledge transfer stage). For example, the MSI shall create and update documents which will require 'version management tool' for managing various versions of the document. So, until the DC environment is set up, the MSI shall provision such tools (including document version control tool, project management tool, document management tool, contract management solution, asset management tool, change management monitoring tool etc.) on the MeitY empanelled government cloud and as per solution feasibility.

f. Preparation of technical documents

MSI shall create, update, and maintain all project documents that would be submitted to UP112. Creation of technical documents would begin in parallel to the requirement gathering stage and continue through the implementation and operations stage such as:

1. Project inception report including project plan and test plan
2. SRS document including system design, DB design, application arch etc.
3. FRS document
4. High level design document
5. Low level design document
6. Deployment document in development, QA, and Production environment
7. Deployment checklist
8. Test cases

MSI shall submit a list of deliverables that they would submit based on the methodology they propose. All project documents are to be kept up to date (updated every six months) during the course of the project. ITECCS will review the deliverables submitted by MSI at various intervals and will provide

recommendations and observations to MSI on the deliverables. All the system documentation (including Configuration Documents, Training documentation, User Manuals and Online help) should be validated and made up to date on a 3 monthly basis or as desired by UP112.

MSI shall prepare the following technical documents during the various stages of implementation (including but not limited to):

i. Software Requirement Specification (SRS) as per IEEE Standards including but not limited to the following components:
    1. System description
    2. System interfaces (system, user, software, communication, etc.)
    3. Performance requirements
    4. Logical database requirements
    5. Standards compliance
    6. Software system attributes like reliability, availability, security, maintainability, portability
    7. Prototype including GUI screens
    8. Operational modes
    9. Use cases
    10. Constraints
ii. System design documents (SDD) as per IEEE standards (including but not limited to)
    1. Application architecture documents
    2. ER diagrams and other data modelling documents
    3. Logical and physical database design
    4. Data dictionary and data definitions
    5. Application component design including component deployment views, control flows, etc.
    6. Decomposition description (modules, processes, data)
    7. Detailed design (Module and Data)
    8. Dependency description (Inter-modules, Inter-process, Inter-data)
    9. Interface description (Module and process)
iii. Software Test Report Document which shall contain documentation pertaining to the testing of each module or system as a whole.
    1. Unit and Integration Testing Plan and Procedure
    2. User Acceptance Testing Plan and Procedure
    3. Test cases for all tests
    4. Test input data set, test results
    5. Quality Assurance/ Testing Plan
iv. UAT and completion report
v. Contingency Plan document containing emergency response procedures; backup arrangements, procedures, and responsibilities; and post-disaster recovery plans, procedures, and responsibilities
vi. End-user documents including but not limited to user manuals. The user manuals and documents etc. shall be in English and may need to be

translated to Hindi as per UP112's requirements. It should be maintained and in soft and/or hard copy. Some of the indicative manuals are:

1. Operations Manual providing instructions for installing the application/ software tools, troubleshooting, interpreting message logs, and FAQs (Frequently Asked Questions).
2. Maintenance Manuals
3. Administration Manual
4. Security Manual
5. Applications and Web Portal Training Manual and others (if any) as per acceptable standards
6. Systems Manual detailing the data structure, table, forms, and report structures
7. Trouble Shooting Guide/ Handbook for helpdesk which describes the various trouble shooting methods

vii. Version control management containing the baseline version for all documents, source codes and applications with procedures for making any changes to the baseline version.

viii. Other General Conditions

1. Environments

   The MSI shall provision for the following environments at DC and DR:

   a. Development environment
   b. Testing environment
   c. Staging environment
   d. UAT environment
   e. Production environment
   f. Training environment for hands on training to user groups
   g. Environment on GSR

   These environments should be secluded in a different VLAN than the production environment. Considerations for setting up environments are as under:

2. The training environment will be required for providing training to users accessing ITECCS application.
3. Any version upgrade/changes in the application shall be implemented in all the environments. The application shall be migrated to the production environment only after adequate testing and approval by UP112.
4. A quality assurance test of the changes to be implemented will be performed in a test environment prior to implementation in the production environment.

4.6 Operations and Maintenance (O&M) stage

In this stage, MSI would be responsible of operations and maintenance of the entire solution for the contract period. This will be applicable after UAT approval or system acceptance.

4.6.1 Work Stream 3: O&M Service Requirements (from T+5 to T+65)

The Operations and Maintenance service for NexGen UP112 Project shall be a critical aspect in the Project. The MSI shall be responsible for end-to-end provision of O&M services including planning, delivery, and execution of services. Based on ITECCS's authorization and approval, MSI should interact and coordinate as necessary for the requirement of the UP112 project with external entities as well. MSI shall liaison with all necessary external agencies to accomplish the implementation and maintenance of the project.

MSI shall ensure compliance with the SLAs in place for operations and maintenance. MSI shall also be responsible to keep all the documents updated during the project period.

Details of responsibilities of MSI and general conditions are as under:

a. Applications support and maintenance

Application support includes, but not limited to, production monitoring, troubleshooting, and addressing the functionality, availability, and performance issues. MSI shall keep the application software in good working order and perform upgrades to applications as requested by the ITECCS team. MSI shall be responsible for managing applications through their entire lifecycle, including the design, testing, and improvement of applications that are part of the IT Services. The MSI's responsibilities with respect to ITECCS Application Management function are described as under:

i. Tuning of application, databases, application, and any other components provided as part of the solution to optimize the performance
ii. Perform changes, bug fixes, error resolutions and enhancements that are incidental to proper and complete working of the application.
iii. Any changes to the application code that may be required because of patches to licensed software being used (if any)
iv. Migrate all current functionality to the new / enhanced version, any future upgrades, modifications, or enhancements.
v. Update and maintain all project documents
vi. End user support in case of technical difficulties in use of the software, answering procedural questions, providing recovery and backup information, and any other requirement that may be incidental/ancillary to the complete usage of the application.
vii. User ID and group management services.
viii. Maintain access controls to protect and limit access to the authorized end users of the application
ix. Administrative support for user registration, creating and maintaining user profiles, granting user access and authorization, providing on going user password support, announcing, and providing networking services for users and providing administrative support for directory and e-mail servers.
x. Configuration of new acts/sections, and any other configurable data entities in the system as required by ITECCS
xi. Release Management for the interim releases of the application
xii. Facilitating ongoing integration with other external entities (conditions given in clause 5.35 on change control management shall apply). MSI should also make available to such agencies, all the data and industry-standard

interfaces and integration touch points for integration with the UP112 suite of applications.

xiii. Implementing all patches and upgrades from OEMs ensuring customization done in the solution as per the ITECCS's requirements. Technical upgrade to the new version, as and when required, shall be done by the MSI. Any version upgrade of the software / tool / appliance by MSI to be done after taking prior approval of ITECCS and after submitting impact assessment of such upgrade.

xiv. In case of critical security patches/alerts, the MSI shall inform about the same immediately along with his recommendations. The report shall contain ITECCS's recommendations on update/upgrade, benefits, impact analysis etc. The MSI shall need to execute updates/upgrades though formal change management process and update all documentations and Knowledge databases etc. For updates and upgrades, MSI will carry it out free of cost by following defined process.

xv. Manage all changes on UP112 portal (and any other sub-portal) including uploading of content as and when required by ITECCS.

xvi. Routine functional changes that include generating reports and configuration of reports (conditions given in clause 5.35 on which change control management may apply, where applicable). Some of the indicative changes include:

1. Configuration changes to improve the performance & efficiency of the system
2. Extension of ITECCS services portal to other departments/ministries
3. Changes in application or development of application modules for strategic control & monitoring of system for ITECCS or appointed body like PMU (Program Monitoring / Management Unit)

b. IT Infrastructure Support and Maintenance

IT infrastructure includes but not limited to servers, storages, back up, networking, load balancers, security equipment, operating systems, database, enterprise management system, help desk system and other related IT infra required for running and operating the envisaged system. MSI shall define, develop, implement, and adhere to IT Service Management (ITSM) processes aligned to ITIL framework for all the IT Services defined and managed as part of this project. MSI to propose necessary hardware, software, and network at appropriate places in the bid submission formats and provide cost for the Wi-Fi component in costing formats. IT infrastructure support, which includes maintaining the network for UP112 HQ, OMCs and filed locations. MDT and Smart phone should be replaced with product with same or better specification after due approval from competent authority, if required for the uninterrupted and smooth operation of the project. The maintenance includes but not limited to the below:

c. Warranty and Annual Maintenance Charge (AMC) support requirements for ITECCS infrastructure

i. MSI shall provide AMC support (through OEM) for all the project infrastructure deployed at the various places.

1. Where such a support for any component(s) is not available or ends off support during the contract period, the component(s) shall be replaced

with latest available component(s) in the market with similar or better specifications at least 6 months before the end of support period. No components supplied should be end of life.

2. No component supplied should have been introduced in the market more than 2 years back as on date of the replacement.
3. MSI has to submit the details to ITECCS and ITECCS's decision on the acceptability of the replacement will be binding on the MSI.

ii. For all the client-side infrastructure procured by the MSI, the MSI shall be responsible for:

1. Configuration, installation and complete commissioning of the infrastructure and network
2. Ensuring that the supplied equipment supports the intended system hardware, operating system, and other software. Any problems encountered in the installation of the hardware/software because of hardware/software incompatibility shall be the responsibility of the MSI.
3. Ensure that all the new hardware is connected with the UP112 network so that there is a full communication between the infrastructure at DC & DRC and the field and the users are able to use the infrastructure for the intended purpose.
4. Proper backup is taken of the desktops or any other component before moving to the new environment and migrate all the data on to the new components as required.
5. A plan has to be provided to HQ and field where replacement is envisaged, and replacement shall be carried out only after prior approval by ITECCS.

iii. Provide OEM warranty (minimum 5 years) and comprehensive AMC support (after the expiry of warranty as and when applicable) for the entire contract period. The comprehensive AMC should include provision and replacement of all spares and parts, replacement of consumables, free of cost during the entire period.

d. Warranty and AMC support requirements for DC and DR IT infrastructure

MSI shall be responsible for provisioning AMC for software and hardware components respectively. AMC for all the licensed software and AMC for hardware should be valid through the entire duration of the contract and for a period of at least one year at the time of expiry of MSI's contract. In case any of the hardware is reaching end of life and MSI is not able to procure the AMC services, such hardware shall be replaced with the then current infrastructure to meet the above requirement.

MSI shall provide comprehensive AMC support directly from the OEM for all the infrastructure components. Key considerations under are as under

i. Where such a support for any component(s) is not available or ends during the contract period, the component(s) shall be replaced with latest available component(s) in the market with similar or better specifications at least 3

months before the end of support period or within the first six months of the project.

ii. No components supplied should be end of life.

iii. MSI has to submit the details to ITECCS and ITECCS's decision on the acceptability of the replacement will be binding on the MSI.

iv. In case the infrastructure will be replaced, the existing infrastructure may be repurposed to create the development, test, and training Environments.

v. For the all the infrastructure procured by the ITECCS, the MSI shall be responsible for

1. Configuration, installation and complete commissioning of the infrastructure and network
2. Ensuring that the supplied equipment supports the intended system hardware, operating system, and other software. Any problems encountered in the installation of the hardware/software because of hardware/software incompatibility shall be the responsibility of the MSI.
3. Proper backup is taken before migrating to the new environment and migrate the applications / data to the new environment as required.
4. Provide OEM warranty (minimum 5 years) and comprehensive AMC support (after the expiry of warranty) for the entire contract period. The comprehensive AMC should include provision and replacement of all spares and parts, free of cost during the entire period.

vi. MSI shall provide the performance warranty with respect of performance of the installed hardware and software to meet the performance requirements and service levels in the RFP.

vii. MSI is responsible for sizing and procuring the necessary hardware and software licenses as per the performance requirements provided in the RFP. During the warranty period MSI shall replace or augment or procure higher-level new equipment or additional licenses/hardware at no additional cost to the ITECCS in case the procured hardware or software is not enough or is undersized to meet the service levels and the project requirements.

viii. During the warranty period MSI shall maintain the systems and repair/replace at the installed site at no charge to ITECCS.

ix. In case any hard disk drive of any server, SAN, or client machine is replaced during warranty / AMC, the unserviceable HDD will be property of ITECCS and will not be returned to MSI.

x. The MSI shall carry out Preventive Maintenance (PM), including cleaning of interior and exterior, of all hardware and testing for virus, if any, and should maintain proper records at each site for such PM. Failure to carry out such PM will be a breach of warranty and the warranty period will be extended by the period of delay in PM. The PM should be carried out at least once in six months as per checklist and for components agreed with ITECCS.

xi. The MSI shall carry out Corrective Maintenance for maintenance/troubleshooting of supplied hardware/software and support infrastructure problem including network (active/passive) equipment, security, and rectification of the same. The MSI shall also maintain

complete documentation of problems, isolation, cause, and rectification procedures for building knowledge base for the known problems in centralized repository, accessible to ITECCS team as well.

xii. MSI shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.

xiii. The MSI shall ensure that the warranty complies with the agreed technical standards, security requirements, operating procedures, and recovery procedures.

xiv. MSI shall have to stock and provide adequate onsite and offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met.

xv. MSI shall ensure that the onsite list of spares is assigned only for ITECCS infrastructure and that this list of onsite spares is made available to ITECCS and updated on half yearly basis

xvi. Any component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA).

xvii. The MSI shall introduce a comprehensive assets management process & appropriate tool to manage the entire lifecycle of every component of NexGen UP112 system.

xviii. Further for operations and maintenance of NexGen UP112, MSI shall be required to provide AMC and OEM support.

e. Maintenance of IT Infrastructure at the DC, DR, and OMC

i. Management of DC, DR, and OMC

MSI needs to deploy well trained and experienced resources (on 24X7 basis) for management of entire NexGen UP112 System including IT infrastructure deployed at DC, DR, and OMC. MSI needs to provide shift wise detail of its team deployment at each site along with the category / roles and number of resources, along with their qualifications (separately with MSI and outside), of back up resources planned at each site to handle the work in case of absence of any resource(s). All resources deployed in the project should be employees of MSI. All the resources for the project need to be dedicated for the UP112 project. Any change in the team once deployed will require approval from ITECCS. It is expected that the majority of resources have proven track record and reliability. Considering the criticality of the project, ITECCS may ask for security verification (Police verification) of every resource deployed on the project and MSI needs to comply the same before deployment of the resource at the project. At all times, the MSI needs to maintain the details of resources deployed for the project to ITECCS and keep the same updated. A detailed process in this regard will be finalized between ITECCS and MSI. ITECCS reserves the right to interview resources deployed for Operations and maintenance and assess the suitability of the resource for the role. In case a resource is not found suitable, MSI will change the resource on request of ITECCS. MSI shall comply with this.

The dedicated team for ITECCS shall be based at the DC, HQ, OMC, and field location of UP112. The shared team of senior resources may operate out of ITECCS's remote delivery centres or any other office. The MSI shall provide all such estimations to ITECCS. In case of any travelling requirements of shared senior resources to DC/DR for UP112, the same shall be at MSI's expense. For any remote based support, the MSI has to ensure the same is done over a secured MPLS link. All accesses by any resources should be controlled, managed, and logged. The scope of work for infrastructure and maintenance includes the following:

1. Ensure compliance to relevant SLA's and KPI's
2. 24x7 monitoring & management of availability & security of the infrastructure and assets
3. Perform regular hardening, patch management, testing and installation of software updates issued by OEM / vendors from time to time after following agreed process
4. Ensure overall security – ensure installation and management of every security component at every layer including physical security
5. Prepare documentation / policies required for certifications included in the scope of work
6. Performance tuning of system as required
7. Design and maintain policies and standard operating procedures
8. User access management
9. Other activities as defined/to meet the project objectives
10. Updating of all Documentation.

During operations stage the MSI needs to submit proof of renewal of support for all IT infrastructure products and other system software. This needs to be submitted on an annual basis and needs to be verified before 2nd quarter of each year.

ii. System Maintenance and Management

1. MSI shall be responsible for tasks including but not limited to setting up servers, configuring and apportioning storage space, account management, performing periodic backup of data and automating reporting tasks, and executing hardware and software updates when necessary. It shall be noted that the activities performed by the MSI may also be reviewed by ITECCS.
2. MSI shall provision skilled and experienced manpower resources to administer and manage the entire system at all primary, secondary and near-line DCs.
3. On an ongoing basis, MSI shall be responsible for troubleshooting issues in the IT infrastructure solution to determine the areas where fixes are required and ensuring resolution of the same.
4. MSI shall be responsible for identification, diagnosis and resolution of problem areas pertaining to the IT Infrastructure and maintaining the defined SLA levels.
5. MSI shall implement and maintain standard operating procedures for the maintenance of the IT infrastructure based on the policies formulated in discussion with ITECCS and based on the industry best practices / frameworks. MSI shall also create and maintain adequate documentation / checklists for the same.

6. MSI shall be responsible for managing the usernames, roles, and passwords of all the relevant subsystems, including, but not limited to servers, other devices, etc. MSI shall be required to set up the directory server. Logs relating to access of system by administrators shall also be kept and shall be made available to ITECCS on need basis.
7. MSI shall implement a password change mechanism in accordance with the security policy formulated in discussion with ITECCS and based on the industry best practices/frameworks like ISO 27001, ISO 20000 etc.
8. The administrators shall also be required to have experience in latest technologies so as to provision the existing and applicable infrastructure on a requirement-based scenario.

iii. System Administration

1. 24*7*365 monitoring and management of the servers in the DC / DR and OMC and field equipment.
2. MSI shall also ensure proper configuration of server parameters and performance tuning on regular basis. MSI shall be the single point of accountability for all hardware maintenance and support the ICT infrastructure. It should be noted that the activities performed by the MSI may be reviewed by ITECCS.
3. MSI shall be responsible for operating system administration, including but not limited to management of users, processes, preventive maintenance, and management of upgrades including updates, upgrades, and patches to ensure that the system is properly updated.
4. MSI shall also be responsible for installation and re-installation of the hardware(s) as well as the software(s) in the event of system crash / failures. MSI shall also be responsible for proactive monitoring of the applications hosted.
5. MSI shall appoint system administrators to regularly monitor and maintain a log of the monitoring of servers to ensure their availability to ITECCS at all times.
6. ITECCS shall undertake regular analysis of events and logs generated in all the sub systems including but not limited to servers, operating systems etc. The system administrators shall undertake actions in accordance with the results of the log analysis. The system administrators shall also ensure that the logs are backed up and truncated at regular intervals. MSI shall refer to CERT-In guidelines so as to ensure their alignment with the practices followed.
7. The system administrators shall adopt a defined process for change and configuration management in the areas including, but not limited to, changes in servers, operating system, applying patches, etc.
8. The system administrators shall provide hardening of servers in line with the defined security policies. Validation of hardening configuration will be carried out quarterly and deviations must be tracked through SLA reporting
9. The system administrators shall provide integration and user support on all supported servers, data storage, security & network systems etc.
10. MSI shall be responsible for documentation regarding configuration of all servers, IT Infrastructure etc.
11. MSI shall maintain a standard naming, numbering convention for networking

12. MSI responsible for managing the trouble tickets, diagnosis of the problems, reporting, managing escalation, and ensuring rectification of server problems as prescribed in SLAs
13. The administrators will also be required to have experience in latest technologies to provision the existing and applicable infrastructure on a requirement-based scenario.

iv. Storage Administration

1. MSI shall be responsible for the management of the storage solution including, but not limited to, storage management policy, configuration and management of disk array, switches, backup appliance, etc. It should be noted that the activities performed by the MSI may be reviewed by ITECCS.

v. Database Administration

1. MSI shall be responsible for monitoring database activity and performance, changing the database logical structure to embody the requirements of new and changed programs.
2. MSI shall be responsible to perform physical administrative functions such as reorganizing the database to improve performance.
3. MSI shall be responsible for tuning of the database, ensuring the integrity of the data and configuring the data dictionary.
4. MSI will follow guidelines issued by ITECCS in this regard from time to time including access of data base by system administrators and guidelines relating to security of data base.
5. Database administration should follow the principle of segregation of duties to ensure no single DBA can update production tables/data singularly.
6. In addition to restrictions on any direct change in data by any administrator, the databases shall have auditing features enabled to capture all activities of administrators.

vi. Backup/Restore

1. MSI shall be responsible for implementation of backup policies as finalized with ITECCS. MSI is responsible for getting acquainted with the storage policies of ITECCS before installation and configuration. It should be noted that the activities performed by the MSI may be reviewed by ITECCS.
2. MSI shall be responsible for monitoring and enhancing the performance of scheduled backups, scheduled regular testing of backups, and ensuring adherence to related retention policies.
3. MSI shall be responsible for prompt execution of on-demand backups of volumes and files whenever required by ITECCS or in case of upgrades and configuration changes to the system.
4. MSI shall be responsible for real-time monitoring, log maintenance and reporting of backup status on a regular basis. MSI shall appoint administrators to ensure prompt problem resolution in case of failures in the backup processes.
5. MSI shall undertake media management tasks, including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in

fireproof cabinets (onsite and offsite as per the detailed process finalized by during project implementation stage).

6. MSI shall also provide a 24 x 7 support for file and volume restoration requests at the Data Centre.

vii. Network monitoring

1. MSI shall provide services for management of network environment to maintain performance at optimum levels on a 24 x 7 basis. It should be noted that the activities performed by the MSI may be reviewed by ITECCS.
2. MSI shall be responsible for monitoring and administering the network within the Data Centre/DR etc., up to the integration points with WAN. MSI shall be required to provide network related services for routers, switches, load balancer etc.
3. MSI shall be responsible for creating and modifying VLAN, assignment of ports to appropriate applications and segmentation of traffic.
4. MSI shall also be responsible for break fix maintenance of the LAN cabling within DC/DR etc.

viii. Security Management

1. Regular hardening and patch management of components of the UP112 system as agreed with ITECCS
2. Performing security services on the components that are part of the ITECCS environment as per security policy finalized with ITECCS
3. IT Security Administration – Manage and monitor safety of information/data
4. Reporting security incidents and resolution of the same
5. Proactively monitor, manage, maintain & administer all security devices and update engine, signatures, and patterns as applicable.
6. Managing and monitoring of anti-virus, anti-malware, phishing, and malware for managed resources.
7. Ensuring 100 percent antivirus coverage with patterns not old more than period agreed on any given system
8. Reporting security incidents and co-ordinate resolution
9. Monitoring centralized pattern distribution (live update) and scan for deficiencies
10. Maintaining secure domain policies
11. Secured IPsec / SSL / TLS based virtual private network (VPN) management
12. Performing firewall management and review of policies on at least quarterly basis during first year of O&M and then after at least on half-yearly basis
13. Resolution of calls for security notifications, system alerts, vulnerabilities in hardware/software and alerting ITECCS as appropriate
14. Performing patch management using software distribution tool for all security applications including content management system, antivirus, and VPN
15. Providing root cause analysis for all defined problems including hacking attempts
16. Monthly reporting on security breaches and attempts plus the action taken to thwart the same and providing the same to ITECCS

17. Maintaining documentation of security component details including architecture diagram, policies, and configurations
18. Performing periodic review of security configurations for inconsistencies and redundancies against security policy
19. Performing periodic review of security policy and suggest improvements
20. Reviewing logs daily of significance such as abnormal traffic, unauthorized penetration attempts, any sign of potential vulnerability. Security alerts and responses. Proactive measures in the event a problem is detected
21. Policy management (firewall users, rules, hosts, access controls, daily adaptations)
22. Modifying security policy, routing table and protocols
23. Performing zone management (DMZ)
24. Sensitizing users to security issues through regular updates or alerts – periodic updates/Help ITECCS issuance of mailers in this regard
25. Performing capacity management of security resources to meet business needs
26. Rapidly resolving every incident/problem within mutually agreed timelines
27. Testing and implementation of patches and upgrades
28. Network/device hardening procedure as per security guidelines from ITECCS
29. Implementing and maintaining security rules
30. Performing any other day-to-day administration and support activities

ix. Other Activities

1. MSI shall ensure that it prepares configuration manual for OS, appliances, middleware, all tool, servers/devices and all equipment's and the same needs to be submitted to ITECCS, any changes in the configuration manual need to be approved by ITECCS. Configuration manuals to be updated periodically.
2. MSI shall maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements, and maintenance.
3. If the operating system or additional copies of operating system are required to be installed / reinstalled / un-installed, the same should be done as part of O&M.
4. MSI should carry out any requisite adjustments / changes in the configuration for implementing different versions of application software.

f. Third party Audit Requirements

During the project timespan, it is expected that several audits will be carried out to not only ensure the conformance of the solution provided by MSI to the scope of work as detailed in this RFP but also to ensure that the solution is implemented in the best of ways to meet the requirements of ITECCS. The audits will be carried out by either PMU or a third-party agency (e.g., STQC, OEMs) engaged by ITECCS at various intervals as per the requirements. MSI shall provide support to such audits and comply with the suggestions as may be given by such a third-party auditor. (It is to be noted that the involvement of the third party for acceptance testing and certification, does not absolve MSI of his responsibilities to comply with all the requirements agreed with ITECCS and meet all SLAs as laid out in this RFP.)

MSI would bear the cost for such third-party audits. ITECCS shall notify MSI of any shortcomings from defined requirements at the earliest instance after noticing the same to enable MSI to take corrective measures. All gaps identified shall be addressed by MSI at the earliest.

The audit will cover all domains of the UP112 project to validate the implementation as per requirements given in the RFP. The scope of the audit will depend on the implementation approach adopted by MSI. In addition to the UP112 requirements provided in this RFP, the audit may also cover all the applicable requirements (functional, technical, performance, security, etc.) of the existing systems and whether the new solution, either after upgrade or re-implementation conforms to all such requirements. Further, the scope of the audit may vary from one audit to the next and will primarily be determined by the nature of changes implemented during that period.

The appointed agency for audit shall review all aspects of project development and implementation covering software, hardware, networking operations and including the processes related to the design of solution architecture, design of systems and sub-systems, coding, testing, business process description, documentation, version control, change management, security, service oriented architecture, performance in relation to defined requirements, interoperability, scalability, availability and compliance with all the technical and functional requirements of the RFP and the agreement. The procedures and parameters for testing will be laid down by the third-party agency after approval from ITECCS.

The indicative items that will be covered in the audit are given below:

i. Functional Requirements
ii. Non-Functional Requirements such as Performance, Availability, Security, and Manageability
iii. Comprehensive Testing Requirements
iv. Infrastructure – Underlying Solutions, Client-Side Infrastructure, and DC-DR Infrastructure
v. SLA Management and Reporting
vi. Project Documentation
vii. Policy Audit
viii. Standards and Protocols
ix. DC-DR Hosting Facilities

g. ISO 27001 Audit

ITECCS envisages implementing a certifiable Information Security Management System (ISMS) as per ISO 27001 Standards. The MSI shall be responsible for implementing the security controls for the UP112 Project and ensure that the certification is obtained. ITECCS shall appoint a certification body for the certification and inform MSI well in advance about the dates of certification.

i. Audit Scope: The scope covers all the components (Software, Hardware, and others) of UP112 Project which does storage, retrieval, transmission,

distribution, and exchange of data which is submitted/written by ITECCS or end users of ITECCS's Application.

ii. The Geographical Scope for Certification is DC and DR
iii. Responsibility of MSI will include (but not limited to):
iv. Develop and Implement comprehensive risk-based program based on ISO27001 Framework.
v. Ensure all Documentation of the Information Security Management System are available as per the latest ISO 27001 standard
vi. Study Existing Systems and processes for information security management and identification of gaps vis-à-vis ISMS Clause Requirements
vii. Define and Implement ISMS as per ISO 27001 Standards.
viii. Provide Training to all required stakeholders on ISO 27001 Standard.
ix. Assist ITECCS in identification of Internal Auditors1* and training of Internal auditor for ISO 27001 Certification
x. Take corrective action against non-conformities/observations raised by Certification agency during certification audit and are closed in time.
xi. Assist the ITECCS in collating all requirements to apply for ISO 27001 Certification
xii. Ensure that ISMS system in UP112 Project is certified for ISO 27001 Certification.
xiii. Assist ITECCS with all artefacts which is required during the audit.
xiv. The MSI shall employ a robust and proven framework for ISMS implementation to ensure successful completion of the project and leading to ISO 27001 (ISMS) certification.
xv. MSI shall be responsible for end-to-end ISO 27001 implementation and certification.

h. Adherence to ISO 22301

The main objective of the MSI is to evaluate and further develop the existing framework to include cybersecurity threats in the context of Business Continuity whilst aligning the same to meet the requirements of ISO 22301.

The MSI must build on and enhance existing practices, assist with improving the effectiveness, efficiency of the methodologies and the relevant supporting documentations of different processes. The MSI is also expected to enhance the capacity of ITECCS staff to implement the Framework through training sessions.

The MSI is expected to conduct an evaluation of in scope IT infrastructure of ITECCS as per ISO22301 standard for assessment of business continuity framework including but not limited to:

i. BCM Governance
ii. BCM Strategies
iii. Business Impact Analysis Process
iv. Risk Assessment Process

v. Emergency Response
vi. Crisis Management Plan
vii. Information Technology Service Continuity
viii. Disaster Recovery Plans
ix. Testing of Recovery Plans Guidelines and Procedures
x. Cyber Security Recovery
xi. Available skills and expertise

i. Operational Audit

In addition to the audits for validating the implementation, ITECCS, through an appointed agency, shall conduct periodical operational audits to ensure compliance / conformance of the IT Operations processes (ex, Demand Management, Service Level Management, Change Management, Release Management) with the requirements provided in the RFP.

The frequency of operational audit could be half-yearly or annual which shall be decided later by ITECCS.

j. Tools for monitoring operations stage

MSI shall ensure that ITECCS or its nominated agency should have the access to the following solutions / tools to track the operations of the project:

i. Service desk solution covering change management, configuration management, asset management, event management, incident management, and problem management processes.
ii. EMS Solution: MSI will be complete responsible to provide system generated report of all the SLA Parameters via EMS Tool.
iii. Version control tool for version management (this shall be made available from T time since all documents created by the MSI need to be version controlled)

k. Others

MSI to ensure

i. Training of deployed manpower
ii. Integration with agencies mentioned in “Scope of Work” clause 4.27.10
iii. Wi-Fi in ITECCS: A robust wireless data network shall be made available in ITECCS, Lucknow for Internet facility for staff at indoor premises. This network will be based on Wireless protocols and will be maintained by MSI. Employees will be working toward enhance wireless coverage in training rooms, board rooms, cabins, common hall, parking space, corridor etc. throughout the campus.
iv. MSI will ensure that all mobiles, laptops, and PCs can access Wi-Fi and propose solution should comply with current industry standard and benchmarking.
v. Taking regular data back-ups and perform DC-DR drill as decided by department
vi. Mock drills and plan updates shall be carried out once or twice in a year and report submitted to the GoUP as per GoUP policy.

vii. Provisioning and replacement of consumables such as Printer Cartages, etc.

4.7 Project Documentation

The MSI shall create and maintain all project documents that are part of deliverables as per the agreed project timelines. The documents created by the MSI will be reviewed and approved by the Governance Structure Setup of the project.

ITECCS would also approve, if deemed necessary and appropriate, any changes required to these documents during the project. The department will finally sign-off on the documents on the recommendation PMUs, governance committees etc.

Project documents include but are not limited to the following:

i. Project Initiation Report
ii. Detailed Project Plan
iii. Risk Plan
iv. Updated/vetted FRS
v. SRS document
vi. HLD documents (including but not limited to)
    - Application architecture documents
    - ER diagrams and other data modelling documents
    - Logical and physical database design
    - Data dictionary and data definitions
    - Application component design including component deployment views, control flows, etc.
vii. LLD documents (including but not limited to)
    - Application flows and logic including pseudo code
    - GUI design (screen design, navigation, etc.)
viii. Requirements Traceability Matrix
    - Detailed Training Plan with Scoring System.
    - SLA and Performance Monitoring Plan
ix. Server-Side detailed hardware specifications and design documents
x. Network Design documents
xi. Hardware Configuration documents
xii. Security configuration documents
xiii. Version Control Mechanism Document
xiv. Operational Manuals and Security Manuals
xv. System and Operational procedures & Policies
xvi. Staffing Hiring and Recruitment Manuals and Policies
xvii. Training and Knowledge Transfer Plans
xviii. Roll Out plan and Completion Report
xix. Contingency Plan and DR plan, policies, and procedures.
xx. Operations Manuals
xxi. Administration Manual
xxii. Physical and IT security Manuals

xxiii. Application Manuals
xxiv. System manuals with details data structures
xxv. Installation and maintenance manuals
xxvi. Exit Management Plan, policies, Procedures, and processes

All project documentation shall conform to the highest standards of software engineering documentation.

Also, any technical document requested by department shall be submitted within 15 days from the date of request.

4.8 System Study and Design

In terms of functionality, the software applications would cover those all functions that are necessary to the goals of the ITECCS. This includes core functions in the areas of voice solution, dispatch management, GIS and LBS Service, Patrol Management, case management, dispatch efficiency and Analysis & Reporting. Therefore, all the applications supplied through this project must be customizable as per the needs of the project and the selected MSI shall assess the requirements through system study and propose the changes to the department and the necessary software changes be incorporated by the selected MSI within the time period of project implementation. The selected MSI, in its proposal shall specify the systematic plan for requirement gathering, customization, testing of COTS features and Customized features with a detailed testing plan.

Architecture Requirements

For the additional functionality required for the Project, the selected MSI shall carry out a detailed systems study to refine the Functional Requirements Specifications & formulate the System and software Requirements Specifications (FRS & SRS) incorporating the functional specifications and standards provided by the department and the project specific requirements. The SRS preparation shall take into account the BPR recommendations suggested by the department.

Note: The MSI is required to update the FRS/ SRS as and when any enhancements/modifications are made to application till the completion of project.

4.9 Software development, customization, rollout of Applications

4.9.1 MSI needs to setup the Development and Testing, and Production environments, which should be separate at the DC-DRC. Establish the required secure connectivity of its development centres with the DC-DRC and carry out the development and testing exercise from its development centres. Staging and Production environment will be deployed at both DC-DRC separately

4.9.2 MSI shall be responsible for installation and roll-out of all the solution components at all the identified project locations

4.9.3 MSI shall ensure that the COTS solution, if any selected are such that they are configured or customized with minimal modifications to the source code.

4.9.4 MSI shall implement quality standards like CMMi for the entire life cycle of the project. The quality process shall include adequate processes for coding, change management, defect tracking, testing, review as per the Software Development Life Cycle processes that shall ensure a high-quality system.

4.9.5 The following sections describe the development activities based on traditional development methodology to be performed by the MSI.

4.9.6 Software Requirement Analysis and Specification: Software Requirement Analysis and specification is a key stage in the project and recognizing its pivotal role in the subsequent stages, sufficient time will be provided to the MSI to capture the requirements from all the project stakeholders accurately.

4.9.7 MSI shall understand the processes related to Emergency Response Systems and other related documents and seek clarifications from the department, if any. MSI shall then hand over these documents to the department.

4.9.8 MSI shall interact with the stakeholders such as department, Internet Service Providers (ISP's) and other associated agencies etc. as well as the department project team to gather requirements. It is expected that MSI gathers requirements through structured questionnaires, focused discussions with different stakeholders. If found necessary to modify the designed processes and other documents for successful implementation, the same shall be discussed and the relevant documents shall be modified as and when required during the solution implementation

4.9.9 After the requirements analysis, MSI shall prepare all type of technical documentation like software requirement specification (SRS), FRS, design documents etc. SRS shall contain the objectives and scope of the overall Emergency Response (ER) system, the various levels of requirements, the process model, data model, data dictionary etc. User Role wise mapping to the various business functions with details regarding their access rights (insert or update or delete or view etc.) shall also be included in this document. Acceptance Criteria shall also be included explicitly promoting clear understanding with the department about what it considers acceptable.

4.9.10 The SRS document shall be reviewed and approved by the department

4.10 Software Design specifications

4.10.1 In this stage, MSI shall develop a logical view of the Emergency Response solution to meet the department and other stakeholder requirements. This logical view shall consist of the functional architecture of the application and the new database design.

4.10.2 MSI shall also define standards for coding, documentation; user interfaces etc., if the same is not already defined.

4.10.3 MSI shall document the high-level design as System Design Document (SDD) consisting of project standards, the functional design, and the database design. The SDD document shall be reviewed and approved by the department.

4.11 Build Stage – Coding and Unit Testing

4.11.1 MSI shall carryout detailed design (Low Level Design, High Level Design), Coding and Unit testing and document should be approved by the MSI architect. And all release plans should be approved by department. Department may opt to get third party agency for SPQC testing.

4.11.2 For any subsequent changes, enhancements to the applications or fixes made to any bugs or defects in the applications, it shall be MSI's responsibility to perform comprehensive regression testing on the system to ensure that the existing applications work as expected even with the new changes. It shall be MSI's responsibility to create the Regression Testing Plan and Test Scripts with all possible scenarios. MSI may use an automated testing tool for quicker execution of Regression Test cases if it so desires

4.12 Roll out

4.12.1 MSI, in coordination with the department, shall set up the production environment at the Data Centre and Disaster recovery, install all the applications in the production environment, create application databases, application user profiles, load the legacy data etc.

4.12.2 MSI shall coordinate with the department to resolve any problems encountered during or after rollout. All post implementation issues shall be documented, and the necessary fixes or resolutions shall be implemented by the MSI.

4.12.3 MSI shall ensure that necessary support is provided to resolve defects. MSI shall document the defects or bugs encountered during this stage as well as document the resolution of the same. MSI shall also prepare and maintain a database of Consolidated List of Common Errors and their Resolution.

4.12.4 The MSI should transfer all the software development documents like Software Requirement Specifications, design document, licenses etc., configuration of both hardware, software including Operation System, custom built software or executables or application and the customized components of COTS applications or systems, implemented during execution of this project, to the department at the time of acceptance procedures of various stages of the project. In the case of custom-built software or customized components of COTS applications the SI should transfer the customized component source code to the Department to ensure that the Department may independently undertake any changes to the system at a later stage.

4.12.5 The MSI should update the development environment in synchronization with the production environment at the DC sites at the time of acceptance of various stages of the project. This is important to ensure the concurrency of data across all the environments.

4.12.6 The MSI should ensure that all solutions are sized adequately to meet the acceptance criteria. In case additional servers, equipment, components, sub-components, licenses etc. are required to meet the acceptance criteria, the same will have to be provisioned by the MSI at no additional cost to the department and without any project delays. MSI to specify the required quantity of hardware, non-IT equipment, software in the bid document clearly. No additional cost shall be borne by the department towards the proposed solution. However, in case there is any change request from the department side beyond the scope of work, the same shall be compensated by the department through its process and change control Management system of this RFP document.

4.13 Performance Testing

4.13.1 The MSI shall carry out the performance test run of the complete system after satisfactory installation or implementation.

4.13.2 Installation, Commissioning and Rollout of servers and all IT hardware

4.13.3 The MSI is expected to undertake the following tasks with respect to roll-out of hardware:

4.13.4 Planning and Scheduling for Installation and commissioning of hardware and equipment at all the locations including Data Centre and Disaster Recovery Centre sites, PRVs etc.

4.13.5 Pre-installation planning at all the locations including OMC, PRVs, Data Centre, Disaster Recovery but not limited to space planning, structured cabling, power points, check on utility services, environmental conditions, etc.

4.13.6 Delivery, Installation and commissioning of the hardware servers and related equipment in the DC shall be carried out by MSI.

4.13.7 The plan and layout design for the placement of equipment in the provisioned data centres is required to be carried out by MSI. MSI shall provide an elevation plan for each of the DC for housing of the servers and other equipment.

4.13.8 The plan and layout design for DC shall be developed in a manner so as to optimal and efficient use the resources and facilities available or being provisioned at data centre and disaster recovery centre viz. space, racks, server, power, air conditioning, cabling, etc.

4.14 The plan and design documents thus developed shall be submitted to the department for approval and the acceptance shall be obtained prior to commencement of installation. MSI shall carry out installation of equipment in accordance with plans and layout design as approved by the department.**MDT, Radio Sets, GPS device and Mobile phones Distribution, Installation, Configuration in the PRV:**

4.14.1 The MSI shall be responsible for distribution of devices such as MDT, Radio Sets, GPS device and Mobile phones along with associated accessories such as MDT Cradle, wiring etc. at the offices of the respective Police departments. MSI has to visit to the district level to place the devices in vehicles. If due to any operational constraints, some police vehicles are not able to join the installation drive at the office on the given date(s), the MSI shall hand over the devices to a person-in-charge or as approved by the department at the time of delivery. The department identified personnel shall then be responsible for installation and configuration of the devices in vehicles at the respective police stations.

4.14.2 MSI shall be responsible for installation and configuration of the software including, but not limited to, Operating System (OS), System software, etc. on the servers. MSI shall also tune parameters for optimal performance of the OS.

4.14.3 MSI shall undertake necessary changes to harden the OS to prevent against malicious and unwarranted attacks.

4.14.4 The tuning of appropriate parameters in the application, database etc. software to ensure optimal performance shall also be undertaken.

4.14.5 MSI shall undertake Installation and configuration of clustering software wherever provisioned.

4.14.6 Configuration or re-configurations or tuning of all the installed equipment and software

4.14.7 Integration and testing of installed systems or subsystems or equipment or Software

4.14.8 MSI shall facilitate solution acceptance testing and certification by coordinating and providing complete support to the nominated agency for acceptance testing and 3rd party audit certification

4.14.9 MSI shall provide support for testing of changes or updates or patches in the testing environment before applying them on production environment as explained in the following section.

4.15 Development and Test Environment

4.15.1 It would be required to deploy a separate set of servers for Development environment where all the new services will be developed and deployed before it is brought on to the production servers. There shall be provision of the hardware for separate Development and Test System for each software application so that production system shall not get affected in case of application of patches, versions change etc. The development and testing server shall make provision for all different system software platform used along with all required compilers and libraries. It shall have all application software and utilities along with the provision to customize and test the applications. It shall also have provision for version control and version management. Test and Development set up shall be the exact miniature replication of production environment.

4.15.2 Staging environment or Testing Environment: A staging environment or QA environment will be having everything as closely replicated to the production environment as possible to maximize the chances of finding any bugs before any release of the software in production. Even the hardware that is used for the staging environment is often the same as the hardware used in the production environment.

4.16 Production Environment

4.16.1 In Production environment, software and other products are actually put into operation for their intended uses by end users. MSI needs to make sure the following activities in production environment.

4.16.2 Plan releases as per the requirements for the approved changes

4.16.3 Build release packages for the deployment for approved changes into production

4.16.4 Test and implement procedures (mechanisms) for the distribution of approved changes to production environment

4.16.5 Effectively communicate and manage expectations of the customer or internal stakeholders or end customer during the planning and rollout of new releases

4.16.6 Monitor, Control, and Report the distribution and installation of changes to all concerned stakeholders

4.16.7 Deploy the release as per release guidelines

4.17 Release management

4.17.1 Release management procedure shall be defined in conjunction with the department to ensure smooth transition of the application changes from release environment to production environment.

4.17.2 As part of the release management, MSI shall perform the following activities:

4.17.3 MSI shall group the related change requests, assess their development progress, and accordingly prepare a schedule for their release

4.17.4 MSI shall in consultation with the department prepare a detailed release plan for every release. This plan shall include the release number and date of release. It shall also contain details about the change request to be released.

4.17.5 Maintenance of post implementation support environment

4.17.6 MSI should provide an environment with the necessary application and database licenses, development and run-time licenses for solutions proposed, etc. to support post implementation activities such as debugging of problems reported, enhancements or developments, subsequent user acceptance, etc.

4.17.7 MSI would be responsible for ensuring appropriate OS, Database versions and patches are installed on the respective servers in this environment.

4.18 Acceptance Criteria

4.18.1 General

a. The MSI should develop user acceptance test cases in line with the minimum acceptance criteria mentioned under 4.18.2 of this section with the assistance from the GoUP.
b. The GoUP may have the acceptance test done by its representatives, prospective system users, Testing Committee of the officials from GoUP, Telecom service provider's, ISP's, or consultants or any third party at any time at its own convenience. The MSI would be required to cooperate with such representatives or third party and provide the required support for this activity
c. The acceptance test shall involve successful supply, delivery, installation and commissioning of all hardware and related software in the DC and DRC sites, Monitoring Centre, Police Vehicles, UP POLICE 112, OMC and other sites.
d. All the required hardware and software must be installed and working properly. The MSI can be asked to demonstrate all the features or facilities mentioned in the bid and technical requirement laid in various section of the RFP.
e. During this period, the installed systems must demonstrate its capability of providing the services enumerated in the contract, RFP document and claimed by the MSI in its bid and specified in the catalogues attached with the respective bid. The MSI will arrange the test equipment, if required for performance verification. Successful MSI will also provide documented test results.

f. On the successful completion of the acceptance test and after the GoUP is satisfied with the working of the entire system at DC and DRC sites, Monitoring Centre. The date on which such certificate is issued shall be deemed date of the successful commissioning of the system for the purpose of starting the warranty and project management period.
g. The MSI will prepare test strategy, traceability matrix, detailed Acceptance Testing Plan (ATP) including test parameters, test cases etc. for each of the site components including hardware and software as per the RFP. The test parameters, commitments etc. as decided and approved by the GoUP shall be final and binding on the MSI.
h. If the quality and the quantity of the items supplied by the vendor are found unacceptable, the successful MSI shall be held responsible for covering up the loss in terms of both quantity as well as quality wise. All the related payments to the successful MSI as per the payment schedule mentioned in the RFP would be made after the successful clearance of the following acceptance tests.
i. All the functionality, features, and configuration relevant to this project shall be documented and demonstrated by the successful MSI to the GoUP.
j. The entire solution will be monitored under production use for a pre-defined period of time for satisfactory performance of the solutions.
k. In case of any performance issues during this period, the MSI should resolve the issues identified on a priority basis.

4.18.2 Criteria for Acceptance

S. No.	Minimum Component	Minimum Acceptance Criteria
DC		
1.	Hardware (like servers, storage)	• Delivery acceptance on completion of installation, connectivity and POST including test run of offered specifications. • Installation and Commissioning Acceptance: On successful integration in the system and Go-Live. • Item should be captured by EMS
2.	Servers	• Delivery acceptance on completion of installation, connectivity and POST including test run of offered specifications. • Installation and Commissioning Acceptance: On successful integration in the system and Go-Live. • Item should be captured by EMS • Demonstrate Hardware RAID functionality by simulating internal disk failure. • Demonstrate High Availability.

S. No.	Minimum Component	Minimum Acceptance Criteria
		• Demonstrate Ethernet connectivity in dual homing configuration. • Demonstrate Fiber Channel Host Bus Adaptors (HBA) in redundant mode (applicable for servers that are connected to SAN). • Demonstrate redundancy and Hot-swap of power supplies. • Verify that none of the servers are populated with any writeable media except Server for Backup.
3.	Backup Solution	• Delivery acceptance on completion of installation, connectivity and POST including test run of offered specifications. • Installation and Commissioning Acceptance: On successful integration in the system and Go-Live. • Item should be captured by EMS • Demonstrate capability to take backup of servers that are not connected to SAN. • Demonstrate backup or restore of SAN data. • Demonstrate backup or restore of data from internal hard disks of servers. • Demonstrate the backup software functionality for configuring automated backups. • Demonstrate capability to read and write to multiple tape and servers.
4.	EMS	• Validation of all specified technical specifications of the EMS. • Demonstrate functioning of all the relevant components of EMS solution for respective phases
5.	Network switching	• Delivery acceptance on completion of installation, connectivity and POST including test run of offered specifications. • Installation and Commissioning Acceptance: On successful integration in the system and Go-Live. • Item should be captured by EMS • Demonstrate the network switching from DC to DRC and access of applications or solutions at the DC and DRC from Monitoring Centre. The network switching should be transparent to end user without the need for any manual changes at the sites.

S. No.	Minimum Component	Minimum Acceptance Criteria
6.	Replication	• Demonstrate Sync Replication of SAN data from DC to DRC and vice-versa ensuring its consistency.
7.	Integrated testing	• Seamless integration of all Hardware components. • Seamless integration of Network components. • Completion of all passive installations. • Deployment of all applications • Seamless co-working of all HW, SW and installed applications. • Delivery of all functional requirements • Comprehensive integrated testing of all the solutions to re-validate the Phase-wise acceptance criteria.
8.	Acceptance of DC and DRC sites	• Hardware, applications, and other components delivered, installed, and configured as per agreement with the GoUP • All components as described above are tested and accepted • Sites are connected with primary and secondary network • Installation of all applications (as agreed during project implementation) • Applications can be accessed from both the DC and DRC sites • Training is completed for all DC and DRC personnel
Monitoring Centre		
9.	Presentation Layer	• Demonstrate the accessing and serving of emergency response applications • Demonstrate test cases as prepared by MSI
10.	Information Security Solution	• Conduct a comprehensive penetration testing covering all the solutions implemented. A penetration testing report should be submitted to GoUP. • Conduct a threat and vulnerability assessment with a view to demonstrate that GoUP infrastructure is adequately secured against internal and external attacks. The assessment report should be submitted by MSI • In addition, following policy documents would be completed: • Network policy

S. No.	Minimum Component	Minimum Acceptance Criteria
		• Service access policy • Firewall design policy • Authentication policy • Test cases minimally for verification of security against following attacks would be run successfully: • Ping Sweep • Port Scan • Email reconnaissance • SYN flooding or DoS • Application specific DoS attack • IP Spoofing • Packet sniffing • DNS transfer • Trojan horse, back doors, and spy ware • Close mutually agreed issues observed during Security Audit.
11.	Acceptance of Monitoring Centre	• Hardware, applications, and other components delivered, installed, and configured as per agreement with the GoUP • All components as described above are tested and accepted • Hardware components can be tracked through EMS • All phones connected and working • Monitoring centre area in UP POLICE 112 is connected with both DC and DRC sites • Applications can be accessed from Monitoring Centre • Training is completed for all Operations centre personnel
UP POLICE 112 and OMC		
12.	Hardware (like desktop, IP phones)	• Delivery acceptance on completion of installation, connectivity and POST including test run of offered specifications. • Installation and Commissioning Acceptance: On successful integration in the system and Go-Live. • Item should be captured by EMS • Testing of hardware functioning by UP POLICE 112 and OMC supervisor
13.	Presentation Layer	• Demonstrate the accessing and serving of emergency response applications

S. No.	Minimum Component	Minimum Acceptance Criteria
		• Demonstrate test cases as prepared by MSI
14.	Acceptance of UP POLICE 112 and OMC	• Hardware, applications, and other components delivered, installed, and configured as per agreement with the GoUP • Installation and working of IP phones • Connected with DC and DRC sites with primary and secondary network • Installation and working of video wall • Installation and working of LED TV • Installation and working of other hardware like printers, scanner • Installation and working of Biometric solution • Installation and working of surveillance system and access control • Applications can be accessed from UP POLICE 112 and OMC • Test cases can be run from the UP POLICE 112 and OMC • GIS map shows the position of all installed MDTs • Wireless communication of all installed Radio device • Establishment and acceptance of training room as per specification • Training is completed for all UP POLICE 112 and OMC personnel
Other sites and field Location		
15.	Other sites connectivity	• Hardware, applications, and other components delivered, installed, and configured as per agreement with the GoUP • Hardware components can be tracked through EMS • Network connectivity at other sites like DHQ, range officers
16.	Acceptance of MDT	• MDT should be listed in EMS • Tracking of MDT from UP POLICE 112 and OMC • Successful test case of sending messages to MDT and closing case through MDT
17.	Acceptance of Radio Devices	• Radio devices should be listed in EMS • Tracking of Radio devices from UP112, OMC and another site location

S. No.	Minimum Component	Minimum Acceptance Criteria
		• Successful test case of Wireless communication to Radio devices

4.18.3 GIS Map Geo-Fencing

a. Acceptance criteria for pilot:
Pilot system shall be able to identify location for each type of subscriber (Fixed Line, Mobile) for each type of operator available in the area for Pilot deployment. It should also be able to identify location of domestic roaming and international roaming. This would be applicable for identified cities for pilot.

4.18.4 Resource Profiles

a. Telephony and ACD expert (from OEM)

i. (S)He shall closely work with the solution architects for designing the entire Telephony and ACD system that shall act as the key constituent of the Contact Centre systems
ii. (S)He shall be responsible for configuration, installation and customization of the OEM supplied applications and shall closely work with the administrators and the GoUP for ensuring the acceptance of the same based on the **acceptance criteria** as defined by the GoUP
iii. (S)He should be familiar with the components of a centralized contact centre's infrastructure e.g., Trunk lines, PBX solution etc. and should be able to complement the efforts of Solution Architects and experts from Network and Security Point of View

4.18.5 Software development, customization, rollout of applications

a. After the requirements analysis, MSI shall prepare all type of technical documentation like software requirement specification (SRS), FRS, design documents etc. SRS shall contain the objectives and scope of the overall Emergency Response (ER) system, the various levels of requirements, the process model, data model, data dictionary etc. User Role wise mapping to the various business functions with details regarding their access rights (insert or update or delete or view etc.) shall also be included in this document. Acceptance Criteria shall also be included explicitly promoting clear understanding with the GoUP about what it considers acceptable.

4.19 AMC Administration

4.19.1 The MSI should ensure availability of AMC support with all the OEMs for proposed software and hardware components. This AMC support period should commence from the date of initiation of O&M stage that is from the date of system acceptance till the end of contract.

4.19.2 MSI should track the Annual Maintenance Contracts for all the IT assets at the locations identified for the project: Data centre and Disaster Recovery Centre, NOC-SOC official locations and initiate procedure for renewal of the same at appropriate points in time.

4.20 IT infrastructure management

The MSI shall provide complete support for the entire IT infrastructure of the system including all the items supplied or procured and installed as part of the contract, for the contract period.

4.21 Database administration

4.21.1 Management of database environment to maintain performance of each database at optimum levels

4.21.2 End-to-end management of the databases on an ongoing basis to ensure smooth functioning of the same

4.21.3 Tasks including, but not limited to managing changes to database schema, disk space, storage, user roles.

4.21.4 Conduct code and configuration reviews to provide inputs to the department in order to improve the performance or resolve bottlenecks if any.

4.21.5 Performance monitoring and tuning of the databases on a regular basis including, preventive maintenance of the database as required.

4.21.6 Back up of data. Report backup status on a regular basis.

4.21.7 Manage database patch update as and when required with minimal downtime.

4.21.8 MSI shall co-ordinate with Datacentre operators or engineers for back-up activities.

4.21.9 Use of DBA tools to perform database creation, maintenance, and database monitoring related tasks.

4.21.10 Management of storage environment to maintain performance at optimum levels.

4.21.11 Management of the storage solution including, but not limited to, storage management policy, configuration and management of disk array, SAN, Virtual tape library, etc.

4.21.12 Storage management, including but not limited to management of space, volume, RAID configuration, LUN, zone, security, business continuity volumes, performance, etc.

4.22 Software Change Management

4.22.1 MSI shall be responsible for managing the changes that happen to the DC and DRC sites setup on an ongoing basis, including but not limited to, changes in hard or soft configurations, changes to system software, changes to policies, applying of updates or patches, etc.

4.22.2 MSI shall undertake planning required for changes, draw up a task list, decide on responsibilities, co-ordinate with the department users, establish and maintain communication with the department to identify and mitigate risks, manage the schedule, execute the change, ensure, and manage the port change tests and documentation.

4.23 SLA Reports

4.23.1 All type of reporting should be submitted periodically as per SLA measurement interval to the department. The following are the minimum SLA reports of the different components. Detail of each component is defined in the sections 6 “Service Level Agreement” of this RFP Document.

4.23.2 There should be a provision to generate the other reports based on the department requirement on later stages of the project

- Data centre and Disaster Recovery sites related performance levels reports
- Network related performance levels report
- Manpower related performance (technical) level report
- Audit related performance level report
- Issue resolution report
- Other performance level report

4.24 TCO management

4.24.1 Continuous improvement to Emergency Response Technology Solution costs and management of the Total Cost of Ownership (“TCO”) will be one of the key responsibilities of the MSI. This section outlines key objectives of cost optimization and TCO management and the MSI’s scope of work and deliverables associated with this.

4.24.2 MSI is required to optimize cost in all areas of MSI’s work through various measures that could include automation, deployment of tools and optimizations in management of services.

4.24.3 The key areas of focus expected from the MSI in this regard are the following:

4.24.4 Continuous measurable reduction in overall cost of providing Emergency

4.24.5 Response services to Personal in distress

4.24.6 Optimizations in DC and DRC operations including optimization of:

- Manpower required to manage the DC and DRC
- Overall power requirements of the DC and DRC
- Power Utilization Efficiency (“PUE”)
- Overall DC and DRC space requirement
- IT Hardware at the DC and DRC sites

4.24.7 The department expects a decline in the Total Cost of Ownership of the Emergency Response Technology Solution over the contractual period. The TCO reduction benefits would be deployed for the purposes of bringing in more efficiency in the way the Emergency Response solution functions.

4.24.8 This section outlines some of the key components where the department is expecting the MSI to carry out cost optimization. The MSI is expected to identify similar components during the course of the assignment for optimization.

4.24.9 Optimization of DC operations: MSI shall perform the following tasks as part of optimization of DC operations:

- Once the DC is fully operational, MSI shall undertake a study to assess the current overall power, manpower, IT hardware and space requirements of the data centre.
- Study and improvement of PUE: The MSI shall undertake a detailed study of the Current PUE factor of the data centre and based on study of local conditions in India, identify the feasible PUE factor for Indian conditions. Benchmarking with leading industry standards should also be carried out as part of this assessment.
- MSI shall co-ordinate with the GoUP and stakeholders for the complete setup of Data Centre sites before commencement of installation of other areas as mentioned in Section 4: of the RFP document. The bidder shall also co-ordinate regarding Network or Bandwidth connectivity in order to prepare the installation plan and detailed design or architectural design documents.
- As per TRAI guidelines, resale of bandwidth connectivity is not allowed. In such a case tripartite agreement should be formed between GoUP, selected Bidder and Internet Service Provider (s).
- The plan and design documents thus developed shall be submitted by the Bidder for
  approval by the GoUP.
- After obtaining the approval from the GoUP, the Bidder shall commence the installation.

4.25 Technology Refresh

Considering the long-term nature of Emergency Response system's operations and with technology changes leading to introduction of new Emergency Response solutions, service models, advanced IT Infrastructure etc. and the critical nature that DC play in successful operations of the system, the MSI shall have an opportunity for improving the performance and efficiencies of the operations of DC sites of the proposed Emergency Response system.

Technology Refresh scope

The MSI shall be responsible for the following activities as part of technology refresh:

4.25.1 Track key technology trends and determine key technology refresh areas e.g., new OS and upgraded or advanced IT Infrastructure components at the Data Centre and Disaster recovery sites

4.25.2 Identify potential alternative technologies and solutions that can be deployed in the DC and DRC sites and co-develop analysis parameters with the department

4.25.3 Technology refresh shall include changes in application, network, manpower or hardware.

4.25.4 In case of any new addition or deletion proposed by MSI and accepted by ITECCS, cost of the new intervention shall be addressed by change control note (details available under clause 5.35)

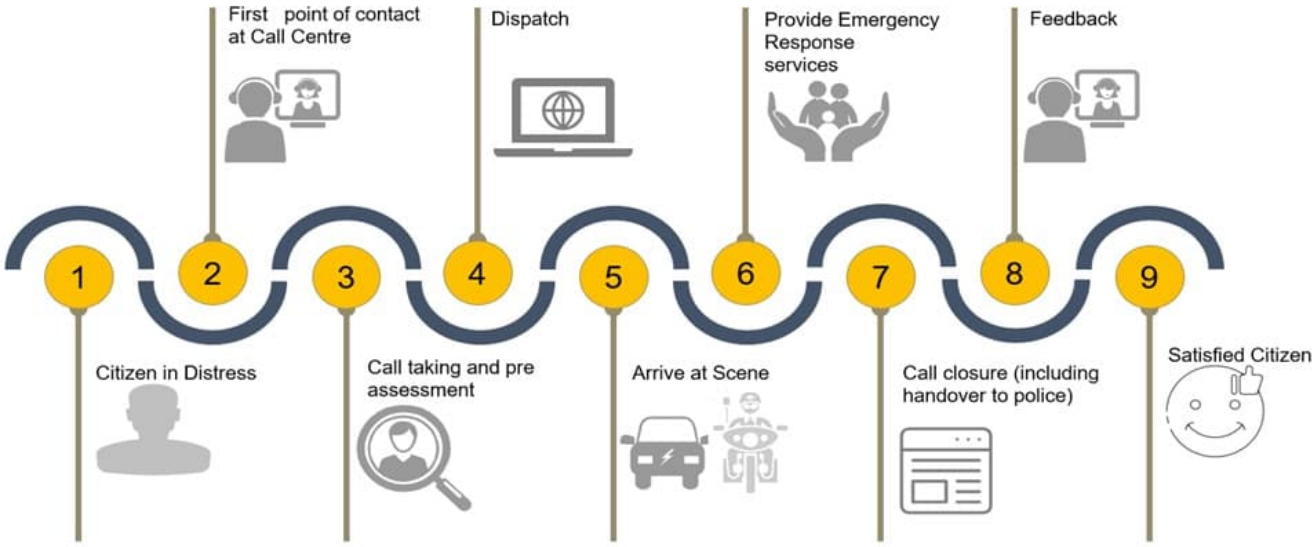
4.25.5 Prepare and submit a technology refresh proposal to the department for approval. This proposal shall comprise of:

- Drivers for technology refresh (e.g., Change in the Emergency Response solution components – Telephony, Network, Database, and storage technology etc.)
- Key options and evaluation of each option (Cost-Benefit analysis, Degree of Social Impact the refreshed solution shall have etc.)
- Detailed plan for implementation of technology refresh at the DC and DRC sites
- Likely impact, if any, on service level agreements with the OEM's, MSI etc.
- Expected cost reduction due to induction of new technology
- Expected process and SLA improvements

4.25.6 MSI has to propose first Technology Refresh Reports at the end of 2nd year, 4th year and in the end of the Contract period.

4.26 Process Overview

This for understanding of MSI

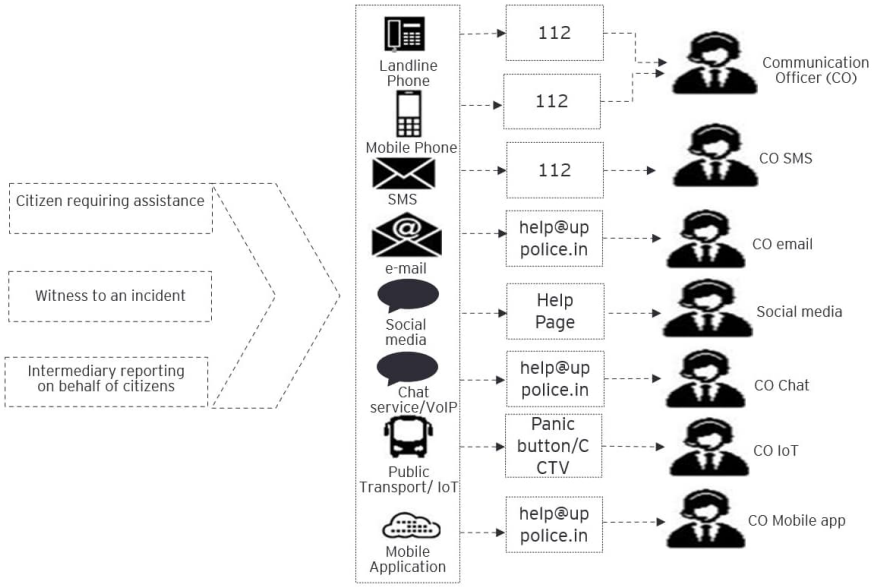


Emergency Response Process Overview

4.26.1 Citizen in distress

A citizen who requires assistance or witnesses an incident shall be able to connect to a centralized system to avail of Police emergency services. The NexGen UP112 system shall have a platform to integrate other services such as Fire, Medical assistance 108, Women Power Line 1090, CM Helpline 1076, Women Helpline 181, Kumbh, GRP, Disaster Helpline 1070, NHAI 1033, UPEIDA and YEIDA Express Way, CCC Smart & Safe Cities thereby provide efficient emergency response services to the citizen. Thus, assistance would be provided to citizens in distress connecting to any of the above-mentioned platforms via 112 or vice versa.

4.26.2 First Point of Contact at NexGen UP112



As illustrated through the diagram above, any citizen facing an emergency will be able to connect to contact centre through various modes of communication as mentioned below:

a. Land Line phone

Citizens shall be able to dial from a fixed-line phone to UP112 system which requires basic land line phones.

b. Mobile Handset

Citizens shall be able to dial from any mobile phone (on any OS i.e., iOS or Android) to UP112.

c. SMS

Citizens will be able to text from their mobile phones to the UP112 system on a number, and possibly that number should be 112 instead of any mobile number. The text message would land on the CAD system itself, and events can be created directly from CAD.

d. Email

Citizens will be able to connect with the UP112 system through email, email shall be with domain name 112. To perform this activity citizen requires a valid email ID and internet access. There would be direct integration with the CAD system where email would land on the CAD itself and events shall be created directly.

e. Chat Services

It will be the communication medium for citizens to inform UP112 system about emergency through messenger services or VoIP systems. System will have pre-decided messenger ID and VoIP number which will be made available for citizen support. The citizen will require installed messenger services on terminal (with microphones) or GPRS activated cellular device with internet access. With VoIP, analog voice calls are converted into

packets of data. The packets travel like any other type of data, such as e-mail, over the public Internet and or any private Internet Protocol (IP) network. Using a VoIP service, citizens can call landline or cell phones. One can also make computer-to-computer calls, with both parties speaking into a computer microphone and listening through computer speakers or headsets.

f. Public transport/ IoT

UP112 will be integrated with IoT devices used by departments/ citizens. The Device-to-Device (D2D) communication will involve collection of data from monitoring sensors installed in IoT devices and transmission over wireless GSM/ GPRS connections. The data received from these registered IoT devices shall be used for the delivery of emergency response services to the citizen.

g. Mobile Application

Through 112 NERS app any registered citizen in an emergency can connect with the UP112 system. These applications use GPS for location tracking of a distressed citizen. The mobile application may be based on the Android / Windows / IOS platform. In NexGen UP112 currently, live applications need to be continued post-development of new features or enhancement in currently running ones.

h. Social media

Distressed citizens shall be able to connect with UP112 via Social media tools/applications. Also, Social media tools/applications will allow UP112 to distribute information to wider audiences, interact with the public. System shall easily populate all the details on CAD solution for event creation.

i. Transfer of calls to and from Integrated Agencies

UP112 system will have feasibility to transfer calls to and from all the integrated agencies that have required infrastructure.

4.26.3 Call taking and assessment

Call taking and assessment play a very crucial part in emergency response. This includes collation of information from a distressed citizen such address, name, and event details. COs will classify the calls under actionable, non-actionable and other emergencies categories during the assessment step before forwarding the event to auto-dispatch.

a. Call taking process

Communication Officers shall be able to handle all mode of communication. COs shall collect information related to incident from the distressed caller and create an incident report. All unanswered calls shall fall under a separate category and shall be handled by 'Unanswered desk' with dedicated COs who calls back to the unanswered phone numbers.

i. **Communication Officers** are classified majorly into two subcategories:

- **Inbound Communication Officers**: These Communication Officers shall be responsible for handeling all incoming calls/connects. COs shall coordinate with the distressed caller to receive information about the emergency and respond according to the defined SOPs.

- **Outbound Communication Officers:** Outbound COs shall call the distressed person to receive the information about incident and create a report. These COs will be resposible for handling any unanswered calls and collecting and collating the Citizen experience post resolution of the emergencies.

ii. **Location Tagging by CO**: COs desk shall have the facility to display GIS based enriched data which can display a Caller Location on GIS map. Location displayed on GIS map would be verified by CO based on caller's details and would be tagged into an event before sending it to auto dispatch.

iii. **Work from Home (WFH):** Considering the severity of Pandemics such as COVID 19 and similar other Force Majeure situations, Work from Home environment shall be created at UP112 HQ for communication officers so that same can be replicated in real situation at HQ and both the OMCs. For achieving its feasibility, 10% COs of any one shift shall be working on WFH setup every day at UP112 HQ. COs working on Work from Home setup shall be rotated on weekly basis so that every CO is accustomed to WFH setup

iv. **Details Availability of Citizen**: In case if a Citizen calls and it got disconnected the details filled by CO shall be available to next COs for at least one day if the Citizen call again with same number.

b. Call Assessment

The assessment of calls requires involves following steps:

i. Actionable Calls shall be classified as per service required e.g., Police, Fire, Ambulance, 1090 etc.
ii. Classification of calls under Actionable calls (ACs) or non-actionable calls (non ACs).
iii. Call prioritization before routing the call to dispatcher and sending alerts to various levels depending on severity of cases

c. Call details records

CAD shall record the particulars such as date(s) and time stamping of call landing. The call details records involve:

i. System records such as Caller Location, Call Type, network processing data, caller classification and other relevant data
ii. System will provide features to create/ read a Call Detail Record and facility to update it
iii. CO will be able to create incident record though CRM/CAD and system will maintain the association between an Incident Record, the Call Detail Record, and Call Recording
iv. CO will be able to record and navigate on display map using CAD with primary interface in Hindi also. The required fields will be as below (indicative):
    1. Unique ID of each case: Every incoming incident would have a unique number and details will have all the necessary data like caller, dispatcher, time stampings, category of incident etc.
    2. Additional Phone number: Any other contact number
    3. Communication medium
    4. Probable time of occurrence of incident

5. Caller Name
6. Caller Gender
7. Caller Address
8. Actionable Call type: Actionable Call will be type of Call, in which citizen requires an emergency help whether it is police, medical, fire etc.
9. Non-Actionable Call type: Non-Actionable Calls are non-emergency calls.
10. Description: Details of distress
11. Notes: special notes about caller

v. For logging an event, COs will have access to GIS map, with enriched data and Navigation keys such as:
1. New
2. Accept
3. Edit
4. Save
5. Cancel
6. SOP
7. Support Information
8. Log file
9. Voice log
10. Add Task
11. Route
12. Conference

d. Call forwarding

Once the CO captures minimum potential data in the CAD she will forward the emergency actionable event to the dispatch system using CAD. Event will populate at the desk of:

i. RoIP Monitoring Officer (RMO) at District Control Room
ii. Event Supervisor (ES) at UP112 HQ

4.26.4 Dispatch

Dispatch process would be an automated process as auto dispatch system will identify the vehicle for dispatch based on the least time for a PRV to reach at the event location. The CAD will dispatch PRVs based on a predefined algorithm. Factors for dispatch will include actionable events type, response action methodology, day, and time of occurrence, PRV availability and number of vehicles required, jurisdiction, proximity, specialization, available equipment on duties resources and logical AND/OR combination within rules. The CAD shall be freely customizable as per operational requirements.

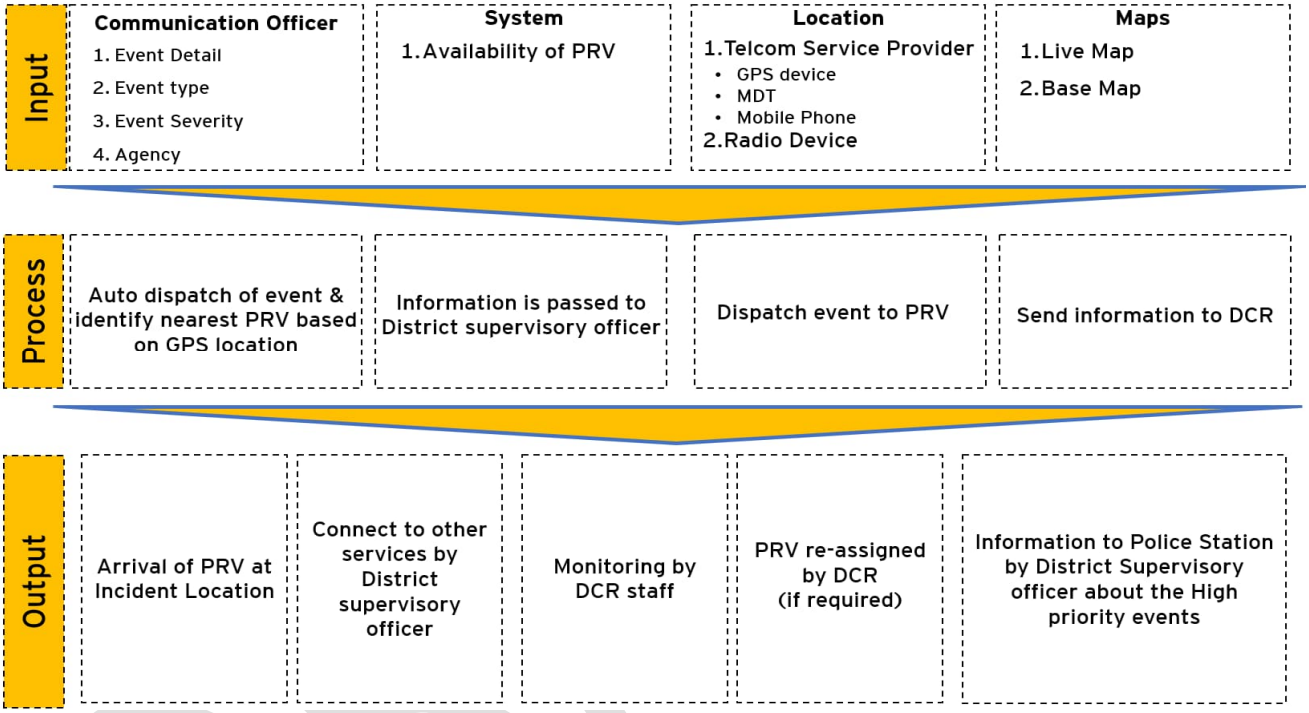
To ensure the availability of Latitude and Longitude, every PRV would have 3 hardware installed

a) MDT
b) Dedicated GPS device
c) Mobile Phone

Different TSP sims would be provisioned to minimize the chances of non-availability of the telecom service provider's network.

Post-event assignment the respective district control room (DCR - RoIP) will come into the action of monitoring and validation whether the correct PRV is tagged or not. In case wrong/ far distant PRV is tagged for an event, PRV staff will have the facility to connect with the respective DCR - RoIP for reassignment of the event to other PRV.

a. Dispatch System in NexGen UP112



Events tagged as actionable event by communication officers would be available to

a) RoIP Monitoring Officer (RMO) at District Control Room
b) Event Supervisor (ES) at UP112 HQ

b. Inputs

i.Inputs captured by Communication Officers

Event related details would be captured in CAD system by COs. The response to an actionable call would be affected by previous experience about the caller, location, or locality. The CAD would retrieve, and display details related to calling number such as past review by caller, past event types, last address details provided by citizen etc.

ii.CAD System and Location

The CAD System will display the information entered by the CO for actionable calls. It would display the event details as mentioned by the CO or address database but the RMO and ES would also have the option of reallotting and retagging the actionable calls. Also, CAD system would display all the last details of caller (repeated caller) as a suggestion.

iii.PRV Status

The GIS will display the assigned / unassigned PRVs using appropriate and intuitive graphical symbols:

a) Unit shall report departure for, arrival at and, departure from a location with time stamp
b) Vehicle beacons colour will change automatically with their change in status, i.e., dispatch, arrival at scene, availability status etc.
c) The entire movement of a vehicle would be time stamped and monitored by the RMO and ES staff
d) The RMO or ES will be able to lock vehicle on map for continuous tracking

c. Process

i. Auto dispatch

The CAD will dispatch PRVs based on a predefined algorithm. The conditions will include actionable events type, response action methodology, day, and time of occurrence, PRV availability and number of vehicles required, jurisdiction, proximity, specialization, available equipment on duties resources and logical AND/OR combination within rules. The CAD shall be freely customizable to include such varying SOPs and operational requirements.

ii. Information to DCR - RoIP

RMO at District Control Room would get all the event details and would perform the activities

Role of RoIP Monitoring Officer (RMO) at District Control Room

a) RMO at District Control Room will get all the information about the case (details captured by CO) in CAD application. He will verify that nearest available PRV is dispatched by Auto dispatch system
b) System will generate auto notifications for events where defined timelines are not complied such as Event Acknowledgement is not made, event location arrival is not made etc. For these notifications RMO will take follow-ups from PRV staff
c) RMO may use wireless system to send information to the field team
d) End to end tracking of all actionable events would be possible at RMOs end
e) RMO will access to all the details such as GPS, Location, Patrol, attendance as per HRMS etc. for follow ups with PRVs
f) RMO would have feasibility to review and may give feedback/ comment on details of ATR submitted by PRV staff
g) Complete staff would be police personnel
h) Coordination with PS/Thana in case of cases handed over to Police
i) In case DCR - RoIP is down, Event Supervisor (ES) at UP112 would take over the activity of RMO at DCR - RoIP.
j) Field event – RMO shall also assist in creation of an event by PRV. In case PRV would like to register an event and get dispatched to a location, the PRV staff can contact the DCR and get event created for self-deployment.

iii. Information to Event Supervisor (ES)

Event Supervisor (ES) at UP112 would get all the event details and would perform the activities

Role of Event Supervisor (ES) at UP112

a) End to end monitoring of High priority cases
b) System will generate auto notifications for events where defined timelines are not complied such as if Event Acknowledgement is not made, arrival at event location is not made etc. For these notifications district supervisor will take follow-ups from PRV staff and DCR - RoIP
c) Event Supervisors (ES) would have responsibility to connect with other emergency services such as fire, ambulance etc. as required

iv. Information to PRV

PRV would get a notification once an event is allocated and would perform the activities defined as per SOP

d. Output

i. Action Taken Reports

In the case of high-priority events, post-capturing mandatory fields such as event type and location by CO, a simultaneous dispatch functionality shall be available in our system. Desktops with screens will be provided to each district control room to monitor the dispatch of vehicles.

Based on information captured at site post-event catering, RMO, ES, or PRV staff would be able to enter their remarks. *A separate extra section shall be available to suggest changes in event detail captured by CO, details captured by communication officers* ***shall not*** *be editable*. In case no changes are required in detail captured by CO, this section can be left blank.

ii. Simultaneous Call Taking and Dispatch

In the case of high-priority events, post-capturing mandatory fields such as event type and location by CO, a simultaneous dispatch functionality shall be available in our system.

iii. Call Conferencing and Patching

Event supervisor would be able to organize a conference call from his/her console and patch with phone or radio. Call Conferencing would be possible between PRV staff, RMO, and ES through mobile phone. Similarly, a video conferencing facility would also be available at all the levels i.e., PRV, District Control Room, and UP112 Headquarter.

iv. Monitoring of the operations

The operations at the contact Centre shall always be commanded by an officer working in shifts. This officer would be responsible for generating an appropriate operational response to each actionable call. It would, therefore, be possible for him/her to monitor all activities of call taking, dispatch, and response on large video

walls. Prompt and appropriate UP112 system with voice, data, and image communication and logging and collaborative, multi-department response to emergencies will be key factors for RMOs and ESs pool for effective emergency response handling.

4.26.5 Arrive at Scene

a. Once an event is received at PRV, the deployed staff must acknowledge that the event is received, post that PRV must en-route, once an event is allocated the PRV would be flagged as non-available in our system and system shall automatically change the status of PRV to arrive once PRV reaches the event location.
b. PRV staff will monitor the event type and location and after quick evaluation moves towards the event location.
c. PRV staff shall also not be able to skip step and directly press the last step and skip the precursor steps.
d. The RMO at District Control Rooms will monitor the movement of the vehicles towards the emergency site and provide route support based on shortest time, distance, traffic conditions, etc.
e. RMO will pass on the instructions and follow up with field personnel. If an ambulance, fire brigade, or district Police are required for handling the emergency, event supervisor would provide the required assistance.
f. If an allotted event is beyond the jurisdiction or if a far distant event is allotted to PRV by auto dispatch system. PRV staff can connect with the district control room for allocation of event to other PRV. District control room staff would have the authority to change the allocation of a PRV for an event.
g. During the free hours, PRVs will patrol as per the designed route plan.

Note: There might be cases when PRV reaches the event location and identifies that wrong details are mentioned in the allocated event that is event is not just a police-related event, requires assistance from other agencies, or that additional personnel are required. In such cases, PRV will directly connect with the RMO at the District Control Room / RoIP.

4.26.6 Emergency response service

Field personnel post arriving at the incident location will be able to take suitable action/provide the required emergency support to the citizen in distress as per the defined SOPs and update the status through MDT.

During NexGen UP112, each field team shall be equipped with suitable measures to perform the following functions:

a. Communication between District Control Room/ RoIP and PRV staff

i. Action taken report shall be received by the district control room
ii. If Action taken report is not received by the district control room. In that case, the district control room will follow up with the PRV staff

b. Location Transmission

Transmit the location and direction of the vehicle to the CAD system. The field unit shall not be able to switch off his GPS Tracking manually.

c. Vehicle Mounted Camera

For critical identified areas, 4 W PRV's will be equipped with PTZ Vehicle mounted camera. While moving to an event location PRV's will record the route and incident. The live feed of the same shall be shared to command centre for effective decision making.

d. MDTs / Mobiles

The MDTs/Mobiles will have an inbuilt camera with a video recording facility. The MDTs will have an audio recorder which shall be used, among other applications, for recording and transmitting the Action Taken Reports (ATR). It will also be used to monitor attendance, vehicle utilization, and other aspects of PRV management

e. Body Worn Camera

For critical identified areas, 4 W and 2W PRV staff will be equipped with Body Worn Camera. Post reaching the event location PRV staff will record the incident. If required, the live feed of the would be sharable to command centre.

f. Push to Talk (PTT)

PRV would have Push to Talk (PTT) features at its disposal. This facility would be available either via radio device or through an application in MDT. Using this option all the PRVs would be able to talk with each other simultaneously. The number of PRVs that can connect simultaneously can be set dynamically when the PTT feature is made available in MDT for example if 3 PRVs are dispatched in a high priority event all of those can connect simultaneously. Hence the number of PRV that can connect simultaneously would be variable.

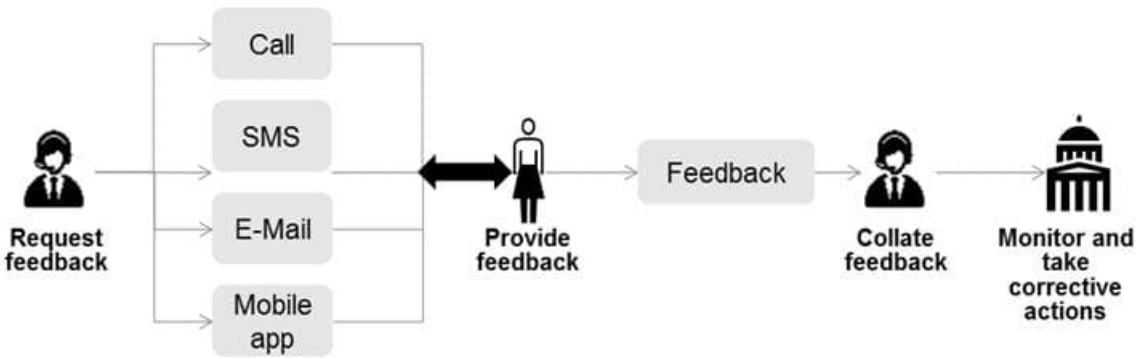
g. Data Transmission

Transmit and receive data through Mobile phones and Mobile Data Terminals.

4.26.7 Event Closer

ES at HQ will check the closure report from the field team and close the case if satisfied with the field team's response. At the end of the operation, PRV staff may either hand over the case to local Police or close the emergency if the case doesn't require local Police intervention. The local Police will download details of the action taken report from a web link or app and initiate the case file and update status in the UP112 system.

4.26.8 Citizen Experience/Feedback



Citizens who reached the UP112 system and were assisted by the Contact Centre will have a facility to represent their experience by rating the quality of service provided by the emergency response team. To know the progress in their registered event, citizens can communicate through Call, SMS, email, or mobile app to contact the Centre and inquire. Additionally, the CO feedback desk shall be able to communicate with distressed citizens post-event closure, after a certain time, to know about his/her experience. To ensure high quality and reliable feedback capture, at max 3 feedback calls will be attempted to a citizen in a span of 24 hrs if call could not be connected in earlier attempts. These calls would be made with a time gap of at least 1 hour within the time allocated for seeking the feedback.

NexGen UP112 aims to achieve customer satisfaction of more than 96% by the assistance of advanced analytics methods such as generating word clouds for quality improvements through data-based decision making and monitoring. Also, by introducing new interventions such as chatbot, SMS text links to take feedback.

4.27 Technology solution

The MSI shall be responsible for operation and maintenance of existing UP112 Project with required up-gradation, addition, customization, integration, testing etc.

4.27.1 Solution overview

Given below is an overview of the components of the solution:

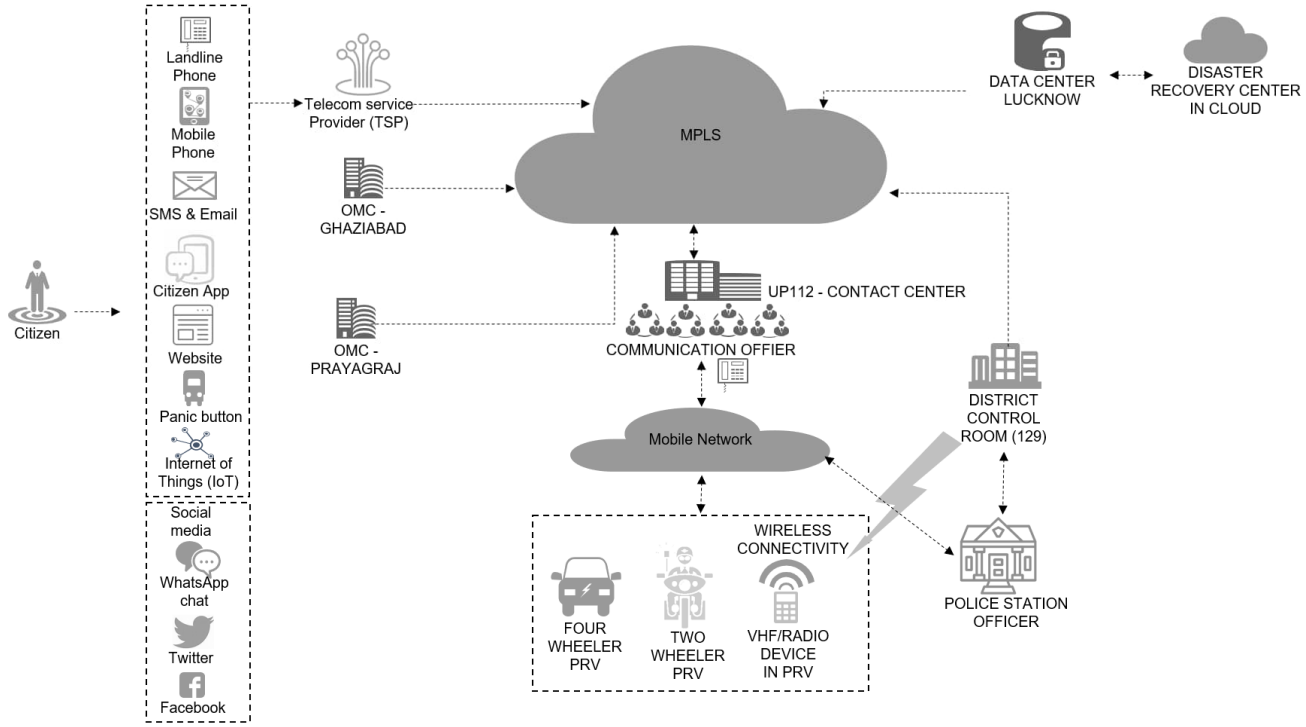


Figure 1: Solution Overview

a. **Solution Holistic View-**

i. Citizen would be able to communicate through call, messages, social media, SOS app etc. for registering a Police, Fire and Medical emergency

ii. Provision of the integration of system with communication channels like e-mail, IVR, SMS gateways, Social media interfaces etc.

iii. As part of current and future integration requirements (emergency services such as Disaster helpline 1070, NHAI – 1033, UPEIDA and YEIDA Express Way, CRIS, Women Power Line (1090), All smart cities, Safe Cities, Disaster Helplines, Metro (Lucknow, Agra, Gorakhpur, Kanpur), Fire Services, SDRF, GRP, CRIS, CM Helpline, Cyber Helpline, 1090, 181, NHAI, UPSRTC etc). will be connected to UP112.

iv. Connectivity of all district control rooms, Commissionerate, other offices directly over MPLS

v. Connectivity via SIM network with all the PRVs in the field

vi. Use of RF network for communication to PRVs from DCRs, Commissionerate's, OMCs and Lucknow contact centre

vii. Two operational mirroring centres (OMCs) at Prayagraj and Ghaziabad will be supporting Lucknow contact centre in routine and disaster situations

viii. NOC, SOC and helpdesk in Contact Centre will be provided for monitoring IT operations

b. **System process steps during emergency handling**

The processes involved in receiving an emergency call and responding to an emergency involves various technical functions. At every step of the functional process, technology involvement is a must to ease and automate the process. Some of the key technical aspects are:

i. **SIP**: All 112 number calls from the state shall be routed through Telecom Service Provider's dedicated channels to the contact centre. SIP routes the incoming calls to the contact centre and time lag for this process is almost negligible. Required channels need to be procured by MSI for contact centre at Lucknow and 2 OMCs at Prayagraj and Ghaziabad. DRC is proposed to be hosted at different seismic zone. MSI has to provide the channel as per the BOQ and all the channels shall have facility of incoming and outgoing both.

ii. RF, Mobile CUG exchange and Land Lines- MSI need to ensure that there will be failover of communication

iii. **IP PBX:** An IP PBX is a private branch exchange (telephone switching system within an enterprise) that switches calls between PSTN and VoIP (voice over Internet Protocol or IP) and vice versa on local lines while allowing all users to share a certain number of external phone lines

iv. **Automatic Call Distribution (ACD):** ACD supports skill-base routing, multiple group support, priority handling and Queue status indicator. ACD shall be provided in 1:1 Hot Standby configuration. Even the COs can receive missed call data etc. from ACD and identify the available CO and then dial the outbound call and connect with the citizen

- **Computer Telephony Integration (CTI):** CTI middleware would be capable of integrating with Case Record Management /Front-end application to facilitate integration features. It shall send notifications and events on CO screen for every call. It shall be provided in 1:1 Hot Standby configuration
- **Call Record Management (CRM):** Call Record Management comprises of various inputs fields like name, address, contact number, incident type, incident location, caller location etc. Pre-populated information from location detection Information about the caller and the incident would be recorded. It shall be used to track all the call records and useful for categorizing the cases in terms of crime, inquiry, priority etc.

- **Computer Aided Dispatch**: CAD will be integrated with CRM application with enriched GIS where CO would collect information related to incident from the distressed caller. CO will further dispatch the incident with information
- GIS coordinates of a distressed person will be in the form of longitude/ latitude and location of PRVs would be displayed on the screen of the event supervisors and district control rooms.
- Information about emergency would pass from CAD system to the identified MDT device installed at PRV via auto dispatch systems.
- Response team at field will complete the case and close the event through MDT by filling action taken report (ATR)

c. Data Centre (DC) and Disaster Recovery Centre (DRC) Technology Architecture

The indicative representation for the DC and DRC technology architecture is presented below for reference purpose only:

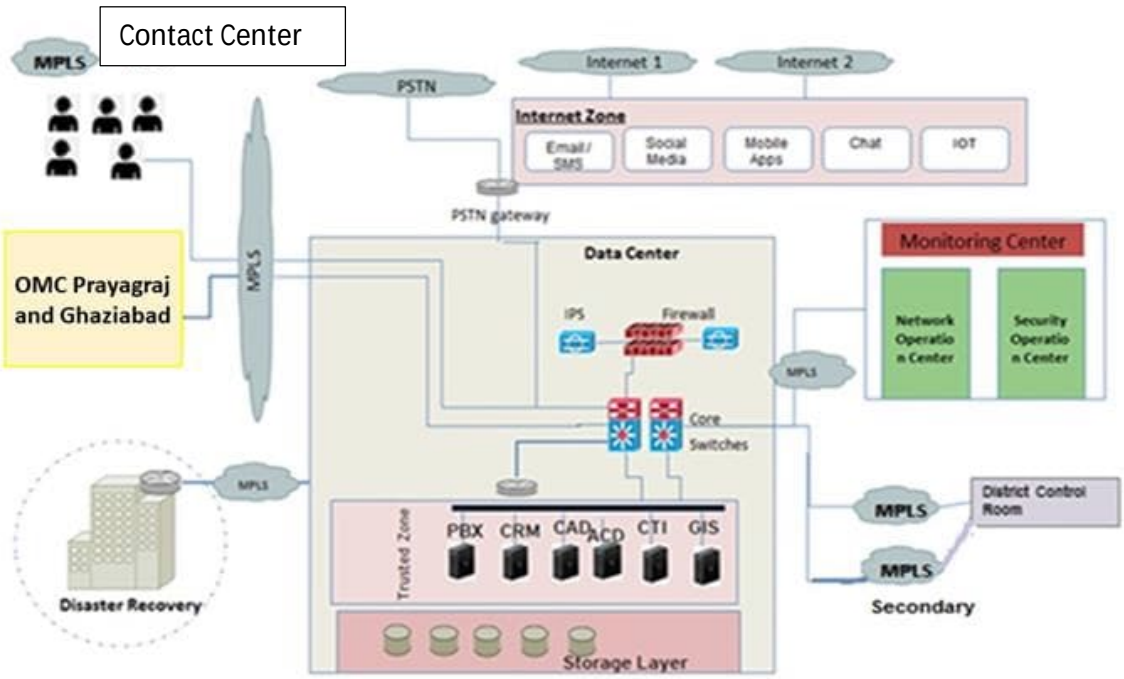


Figure 2: DC- DRC - Technology architecture

i. The Data Centre would consist of compute, storage, network, and security elements in redundant modes. The DC and DRC would have redundant capacity of components, dual powered equipment, and multiple uplinks. All these elements would need to be connected in a logical and functional manner with robust redundancy. Militarized and de-militarized zones would be segregated by implementation of firewalls and IPS. The internet and intranet zones shall ensure that public and private traffic is handled properly with appropriate security mechanism.

ii. The Data Centre will be hosting a number of compute and storage elements for applications like CAD, GIS, IDM etc. with backup facility for major applications and data transacted during all the steps of the emergency process
iii. MSI need to provision the data at centralized location in DC and DRC so that it will be used at all places to assure data accuracy and simplify data management
iv. DRC need to be hosted on cloud in different seismic zone from DC.
v. The DC would have redundant power sources at three levels, Main supply, Generator (Not in scope of MSI) and UPS (MSI Scope)
vi. The Disaster Recovery Centre shall consist of key elements similar to DC in terms of network connectivity to servers and storage devices in case of a disaster. The internet and intranet zones shall ensure that public and private traffic is handled properly with appropriate security mechanisms even through the DRC. Major applications, data base replica will be co-hosted at DRC
vii. The infrastructure provisioned in DC shall be capable to handle 100% load at any point in time and DRC shall be capable to handle 50% load in case the DC is down
viii. Applications will be hosted on multiple VMs as hot standby and load will be shared. It is important that Application/ global load balancer needs to be stabilized so that load sharing among the VMs can be done. The DRC acts as backup to the DC for Business Continuity.
ix. All the historical data of UP112 shall be saved and NexGen UP112 data shall be available in archive whereas 6 months data shall be readily available on primary storage
x. DC and DRC shall operate in an active-passive mode. The connectivity between both the data centre and disaster recovery would ensure the replication works seamlessly with no data loss.
xi. The replication between both the DC and DRC would ensure that there are no data inconsistencies on both application as well as storage level.
xii. The replication technique between data centres and disaster recovery shall be both database as well SAN storage based replication. There shall be no data inconsistencies issues with either the data centre site or disaster recovery site
xiii. MSI need to ensure that in the DC two copies of data will be stored in real-time and further in 30 minutes that data will be stored in Disaster Recover location. End of day backup should be done on Virtual tape Library
xiv. The server load balancer can be effectively utilized in order to seamlessly manage the server failover conditions. The design for the Disaster Recovery Centre should be built with the same logic
xv. The zone shall be defined on a router to divert trusted, internet zone, Network management zone respectively. The intranet zone and Staging Zone connects directly to MPLS with separate provisioning of IPS, redundant firewalls which intercepts all internal traffic which comes from NexGen UP112 Contact centre.
xvi. The classification of zones on the firewall shall play an important role to diverge the public traffic by the means of setting up of internet zones. The internet zone shall receive traffic request from all external users which shall need to access the web services for respective applications

xvii. The trusted zone on firewall carries all the key critical applications such as Voice gateway, IP PBX, ACD, CTI, CAD, GPS data etc. which ensures that the critical applications are protected from external attacks

xviii. The security device has been proposed to ensure that the traffic is filtered for all deep packet malicious activity which passes through the firewall

xix. The internal user should not be able to access any content, website or application not authorized through the IT infrastructure such as watch videos, social media etc.

xx. The core switches in redundancy shall be provisioned in a manner where inter VLAN routing happens. Management zone VLAN is also created to ensure the NOC i.e., EMS, NMS, MDM and SOC elements need to be provisioned within the DC and DRC environment

xxi. The disparate elements DC, DR, UP112 contact centre, OMCs, PRVs and field locations would be networked and provisioned in a manner that optimal operational redundancy exists. In case, both the DC and UP112 contact centres are down, the DRC will point to the backup operational mirroring Centres at Prayagraj and Ghaziabad.

xxii. Once the DC will be UP the data from DRC of down time will automatically be pushed by DRC to DC to establish continued historical data backup.

xxiii. MSI will provide mechanism that in case the Lucknow Contact centre is down while DC is up, all the applications of DC including incoming emergency calls will be pointed towards two OMCs in load sharing mode

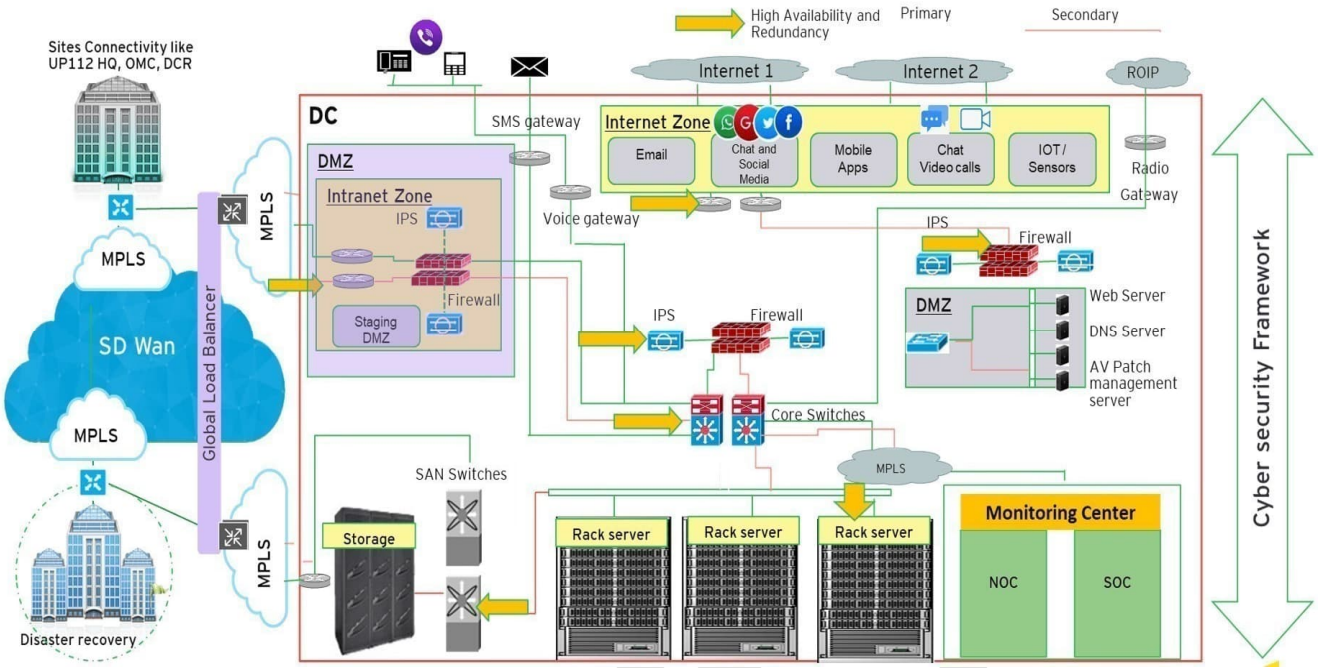
xxiv. MSI will provide mechanism that in case DC is down while UP112 contact centres is up then UP112 Contact centre will receive inputs from DRC for functioning

xxv. MSI will have to provide mechanism that, in case complete UP112-ITECCS is down then handling of all incoming calls will be routed from OMCs and DRC

xxvi. The DC and DRC would have exclusive VPN management system

d. **System Architecture-**

The indicative representation for UP112 System architecture is presented below -



a. The UP112 architecture has UP112 Contact centre and Data centre hosted in Lucknow, 2 OMCs at Prayagraj and Ghaziabad respectively and DRC will be hosted on cloud.
b. All the sites will be connected to each other via MPLS network.
c. The proposed solution should be fully cyber secured as per security principles mentioned in clause 4.27.4
d. Global load balancer will be used so that the traffic can be easily distributed among UP112 Lucknow, 2 OMCs and DR.
e. All the application as per the section 4 will be hosted on data centre.

e. Contact centre

i. Contact centre of UP112 is located in Lucknow
ii. All voice calls and data messages would mature at UP112
iii. CO's and ES's will be placed in contact centre for their operational purpose it will have all necessary IT infrastructure like multi-screen desktops, printers, copiers, UPS etc

f. Operational Mirroring Centres

i. OMCs located at Prayagraj and Ghaziabad will be functional actively during normal routine or in case of a failure at contact centre in Lucknow and for special cases which require special monitoring.
ii. Backup operational centres (at Prayagraj and Ghaziabad) at eastern and western part of state are designed as operational mirroring centre of HQ contact centre, Lucknow. Each OMC will have 15% capacity of overall contact centre capacity and perform the function of Call receiving and supervision
iii. These centres are to be connected to DC and DRC for accessing applications and are equally operational to handle all emergency services

g. **UPS and Earthing Solution**

i. **UPS Solution**

a. MSI need to install the UPS as per required capacity in DCRs and Commissionerate's.
b. The UPS to be deployed needs to be online UPS, SNMP based monitoring so that all the input power faults are isolated and reliable power is fed by the battery/inverter system.
c. MSI may choose the option of using existing UPS till the time product is not EOS/EOL, but MSI need to ensure the replacement of all battery packs in their scope for all the locations

ii. **Earthing at Remote Locations and UPS**

a. MSI has to provide a path (a protective conductor) for a fault current to flow to earth. MSI responsibility is that all the DCRs-RoIP and Commissionerate's need to be equipped with state-of-the-art earthing systems. Earthing is required to make all the infrastructure of this project run reliably and efficiently.
b. MSI has to ensure proper Rack Earthing secure the equipment in the rack at all locations.
c. MSI need to ensure two time earthing during the initial and mid stage of the project
d. MSI need to maintain the proper earthing during the project

h. **UP112 ROIP SOLUTION**

i. MSI to ensure communication through ROIP between contact centre at Lucknow and OMCs, DCRs and Commissionerate's to the PRV's in the district which are present in line of sight (LOS)
ii. Radio Frequency devices will be integrated with NexGen UP112 application connected on MPLS network and provides the communication path between the Event supervisor console and the existing wireless radio equipment. RF communication will act as part of communication system for alternate path over IP network. All the wireless radio equipment present in police mobile vehicle is wirelessly connected to the RADIO Server in broadcast mode over RF.
iii. Host the radio application at DC and DRC
iv. MSI should ensure that ROIP hardware and software and other relevant components will be provided in DCRs, Commissionerate's, 112 Contact centre and OMCs

i. **Monitoring Centre (MC)-NOC, SOC (Network Operations Centre and Security Operations Centre) and IT Help Desk**

i. MSI has to setup NOC, SOC and IT helpdesk under monitoring centre at UP112 Lucknow

ii. Set up NOC and SOC services to monitor and control the network, applications, hardware, and security operations for the entire project.
iii. Set up IT Help Desk for all IT related resolutions for the entire project
iv. The MC will provision for an IT Helpdesk to facilitate users on their day-to-day activities. MC personnel will be responsible for monitoring all devices. This is required to manage different networks and security devices or to provide geographic redundancy in the event of one site becoming unavailable. The Monitoring centre will be manned 24X7X365 for the duration of the contract.
v. MSI have to develop the NOC and SOC operating procedures in adherence with UP112 applicable policies and guidelines.
vi. MSI has to ensure authentication-based access controls are followed for NOC and SOC operations.
vii. The details of NOC and SOC are mention in clause 4.27.6 and 4.27.4 of RFP respectively
viii. Details of IT Helpdesk services to be performed by MSI-
    a. The MSI needs to provide IT Helpdesk services at the Monitoring Centre in Lucknow for all the system users (Communication officers, Field personnel, Supervisors, IT Support staff, etc.) to address and assist in troubleshooting any IT related issues they might face on a day-to-day basis.
    b. The IT Helpdesk should be accessible by the users through a dedicated 24 X 7 helpline and through the helpdesk sub-module of the EMS system and shall be the single point of contact for issue management and resolution for all the users. It shall be integrated with the EMS and shall be designed to meet the SLA response and resolution timelines
    c. The IT Helpdesk staff should be able to log a ticket based on the user queries related to any component of the Emergency Response system as defined under the scope of work and assign them a unique number.
    d. The IT helpdesk staff shall assign severity level to each query; assign the queries to the appropriate personnel for resolution e.g., System or Network or Database or Security administrators for queries or issues related to any of the corresponding areas.
    e. The IT helpdesk staff shall track each query to resolution, escalate the queries, to the Project Manager if necessary and provide feedback to users on the current status of their ticket.
    f. The IT helpdesk must always maintain high user satisfaction levels
    g. The IT helpdesk must maintain the SLA statistics and submit monthly and quarterly report to the UP112
    h. Help Desk Coordinators shall generate reports using a call logging and reporting tool which should have the following reporting capabilities:
    - Call Analysis
    - Call Trend
    - Call History Report
    - Daily Call Completed and pending Reports

j. **Monitoring by Field Supervisors (Thana, SP/SSP/Commissionerate, District Control Room/ROIP, Range, Zone)**

i. The Police officers/personnel of DCR-ROIP, Zonal and Range officers, Commissionerate and other Police Units will be able to track events in their respective jurisdiction area
ii. All DCR-ROIP of districts, Commissionerate's and other offices will be equipped with desktops, bandwidth, and wireless equipment to track events
iii. These field locations as mentioned above will have ROIP devices with installed software and required hardware. Even IP phones with Video conferencing facility will be provided at these locations.
iv. SO/SHO (Police Station Officers), Circle Officers, Addl. SPs of district police and SSP/SP/CP (other police officers at Commissionerate) at field level access mobile applications to locate events under their purview and would be able to monitor the incidents reporting on web application

Overall solution can be better understood by the principles and the architecture requirements as per Section below-

1. **System Architecture Principles**
2. **Security Principles**
3. **Data Architecture Requirement**
4. **Network Architecture Requirements**
5. **Application Architecture Requirements**
6. **Hardware Requirements**

4.27.2 System Architecture Principles

a) MSI has to ensure that the Service-oriented architecture (SOA) would be followed to enable increased process agility, improved process workflows, extensible architecture, enhanced reuse, and longer life span of applications
b) N-Tier model need to be adopted by MSI which is a multi-tier framework in which application user interface, logic, data, and their associated processing and repair are separated from each other in a logical manner. This model is more flexible in response to changes in internal logic, platforms, and structures which isolates/minimizes the impact of change. Considering the requirements of ease of support, scalability and interoperability, N-tier model is being proposed to be adopted by MSI
c) Each incoming emergency would be registered with a unique event ID in the system
d) MSI should make the provision of Active-Passive between the DC-DRC and, servers and services across the solution will be in high availability (HA) mode
e) MSI has to proposed solution that has Business Continuity and Disaster recovery capabilities by achieving the Recovery Time of Object (RTO) and Recovery Point of Object (RPO) The recovery point objective (RPO) should not be more than 4 minutes and the recovery time objective (RTO) will not be more than 20 minutes
f) MSI has to ensure that there would be no single point of failure in the system
g) MSI has to maintain the principal of minimal manual intervention and maximum automation

h) MSI has to ensure that the system should be of high performance to provide timely emergency response across the State
i) IT solution provided shall have the ability to scale-up quickly to meet the increasing number of incoming calls/ inputs from various sources
j) MSI has to ensure that all calls/ other inputs would be recorded for future purpose for a defined period of time. In case of any judicial proceedings, the records would be maintained as long as the proceedings last. Easy data mining and data retrieval facilities would be available
k) System shall have user friendly Interface and easy to use features
l) The infrastructure management shall be Directory services driven with Domain Schema
m) The system would be built from best of breed components with no obsolescence and with futuristic designs
n) MSI should take care that the technology adopted would be periodically refreshed to achieve significant improvements in Total Cost of Ownership (TCO)
o) Scalability, manageability must be present in the solution to handle huge data volumes
p) Efficient resource utilization by separation of Compute and Storage resources and through distribution of load among all sites
q) MSI has to ensure that all the system components must follow open standards
r) The data should be stored simultaneously on primary and secondary storage and later stored in DRC.

s) **Compute Design at Data Centre:** While designing the compute architecture MSI may opt to ensure that designing should be -
    i. Deployed in high availability mode with diversity in Blade server and Virtual machines created on the blade servers.
    ii. The Virtual machines will be connected on the LAN network with diversity on LAN ports and LAN switch.
    iii. The Storage should also be on high availability mode with diversity in SAN Switches.

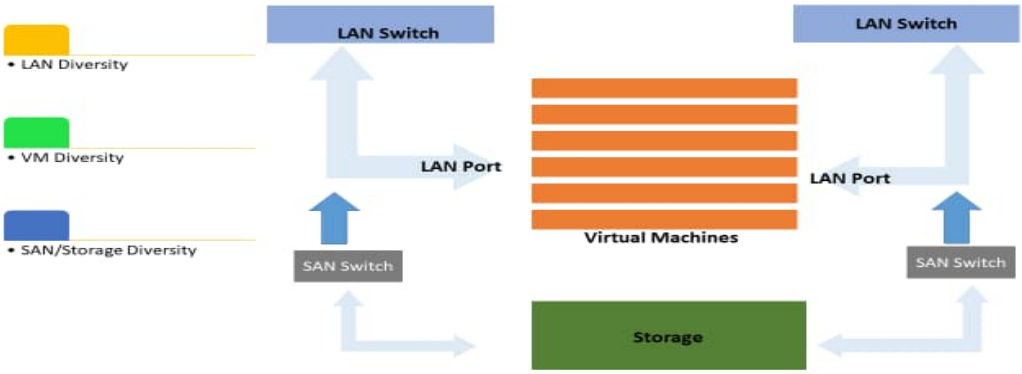


Figure 3: Compute Architecture Design

iv. The deployed hypervisor environment should be a client or hosted hypervisor. While bare metal hypervisors run directly on the computing hardware, hosted hypervisors run within the operating system of the host machine.

v. Hosted hypervisors run within the OS, additional operating systems can be installed on top of it.

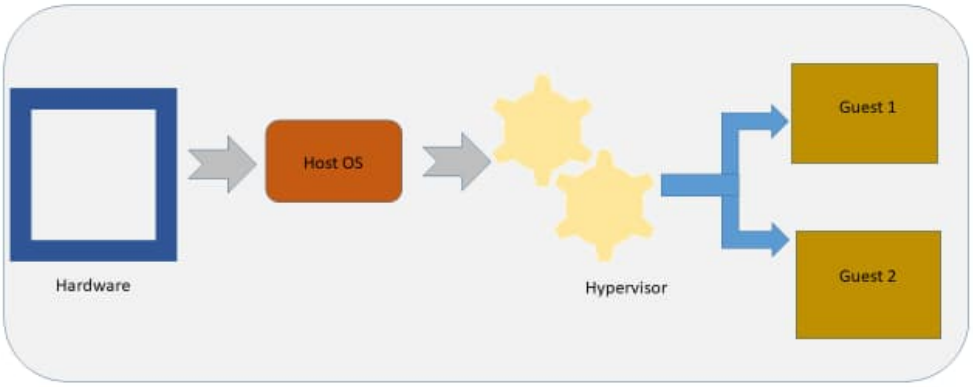


Figure 4: Hypervisor Deployment Design

vi. The Application will be hosted on high availability mode on multiple VMs available in DC and DRC.

vii. The User session load is distributed across multiple VMs.

viii. The Application should be connected via DB Server (if required) on high availability mode.

4.27.3 Security Principles

a) MSI should follow the security principles such as “defense in depth”; for numerous defense mechanisms (“layers”) in place shall be designed so that an attacker has to defeat multiple mechanisms to perform a successful attack. Multi-layered security shall be employed starting with networks, perimeter, DMZ, Data Centre, Disaster recovery, applications and databases

b) It shall also follow the principle of “least privilege”. Each user and program shall operate using the fewest privileges possible. This principle shall limit the damage from an accident, error, or attack. It shall also reduce the number of potential interactions among privileged programs, so unintentional, unwanted, or improper uses of privilege are less likely to occur. This idea can be extended to the internals of a program: only the smallest portion of the program which needs those privileges should have them

c) MSI has to ensure that all IT and IS operations will be governed by the IT and IS Policy . MSI has to prepare detailed procedures for the same and implement accordingly. All project documentation should be prepared by the MSI as per the policy and related regulations

d) Latest version of industry best practices such as ISO 27001, ISO 20000, ISO 27701, IT Act, should be followed by MSI
e) MSI has to ensure that the access to Infrastructure and Application shall follow n-Factor authentication
f) The privacy of data has to be ensured by the MSI at all times. MSI also need to ensure that data sharing is done as per the policy and the Databases and Data stores must be encrypted
g) Security in Design will encompass security risk assessment on user specifications, secure information architecture, proper role based access design and secure application and database design
h) The system will be secure at all the user touch points by using suitable security protocols and data protection methods
i) MSI needs to identify all the network attacks and counter measures must be put in place
j) MSI need to ensure that the ICT assets must also be secured throughout their life cycle as they may contain sensitive data with hardening, asset disposal and data disposal principles
k) The Network layer must have in-depth packet inspection and intelligence in blocking attacks
l) MSI should provision that the access to data would be given through application layer (via an application) at all times
m) MSI should setup the VPN and VLANS as the principle of operations for remote access and isolation of internal traffic and external traffic

t) MSI Key Response Area includes (but not limited to):
    1. In case of any security incident, the MSI will share event logs along with action plan / mitigation steps to TS-SDC DCO and ITE&C as per the SLA.
    2. MSI should detect both internal & external attacks. In addition to security attacks on IT infrastructure, Service Provider should also monitor for security events on business applications, databases and also identify network behaviour anomalies.
    3. MSI should monitor, detect, and manage incidents for the following minimum set of IT infrastructure security events:
        - Buffer Overflow attacks
        - Port & vulnerability Scans
        - Password cracking
        - Worm/virus outbreak
        - File access failures
        - Unauthorized server/service restarts
        - Unauthorized changes to firewall rules
        - Unauthorized access to systems
        - SQL injection
        - Cross site scripting
    4. MSI should monitor, detect, and manage incidents for the following minimum set of business application security events:
        - Attempted violation of defined role

- Attempted access violations
- Critical user additions, deletions
- Creation, deletion & modification of critical application roles/groups
- Changes to permissions or authorizations for critical application roles/groups
- Changes to account & password policies in the application
- Changes to critical application parameters
- Changes to audit parameters
- Sensitive data exposure

5. MSI should monitor, detect, and manage incidents for the following minimum set of database security events:
    - Granular monitoring of queries, objects, and stored procedures with real-time alerts
    - Monitor Access to Sensitive Data
    - Database access including logins, client IP, server IP and source program
    - information
    - Track execution of stored procedures, including who executed a procedure, what procedure name and when, which tables were accessed as a result
    - Track and audit administrative commands such as GRANT
6. MSI should monitor, detect, and manage incidents for the following minimum set of network behaviour anomaly events:
    - Network Traffic Pattern Analysis and Bandwidth Analysis
    - Host behaviours and traffic analysis to identify threats
    - Analysis of traffic patterns & identify nonessential ports and services for normal business operations
    - Anomaly event as belonging to a class of security events (DDoS, Scans, etc.)

Apart from above security principles MSI has to abide Cyber security Principles as per details given below-

4.27.4 Cyber Security Principles

Cyber Security Principles is a set of simple but effective schemes that help to protect the organization. It is a starting point for implementing cyber security programs and to provide opportunity to benchmark against minimum set of cyber security controls.

Note: Entire cyber security setup shall be so robust that in case UP112 operations is switched to work from home setup the cyber security of operations in not compromised.

a. Software and Hardware Inventory

MSI has to provide an up-to-date list of all authorized software and hardware to be identified and maintained that is needed to run the business process of the UP112. MSI to ensure a secure and proper management of access control. It will also keep track of what software/ application is running on the hardware devices and helps to identify which device or hardware needs to be secured.

b. Administrative Privileges Management

MSI need to provide controlled access to data through accounts. Administrative privileges shall be given to authorized individuals only. User access applies to web and application servers, desktop and laptop computers etc. User accounts shall be given only as much access as needed to reduce the risk of information being stolen or damaged. A mechanism to track and log administrative as well as user access shall be maintained.

c. Secure configuration of Hardware and Software

MSI to ensure secure configuration practice of securely configuring devices to minimize risk. This is achieved by ensuring that systems have been correctly configured to mitigate vulnerabilities and that, thereafter, this is continually maintained. Securely configuring devices, software and hardware is vitally important as they ultimately dictate the risks the organization's information security system is exposed to. Secure configurations include blocking downloads, disabling unauthorized USBs, and blocking unreliable websites to reduce the risk of an employee mishap, patching, and updating firmware and software, hardening configurations by allowing only required services etc.

d. Malware Protection

MSI to ensure that no Malicious programs can be delivered physically to a system through a USB drive or other means, or via the Internet through drive-by downloads, which automatically download malicious programs to users' systems. Malicious websites and phishing – scam emails disguised as legitimate messages that contain malicious links or attachments – are two common delivery methods. Protecting against a broad range of malware (including computer viruses, worms, spyware, botnet software and ransomware) and including options for virus removal will protect the computer, privacy, and important documents from attack in an organization. Various mechanism like antimalware software, application whitelisting etc. will be deployed to detect and counter spreading and executing of malware in a network. Organization should be aware about malware, its malicious activities and its impact and shall implement the controls for secure and safe business process.

e. Vulnerability Management

MSI to ensure Vulnerability management process of identifying, categorizing, prioritizing, and resolving vulnerabilities in operating systems (OS), enterprise applications (whether in the cloud or on-premises), browsers, and end-user applications. It's an ongoing process, vulnerability management seeks to continually identify vulnerabilities that can be remediated through patching and configuration of security settings. Organization should implement vulnerability management by

i. Understanding its current IT environments by tracking hardware and software assets, including current versions and applied patches.
ii. Set standards for the hardware and software components that is used to avoid creating unnecessary vulnerabilities.
iii. Stay up to date of newly identified vulnerabilities in the hardware and software products that is going to be used.
iv. Continuously monitor IT environments to identify vulnerable assets and avoid re-introduction of known vulnerabilities.

f. Patch Management

MSI to ensure Patch management on all IT assets up to date and capable of resisting low-level cyber-attacks. Prompt patching is essential for effective cyber security by an organization.

g. Cyber incident prevention strategy in UP112

i. Identification of CISO from one of the SOC expert

MSI need to adhere as per the guidelines released by National Critical Information Infrastructure Protection Centre (NCIIPC) under Ministry of Electronics and Information Technology (MeitY), the organization having 'Protected System' shall nominate an officer as Chief Information Security Officer (CISO) with roles and responsibilities as per latest "Guidelines for Protection of Critical Information Infrastructure" and "Roles and Responsibilities of Chief Information Security Officers (CISOs) of Critical Sectors in India" released by NCIIPC.

ii. Information Security Policy and Implementation of Best Practices

UP112 shall define Information Security Policy at organization level and identify appropriate information security management practices keeping in view their business needs. MSI should implement the policies as per ISO 27001

iii. Business Continuity Plan (BCP) & Disaster Recovery Plan (DRP)

Business Continuity Plan (BCP) i.e., contingency plan is a plan framed to counteract interruptions to business operations/activities and protect critical operations/business processes from effect of major disaster.

Both Business Continuity Plan (BCP) & Disaster Recovery Plan (DRP) are proactive measures that will assist UP112 in preparing for unexpected, catastrophic situations.

Rather than reacting to a disaster, both disciplines take a proactive approach, attempting to mitigate the consequences of a disaster before it occurs.

Both can be used by UP112 to prepare for a variety of natural and man-made disasters. Prepare for pandemics, natural disasters, wildfires, and even cyberattacks with business continuity and disaster recovery.

iv. Security of Informational Infrastructure, Network & Applications

MSI to ensure that all the servers, Local Area Network (LAN), Wide Area Network (WAN) in all the IT infrastructures deployed in the project will be secured by installing appropriate perimeter security devices such as Firewalls, Anti-Virus software etc.

The various actions taken by MSI for IT infrastructure security are: -

1. Providing Firewall: IT systems need to be equipped with two different layers of firewall i.e., External & Internal Firewalls. They should be equipped with the Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to meet the cyber security requirements.
2. Secured Internet connection for IT systems to be provided for accessing the web-based applications hosted at UP112 Data Centre, such as antivirus update & patch management.
3. Regularly monitoring the logs & traffic on Firewall so as to mitigate the possible external cyber-attack. The firewall policies shall also be reviewed on a regular basis. Any flooding attempts need to be regularly monitored and analysed initiating necessary preventive measures.
4. Providing Routers: This shall be Layer-3 security device which will be used to connect multiple systems in different networks.
5. Providing Antivirus and anti-spyware software: In UP112 servers and consoles, the licensed antivirus need to be installed. The antivirus shall be scheduled to run automatically on predefined periodic basis. Further the antivirus patches should also be updated on a regular basis. The antivirus management in these systems will be the responsibility of the MSI.
6. Setting up Virtual Private Network (VPN) site-to-site: The site-to-site VPN setup need to be done to facilitate users at contact centres of UP112 to access servers and resources at remote site.
7. MSI need to ensure that based on the input from UP112, project manager, Network Admin department interacts with team to establish VPN.
8. Providing LAN IP Address Management: - MSI need to use Class IPv4 address pool for its connectivity requirements.
9. Process of Adding/Deleting Network: For any network addition and deletion Initiator will discuss with Network/System Admin and take approval of head of IT department in consent with UP112 department. Such changes will go through defined change management Process.
10. Implementation of application security controls for web and mobile applications: Proper handling of mobile devices and portable storage devices is the responsibility of all MSI, including consultants,

contractors, and temporary employees. All authorized staffs are responsible for protecting mobile devices from physical security threats.

11. Secure Application Development: As per the contractual agreements with the OEMs of various IT infrastructure deployed at UP112, the MSI needed to ensure for applying security checkpoints and techniques at early stages of development as well as throughout the software development life cycle. Special emphasis is given to the coding stage of development. Security mechanisms including threat modelling, risk analysis, static analysis, digital signature etc. are deployed. Further the application design and development of the system are ensured to comply as per policy and regulation mentioned in the contract agreement.
12. MSI to ensure security assessments of any system, cyber audit of all the IT systems is to be strictly conducted before the final deployment of such system on production. Any vulnerability observed is to be taken care before taking over of IT system.

v. Risk Identification & Evaluation

MSI need to carry out Risk identification on regular intervals. For each identified risk, an official shall be identified as the risk owner, who will be responsible for the system /process. The Risk Matrix in accordance with ISO:31000 shall be developed by MSI for each vertical function and should be approved by UP112 department. The Risk Matrix must be reviewed at least once every year, and on every such occasion when there are major changes in the function/ infrastructure. Residual risks after risk treatment through identified control mechanisms, which are beyond the organization's policy sanctioned risk tolerance level, should be approved by the department.

vi. Network Traffic Scanning

MSI need to perform the network traffic scanning which provides visibility into the state of the network and identifies deviations from baselines that may indicate abnormal or suspicious behaviour. The traffic patterns provide leads on the targeted ports which gives leads to attack targeted on the services like HTTP, SMTP, FTP or spread of malicious code like Bots.

MSI need to implement following measures: -

1. Monitoring of traffic on ports through firewall logs. The network traffic flow gives the exact portrait of the communications happening on the network, irrespective of their state whether normal or anomaly. Majority of attacks such as Distributed Denial of service (DDoS), Worm, Spyware, Botnet detection, malicious scan of any nature etc. at the organization level could thus be detected by analysing network flow-data traffic.
2. Any unused network services or ports or applications should be removed or disabled. Unused applications are often used to attack firewalls because many administrators neglect to implement default-restrictive firewall access controls. In addition, unused network

services and applications are likely to run using default configurations, which are usually much less secured than production-ready application or service configurations.

3. The default policy for the firewall for handling inbound traffic should be to block all packets and connections unless the traffic type and connections have been specifically permitted. This approach is more secure than another approach used often: permit all connections and traffic by default and then block specific traffic and connections.
4. Any protocol and traffic that is not necessary, i.e., not used or needed by the organization and/or denied by policy, should be blocked via use of a boundary router and packet filtering technology. This will result in reduced risk of attack and will create a network environment that has less traffic and is thus easier to monitor.
5. The following types of network traffic always should be blocked:
    - Inbound traffic from a non-authenticated source system with a destination address of the firewall system itself.
    - Inbound traffic with a source address indicating that the packet originated on a network behind the firewall.
    - Inbound traffic from a non-authenticated source system containing SNMP (Simple Network Management Protocol) traffic.
    - Inbound or outbound network traffic containing a source or destination of 0.0.0.0.
    - Inbound or outbound traffic containing directed broadcast addresses.

vii. Implementation of Security Guidelines

MSI has to adhere the Cyber security guidelines that are being issued by Ministry of Electronics and Information Technology (MeitY) & CERT-In on regular basis regarding the possible vulnerabilities and cyber threats in the Operating system, various installed software etc. and the actions that should be taken to mitigate those vulnerabilities. MSI need to regularly abide by the guidelines issued by the MeitY & Cert-In & takes corrective actions accordingly as per the guidelines.

viii. Cyber Security Audit

MSI shall undertake comprehensive security audit of the entire IT infrastructure including network and applications by employing CERT-In certified agencies. Vulnerability Assessment & Penetration Test shall be carried out once every 6 months. Improvement in the security systems shall be caried out based on the observations & findings of these tests and documented accordingly.

The audit of the system will be undertaken at least once in a year and as and when any significant addition or alteration in respect of hardware, software, network resources, policies and configurations of systems will be found affected.

ix. Cyber Security Drill

MSI need to conduct cyber security mock drill exercises. MSI shall execute different scenarios during the cyber security exercise & focus on assessing effect on critical systems and data that will have an impact on the operations of Project.

The various objectives of conducting Cyber Security Mock Drill are as under:

1. Determining effectiveness of the cyber education or training provided to the UP112 officials.
2. Assess ability of the training audience to detect and properly react to hostile activity during the exercise.
3. Assess the UP112's capability to determine operational impacts of cyber-attacks and implement proper recovery procedures for the exercise.
4. Understanding the implications of losing trust in IT systems and capture the work-around for such losses.
5. Expose and correct weaknesses in cyber security systems.
6. Expose and correct weaknesses in cyber operations policies and procedures.
7. Determine what enhancements or capabilities are needed to protect an information system and provide for operations in a hostile environment.
8. Enhance cyber awareness, readiness, and coordination.
9. Develop contingency plans for surviving the loss of some or all IT systems.
10. MSI shall regularly conduct Cyber Security Mock Drill once in every quarter for all the IT systems. Observations during the drill shall be documented and corrective action shall be taken based on the experience during the drill.
11. MSI shall also regularly practice the cyber security mock drills conducted by organizations like CERT-In/NCIIPC etc.

x. Coordination and incidents information sharing

MSI should strive to improve coordination and communication with CERT-In, Ministry of Home Affairs and other designated agencies and should share all information pertaining to cyber security incidents with CERT-In.

h. Key Cybersecurity Activities and Periodicity

List of key activities and project work products as part of this engagement:

S.No.	Deliverables	Periodicity
1.	Developing & Implementing the Information Security Management System (ISMS) Policies & IT Standard Policy Audit	Yearly
2.	Security audit of IT infrastructure (Vulnerability Assessment and Penetration Testing)	Half Yearly
3.	Secure Configuration Review of IT Infrastructure	Half Yearly
4.	Cyber Security Crisis Management Plan	Once/To be updated yearly
5.	Cyber Security Standard Operating Procedure (SOP) Document	Once/To be updated yearly
6.	Cyber Mock Drill	Half Yearly

i. Required IT Security Tools and Solutions

Following are the key features of the required cyber security tool and solution while details are provided in technical specifications as per TRS document

1. **Anti-APT (Advance Persistent Threat)**

   The term Advanced Persistent Threat (APT) refers to a potential attacker that has the capability and the intent to carry out advanced attacks against specific high profile targets in order to compromise their systems and maintain permanent control over them in a stealthy manner. APT attacks often rely on new malware, which is not yet known to and recognized by traditional anti-virus products. Therefore, a range of new solutions (known as Anti-APT solutions), specifically designed to detect APT attacks, have appeared on the market in the recent past. It enables detecting attacker presence on the network with maximum speed and recreating a full picture for thorough investigation. Detects attackers both on the perimeter and inside infrastructure. Automatically identifies previously unknown hacks.

2. **Endpoint Detection & Response (EDR)**

   It offers a capability that fits with the detection - mitigation model of modern cybersecurity. Indeed, EDR solutions continuously monitor all files and applications entering your enterprise's endpoints. Additionally, EDR solutions can offer granular visibility, threat investigations, and detection of fileless malware and ransomware. Also, EDR provides your investigation teams with alerts for easy potential threat identification and remediation.

3. **Patch Management Solution**

   Patch management is the process of distributing and applying updates to software. These patches are often necessary to correct errors (also referred to as "vulnerabilities" or "bugs") in the software. Common areas that will need patches include operating systems, applications, and embedded systems (like network equipment). When a vulnerability is found after the release of a piece of software, a patch can be used to fix it. Doing so helps ensure that assets in your environment are not susceptible to exploitation.

   The number of ransomware attacks is rapidly increasing with each passing day. For organizations with multiple servers and computers, ensuring that all of them are updated can be both time-consuming and challenging. Trying to manually manage these patches is not only hectic but also a major risk for businesses. So, patch management tool provides an automated patch management system which frees your IT administrators from the routine work of manually patching computers, so they can focus on other critical tasks.

4. **SOAR Threat Intelligent Platform**

   SOAR (Security Orchestration, Automation, and Response) refers to a collection of software solutions and tools that allow organizations to streamline security operations in three key areas: threat and vulnerability management, incident response, and security operations automation. To break it down further, security automation is the automatic handling of security operations-related tasks. It is the process of executing these tasks—such as scanning for vulnerabilities or searching for logs—without

human intervention. Security orchestration refers to a method of connecting security tools and integrating disparate security systems. It is the connected layer that streamlines security processes and powers security automation.

5. **DDoS Protection Solution**

   A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

   DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices. A successful distributed denial of service attack is a highly noticeable event impacting an entire online user base. This makes it a popular weapon of choice for hacktivists, cyber vandals, extortionists, and anyone else looking to make a point or champion a cause. To truly protect against modern DDoS attacks, we should use a DDoS mitigation solution. Solutions can be deployed on-premises but are more commonly provided as a service by third-party providers.

   We would need DDoS protection solution that mitigates large-scale DDoS attacks quickly, without disrupting service to legitimate users. It should provide protection for websites and web applications, networks and subnets, domain name servers (DNS), and individual IP addresses.

6. **Intrusion Prevention System (IPS)**

   An intrusion prevention system (IPS) is a network security tool (which can be a hardware device or software) that continuously monitors a network for malicious activity and takes action to prevent it, including reporting, blocking, or dropping it, when it does occur.

   It is more advanced than an intrusion detection system (IDS), which simply detects malicious activity but cannot take action against it beyond alerting an administrator. Like many network security technologies, they must be powerful enough to scan a high volume of traffic without slowing down network performance. Once the IPS detects malicious activity, it can take many automated actions, including alerting administrators, dropping the packets, blocking traffic from the source address, or resetting the connection.

7. **Web Application Firewall (WAF)**

   A WAF or web application firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others. A WAF is a protocol layer 7 defence (in the OSI model) and is not designed to defend against all types of attacks. This method of attack mitigation is usually part of a suite of tools which together create a holistic defence against a range of attack vectors.

   By deploying a WAF in front of a web application, a shield is placed between the web application and the Internet. While a proxy server protects a client machine's identity

by using an intermediary, a WAF is a type of reverse-proxy, protecting the server from exposure by having clients pass through the WAF before reaching the server.

8. **Next Generation Firewall (NGFW)**

   A next-generation firewall (NGFW) is a network security device that provides capabilities beyond a traditional, stateful firewall. While a traditional firewall typically provides stateful inspection of incoming and outgoing network traffic, a next-generation firewall includes additional features like application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence. A traditional firewall provides stateful inspection of network traffic. It allows or blocks traffic based on state, port, and protocol, and filters traffic based on administrator-defined rules.

   In addition to access control, NGFWs can block modern threats such as advanced malware and application-layer attacks. According to standard definition, a next-generation firewall must include:

   - Standard firewall capabilities like stateful inspection
   - Integrated intrusion prevention
   - Application awareness and control to see and block risky apps
   - Threat intelligence sources
   - Upgrade paths to include future information feeds
   - Techniques to address evolving security threats

9. **VAPT Tools/Solutions**

   Vulnerability Assessment and Penetration Testing (VAPT) is a process of securing computer systems from attackers by evaluating them to find loopholes and security vulnerabilities.

   Some VAPT tools assess a complete IT system or network, while some carry out an assessment for a specific niche. As we become increasingly reliant on IT systems, the security risks are also increasing both in terms of quantity and scope. It has become mandatory to proactively protect important IT systems so that there are no data security breaches. Penetration testing is the most useful technique adopted by companies to safeguard their IT infrastructures.

10. **Security Information & Event Management (SIEM)**

    SIEM stands for security information and event management and provides organizations with next-generation detection, analytics, and response. SIEM software combines security information management (SIM) and security event management (SEM) to provide real-time analysis of security alerts generated by applications and network hardware. SIEM software matches events against rules and analytics engines and indexes them for sub-second search to detect and analyse advanced threats using globally gathered intelligence. This gives security teams both insight into and a track record of the activities within their IT environment by providing data analysis, event correlation, aggregation, reporting and log management.

    SIEM software can have a number of features and benefits, including:

    - Consolidation of multiple data points
    - Custom dashboards and alert workflow management

- Integration with other products

11. Endpoint Security (Antivirus)

Endpoint security is the practice of securing endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices from being exploited by malicious actors and campaigns. Endpoint security systems protect these endpoints on a network or in the cloud from cybersecurity threats. Endpoint security has evolved from traditional antivirus software to providing comprehensive protection from sophisticated malware and evolving zero-day threats. Endpoint security is often seen as cybersecurity's frontline and represents one of the first places organizations look to secure their enterprise networks.

12. Network Access Control (NAC)

Network access control, or NAC, solutions support network visibility and access management through policy enforcement on devices and users of corporate networks. A NAC system can deny network access to noncompliant devices, place them in a quarantined area, or give them only restricted access to computing resources, thus keeping insecure nodes from infecting the network.

NAC solutions help organizations control access to their networks through the following capabilities:

- Policy lifecycle management: Enforces policies for all operating scenarios without requiring separate products or additional modules.
- Profiling and visibility: Recognize and profiles users and their devices before malicious code can cause damage.
- Guest networking access: Manage guests through a customizable, self-service portal that includes guest registration, guest authentication, guest sponsoring, and a guest management portal.
- Security posture check: Evaluates security-policy compliance by user type, device type, and operating system.
- Incidence response: Mitigates network threats by enforcing security policies that block, isolate, and repair noncompliant machines without administrator attention.
- Bidirectional integration: Integrate with other security and network solutions through the open/RESTful API.

13. Identity and Access Management (IAM)

Identity and access management (IAM) ensures that the right people and job roles in your organization (identities) can access the tools they need to do their jobs. Identity management and access systems enable your organization to manage employee apps without logging into each app as an administrator. Identity and access management systems enable your organization to manage a range of identities including people, software, and hardware like robotics and IoT devices.

With an IAM framework in place, information technology (IT) managers can control user access to critical information within their organizations. Systems used for IAM include single sign-on systems, two-factor authentication, multifactor authentication, and privileged access management. These technologies also provide the ability to

securely store identity and profile data as well as data governance functions to ensure that only data that is necessary and relevant is shared.

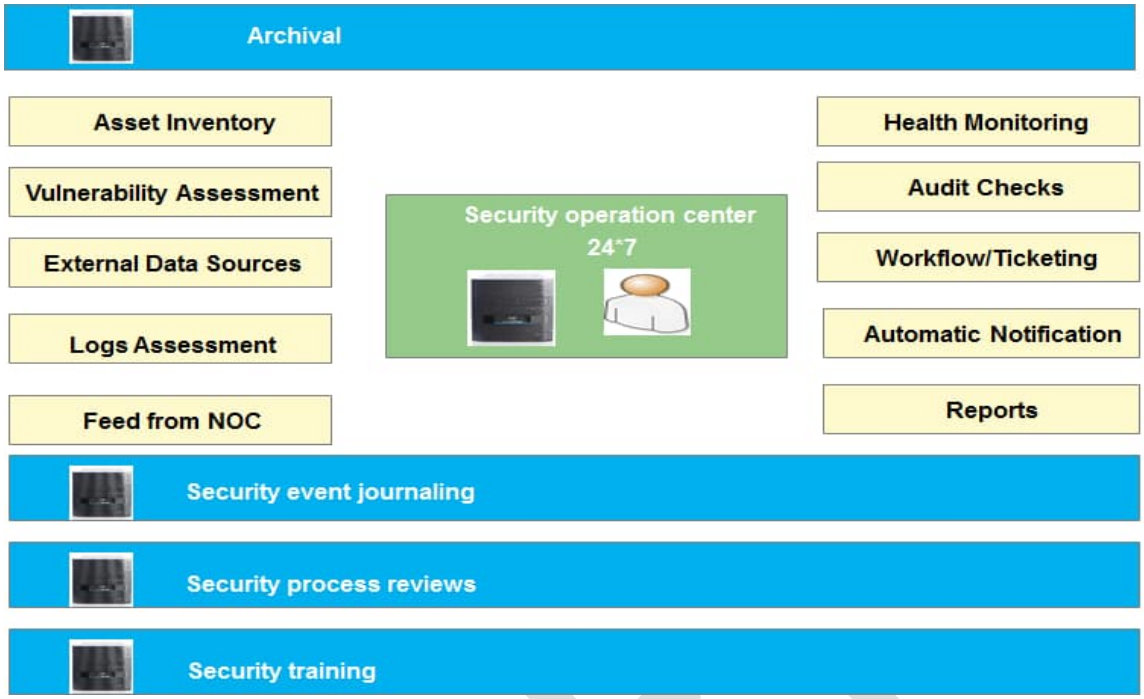
14. Cloud Security

MSI has to ensure, Cloud Service Provider must provide native service for security mentioned below but not limited to-

1. Identity & access management
2. Manage user access and encryption keys
3. Single Sign on Service for Cloud
4. Centralize Governance and Compliance Management
5. Detection Control
6. AI Powered Threat Detection Service
7. Unified Security and Compliance Dashboard
8. Vulnerability Assessment
9. Record and Evaluate Configuration
10. Track API and User Activity
11. Infrastructure Protection
12. Network Firewall with IPS capability
13. Web Application Firewall
14. DDoS protection
15. Central Management of Firewall Rules
16. Data Protection:
17. Sensitive Data Discovery and Protection
18. Encryption Key storage and Key Management (FIPS compliant)
19. FIPS Compliant Fully managed scalable Hardware Security Module
20. Centralize Provision, manage, and deploy public and private SSL/TLS certificates
21. Central Store to Encrypt, Rotate, manage, and retrieve secrets
22. HSM
23. Should support FIPS 140-2 Level 3 for the storage of encryption keys ssl certificates etc. as managed service
24. Should provide managed backup service for HSM Cluster
25. Incidence response
26. Potential Security Threat Investigating Control
27. Fast and Automated Control for Disaster Recovery and Ransomware Recovery.

In order to mange the security principles **Security Operation centre (SOC)** need to be establisted by MSI and below are the fuctionalities of SOC but not limited to-

a. Infrastructure security's objective is to prevent attacks from internal and external sources to all ICT asset part of the project. The SOC will be manned 24X7X365 for the duration of the contract. The main objective of the SOC is to ensure confidentiality and integrity of information assets.
b. The MSI needs to provide adequate IT infrastructure for all the persons manning SOC.
c. The indicative representation for the SOC with required minimum features:



d. Services to be provided through SOC

The Services procedures for the SOC has to be prepared by the MSI and get a sign off from UP112.

Indicative list of services that have to be provided through the SOC are mentioned below.

i. MSI shall supply of skilled manpower for Security Operations Centre (SOC) monitoring over a period of contract at the UP112 decided or approved location. MSI resources are expected to deliver SOC monitoring services including but not limited to performance monitoring, performance tuning, optimization, maintenance of SIEM tool, security monitoring, etc. The detailed SOC Reports formats will be discussed and finalized with the selected MSI.

ii. This SOC will help UP112 to monitor for security events throughout its network by analysis of logs from all servers, devices, and key applications in the Data Centers and other locations. The indicative security monitoring service will have following components but not limited to:

a. 24X7X365 security monitoring
b. Threat intelligence
c. Log collection and management
d. Event correlation
e. Rapid response to incidents and forensics
f. Patch Management
g. VA and PT Management
h. Perimeter Security Management

iii. MSI have to provide services for 24x7 monitoring of ICT Assets such as Operating systems, web servers, databases, network devices, MDTs (handheld devices in states), security devices and business applications, etc. The services will include review of the logs generated from servers and applications in real time to detect suspicious activities and potential attacks. Immediate response action will need to be initiated by the MSI to stop the attacks. MSI need to provide the services using the SIEM platform procured by UP112 and

through its dedicated personnel and processes based out of the Security Operations centre of UP112.

iv. MSI should monitor, detect, and manage incidents for the following minimum set of IT infrastructure security events. This is indicative minimum list and is not a comprehensive or complete set of events. MSI should indicate their event list in proposal response.
   a. Buffer Overflow attacks
   b. Port and vulnerability Scans
   c. Password cracking
   d. Worm or virus outbreak
   e. File access failures
   f. Unauthorized server or service restarts
   g. Unauthorized changes to firewall rules
   h. Unauthorized MSI access to systems
   i. SQL injection
   j. Cross site scripting

v. MSI operations team at UP112 should send alerts with details of mitigation steps to designated personnel within UP112 and any identified service provider.

vi. MSI should provide coordinated rapid response to any security incident. MSI should contain attack and coordinate restoration of services. While MSI personnel will enlist support of other departments and service providers in UP112, primary responsibility for incident response will be with the MSI.

vii. MSI should maintain a knowledge base of alerts, incidents and mitigation steps and this knowledge base should be updated with evolving security events within and outside UP112. Team should send customized alerts advisories to respected teams in UP112.

viii. Evidence for any security incident should be maintained in tamper proof manner and should be made available for legal and regulatory purposes, as required.

ix. MSI should add or delete or modify rules, reports and dashboards based on UP112 requirements

x. MSI should provide backend support to the onsite team from its own SOC. Such support at the minimum includes-
   a. Managing escalations from onsite team for detection and response to new threats and complex attacks that onsite team is unable to resolve.
   b. For adding new or updated threat scenarios and other best practices in UP112 SIEM tool for detection and response based on MSI SOC visibility
   c. Analysis of attacks or incidents including making available specialists, domain experts, tools.

xi. MSI should identify threat and incident patterns and devise mitigation plans for the same to facilitate Threat intelligence.

xii. MSI should facilitate Threat Intelligence by regularly updating the knowledgebase of personnel by providing access to various sources (OEM based, cloud based, govt. portals etc.) containing updated information pertaining to new threats, attacks, malwares, etc.

xiii. MSI has to perform Web Application based vulnerability assessment: provide proper evaluation of security vulnerabilities associated with web applications

xiv. MSI has to perform OS level vulnerability assessment: provide proper evaluation of security vulnerabilities associated with operating systems

xv. MSI has to perform Database Vulnerability assessment: provide proper evaluation of security vulnerabilities associated with database, thereby, recommend solutions to problems. Vulnerability Assessment will include checks like Port scan, unnecessary or

vulnerable services, file permission, user access control, password protection, system vulnerability etc.

xvi. The MSI has to be provision for authenticated mode VA. This will include assessment by providing credentials of assets in the VA process.

xvii. MSI has to perform Android/iOS/Windows Vulnerability Assessment – The MSI shall provide the facility of Vulnerability Assessment of Android platform that will be running on the MDTs and smartphones.

xviii. MSI has to perform Penetration Testing, the Penetration Testing will include activities but not limited to the test should simulate activities in conjunction to IT Act, National Cyber Security Policy and Cert-In guidelines. These activities should be carried by an expert team, who bear certified by industry recognized bodies. These activities should identify specific exploitable vulnerabilities and expose potential entryways to vital or sensitive data. The results should clearly articulate security issues and recommendations and create a compelling event for the entire management team to support a security program. A complete project-based approach should be followed that covers areas including but not limited to the following:

a. Network Security
b. Network Surveying
c. Port Scanning
d. System Identification
e. Services Identification
f. Vulnerability Research and Verification
g. Application Testing and Code Review
h. Router Testing
i. Firewall Testing
j. Intrusion Detection System Testing
k. Trusted Systems Testing
l. Password Cracking
m. Denial of Service Testing
n. APT Testing

Penetration Testing shall be done for either sample of devices or all. The sample should be chosen in a way that one device from each of the device type is captured. The sample to be taken for assessment will be mutually discussed and agreed upon between UP112 and the successful MSI.

xix. MSI has to perform OS Hardening: OS Hardening will include activities but not limited to the removal of all non-essential tools, utilities, and services with other system administration by activating and configuring all appropriate security features. The entire scope of this service will differ on different Operating System basis.

xx. Secure Code Review: The MSI is required to provision for tools or software or hardware or appliance as a part of its technical solution to ensure quality.

xxi. Infrastructure Security Management: The MSI shall provide services (monitoring and management) for the following infrastructure systems related to information security. It should be noted that the activities performed by the MSI will be under the supervision of UP112.

xxii. MSI has to perform Firewall Monitoring and Management, and this will include-

a. Installation and maintenance of the firewall

b. Firewall Hardening with initial configuration
c. Performance Monitoring
d. Regular Monitoring of the LAN errors
e. Firewall Rule based policy changes
f. Create and maintain Network Access Policy (NAP) document (the access specification) agreed between the parties from time to time.
g. Log File review and analysis of information on traffic flow
h. Log File trend upgrade and analysis
i. Compliance Testing
j. Design, configure and maintain all Network Address Translation (NAT) services.
k. Access control management through creation of the Network Access Policy and firewall rules
l. Implementation and maintenance.
m. Manage access to F or W logs policies and performance statistics for viewing through secure web portals in conjunction with SOC tools
n. Manage the functioning of Regular Reports in conjunction with SOC tools so as to provide detailed auditing of configuration history and change of journals. Alerts include critical configuration changes, potential malicious activity, and operational alarms
o. Incidence response
p. Lifecycle Management of all Hardware and Software components
q. Firewall Backup

e. MSI has to perform Virtual Private Network Monitoring and Management which includes-
   a. Configuration and maintenance of the VPN gateway to meet customer's specific requirement of VPN - Client to Site and Site to Site.
   b. Monitoring of the local and remote VPN gateway availability
   c. Monitoring of the VPN tunnel availability through artificial traffic inside the VPN tunnel
   d. Monitoring of the VPN tunnel delays and detection of slow VPN connections
   e. Transparent VPN tunnel (virtual connection) between pairs of sites using technology specification
   f. Cryptographic services according to IPsec specification with strong encryption and pre-shared secrets authentication.
   g. Access control management through creation of the Network Access Policy and firewall rules

f. Patch Management: The MSI will be required to provide services related to Patch Management. The security administrators should be aware of security precautions in place in their environment. If they do not personally manage the company firewall, they should obtain configuration information from the firewall administrator. Ensure that there is available documentation as to what traffic is being allowed through to the internal network. This will help in the evaluation of threats posed by known vulnerabilities and assign a risk factor to them.

   Personnel designated to evaluate patch stability should have expertise in mission critical systems and be capable of verifying stability of systems after patch installation.

Before any patch is installed, a full backup of all data and server configuration information must be made. Best practices for disaster recovery recommend periodic testing of the restore process to ensure the integrity of the back-up data. The patch management should be executed efficiently for all kinds of environments like for operating systems and Data bases. The activities mentioned above are indicative in nature.

g. Key Management Service: Services to be delivered through the SOC would be the Key Management Service in which the generation, distribution and management of cryptographic keys have to be managed by the MSI and it should be only Tool based Key management

h. MSI has to provide Data Leakage Prevention Services: Key objectives to be achieved through this service are:
   i. Locate and record sensitive stored information.
   ii. Monitor and control the movement of sensitive information across the network.
   iii. Monitor and control the movement of sensitive information on end-user systems.

i. IT Infrastructure at the SOC
   a. The MSI has to ensure the proposed SOC services can be operated from SOC.
   b. MSI has to provide required Desktops with OS and other relevant software.
   c. MSI has to provide the required network connectivity to operate SOC.

j. MSI has to setup a Security management dashboard which will provide-
   a. MSI needs to provide a Security Management Solution Console for reporting all the SOC activities including incidents from HIPS, Firewall, SIEM, vulnerability scan reports, remediation process progress etc.
   b. This service will help UP112 to centralize the management of security products like SIEM, Firewall APT etc. and to have tight control on the security rules.
   c. The SIEM solution should provide dashboard functionality for all the above requirements.
   d. The dashboard solution should be on premise or cloud and not a hosted solution. There should be a feature to create any kind of report from any of the available data from the feeds like top incidents by application, by hosts, users etc.

4.27.5 Data architecture and requirements

UP112 system and its applications generate data from multiple sources and UP112 wants to use the power of data for optimization of system on continuous basis. Analytics and research centre (ARC) is envisaged in NexGen UP112 DRP to serve this purpose by generating insights on issues and discovering bottle necks. But for ARC to function well data shall be available in a form that insights, rich visualization, or useful reports can be generated. Accordingly, ARC wing is expected to use all the possible data analysis, business intelligence and data science techniques to serve its developed for availability of data in both the data environments, post logical integration of all the data sources.

UP112 has multiple applications such as CTI, Biometric Attendance System, LBS etc., as its backbone to support its operations. In current stage data from these applications

are available and integrated to provide event related details. However, vision is to create a Datawarehouse through which holistic 360-degree view of complete NexGen UP112 can be obtained for decision making by UP112. Thus, MSI shall:

1. **Determine the list of possible integrations:**
   The system shall be flexible enough to add any data source in the ecosystem such as IP PBX, Outbound Dialler, ACD, CTI, Multimedia System, Core CAD, Mobile CAD, Supervisory APP, Web and Desktop Application, UP112 Portal, EMS, MDM, Inventory Management S/w, Human Resource Management S/w, Biometric Attendance, Patrol Management System, Fleet Management Solution, GIS Application, GIS Map Geo-Fencing Process, GIS Data Capturing Mobile Application, LBS (Location Based Services), Auto Arrive, Geo Fencing of PRVs, Vehicle Tracking System, PRV Location Tracking by Citizen, ELS/ALS, Identity Management Software (IMS)
2. **Design the Dimensional Model:**
   The dimensional model must address the needs of the UP112 leadership, and it must contain information that is easy to access. The model should be designed to allow for future scalability.
3. **Design Data Warehouse Schema:**
   MSI shall provide the structure of schema, whichever makes querying data easier. Some of the most popular schemas used for the development of a dimensional model are Star Schema, Snowflake Schema, Distributed Star Schema, etc.

   a. Data Management Approach

      i. MSI has to ensure that all the master data generated from applications (business process) is available for Data warehousing. This data shall be later available for business intelligence and reporting

      ii. MSI has to ensure that multiple environments are available in the system such as production and development environment

      iii. A regular data refresh mechanism shall be established to ensure availability of data at both the environments (production and development environment)

      iv. Availability of source data at Datawarehouse should be in near real time basis

      v. MSI has to ensure system is scalable enough at all the levels for the entire duration of project

      vi. MSI has to ensure that at staging level that is before Data warehousing stage ETL (Extraction, Transformation and Loading) process is well defined and customisable with complete flexibility to perform CRUD (Create, read, update, and delete) operations in development environment and read access in Prod environment.

vii. MSI has to ensure that Datawarehouse is capable to handle raw and unstructured data

viii. MSI's deployed system shall be able to provide drill down and drill up functionality till lowest and highest granularity level

ix. All current and historical data of the existing UP112 system shall be migrated to NexGen UP112 with due audit checks/ verifications and reconciliation. The MSI should chalk out a proper data federation policy in this regard.

x. All the historical data of UP112 shall be saved and NexGen UP112 data shall be available in archive whereas data shall be readily available on primary storage for 6 months.

xi. MSI to ensure complete data mapping along with Metadata

xii. MSI shall identify various data sets available with ITECCS and detect issues in data quality, if any, and shall also perform the cleaning/ reformatting of data in consultation with ITECCS

xiii. The MSI shall be required to create ingestion streams of data into Datawarehouse to populate required schemas.

xiv. Any incremental data from the data sources shall be streamed into Datawarehouse and reconciliation of data between data marts/ source/ stores and Datawarehouse and vice-versa shall be the responsibility of the MSI.

xv. The MSI shall be required to provide for data exchange mechanisms like API/ web services, SFTP/FTP etc. MSI shall ensure that data to be acquired from external regulators/ any other source (*as defined under section Integration with Other Agencies section number 4.27.10*) as specified by ITECCS shall be managed through the system using various methodologies such as SFTP, FTP, API etc.

xvi. Provisions shall be made for secured data exchange and the confidentiality of the data shall be maintained, and the data shall be made available to only designated users as per the requirements of ITECCS

xvii. Data ingested shall be formatted and transformed in a form where the data can be exported in leading formats like JSON, CSV, MS-Excel etc.

xviii. The MSI shall be required to design a strategy for on-demand ETL and provision for the required infrastructure and solution for this bulk data exchange.

xix. Appropriate storage solution shall be provided by the MSI to export the data from the system and stored in a repository from where the external agencies would collect the data required by them.

xx. ITECCS data is required by a lot of external agencies and regulators, wherein a huge amount of data exchange both for import and export would

be required. Data import would include both structured and unstructured data from multitude of heterogeneous sources. This data exchange has to be streamlined and homogenized for populating the raw data in data lake.

xxi. The solution should provide user with an option to export data to internal or external stakeholders with appropriate filters built-into the system.

xxii. MSI to ensure the implementations of concepts Slow Changing Dimensions 2 or 3 (SCD 2 or 3) in datasets such as CO, PRV Staff etc (wherever applicable).

b. Data entity, structure, and flow

The data structures used, and the data flow diagram components highlighted below give an overview of the collection processing system and ETL processes. The various layers of the data flow are:

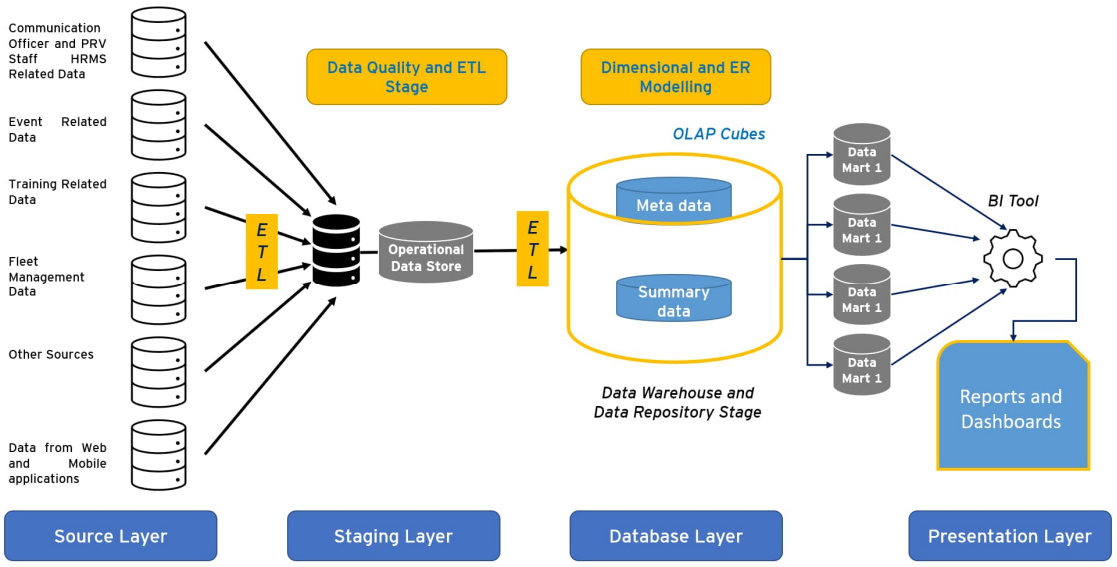
i. **Source Layer** consisting primarily of data which is generated by various modules of UP112 system such as CTI, Communication Officer Related Data, CAD Data, Training Related Data, Fleet Management Data, PRV staff related HRMS Data and data from other agencies.

ii. **Staging Layer** consists mainly the staging repository for DataStage and Quality Stage which is used for ETL, data standardisation, de-duplication and transformation into Universal Message Format. Following activities shall be performed in this stage

1. Integrate data from the widest range of application and external data sources
2. Data validation rules implementation
3. Processing and transforming large amounts of data
4. Scalable parallel processing approach
5. Handling of complex transformations and multiple integration processes
6. Leverage direct connectivity to enterprise applications as sources or targets
7. Leverage metadata for analysis and maintenance

iii. **Database layer** consisting of the applications database and data stage repository for entity and relationship resolution and modelling. The entity and relationship data is also made available at the staging layer to improve validations, cleansing and standardisation rules.

iv. **Presentation layer** for data mining, case management and generation of MIS.



c. Historical Data Processing

i. All processes from cleaning the data to entity and relationship resolution shall be carried on as a part of the historical data processing activity.

ii. The process shall include reprocessing of entire historical data including data validation, cleansing and standardisation. Verification and redevelopment of linkages including identities and relationships shall also be done and the confidence level should be displayed by the envisaged system.

iii. The MSI must provision hardware and software in accordance with the volume of data to be reprocessed. The new system shall be accepted by ITECCS only when 100% historical data is re-processed, validated and sign offs is obtained.

iv. The new system shall maintain all old data and events, including the relationships which were identified.

d. Entity and Relationship Resolution tool

The solution should access, store, and analyse structured and unstructured purpose.

Thus, MSI is expected to take all relevant steps to ensure that a data pipeline are

i. data from various sources.

ii. The solution should be able to classify the entities into same, similar, or different clusters.

iii. The solution should create and update ontologies defining the entities, their attributes, and their relationships.

iv. The solution should also have the ability to add more links to the existing relationships and de-link the disjoin matches (manually or rule based)

v. The solution should be able to receive search requests and provide search results from other applications through APIs.

vi. The MSI shall specify the processing capacity of the solution proposed in the technical proposal itself. The MSI shall maintain the system's minimum throughput at this level.

e. Solution for Extract, Transform, Load tool (ETL)

i. The solution shall have the facility to extract data from multiple data sources, transform the data to make it accessible for analysis, and load the same to multiple target(s) if needed. The solution should allow for bulk movement of data to the server storage and the database.

ii. The solution should have the facility to configure ready to use library of transformation routines such as data type conversions such as string to numeric, numeric to string, other string manipulations and simple calculations.

iii. The solution should provide the facility for error handling and reporting through alerts for the likes of data related errors and tool related errors producing an event log containing information like time/status of operation/reason for failure etc.

iv. The solution should also have the following functionalities

1. Generate output files in multiple formats
2. Capability to secure sensitive data by data masking techniques / algorithms to facilitate development and testing efforts without compromising data security
3. Facility to log and notify the designated users by email on the status of various processing such as data extraction, transformation, validation, enrichment etc.

v. The solution should have the facility for an administrative console having a visual end to end process designer with Visualisation and viewing of metadata, tables and columns and records. **Note: Data cleansing and business rules shall be guided by UP112*

f. Data Aggregation (Data Sources and Data Mapping)

i. Indicative list of data types generated by UP112 system are given below:

Applications	Data Types									
	Caller Details	Location	Event Information	Dispatch Related Details	Fleet Related Data	Hardware Details	PRV Details	Closure	Feedback	HRMS
IP PBX	x									
IP Phone										x
Outbound Dialler	x									x
ACD	x		x						x	
CTI										
Multimedia System	x		x							
Core CAD	x	x	x	x	x		x	x	x	x
Mobile CAD	x	x	x	x	x		x	x	x	x
Supervisory APP	x	x	x	x	x		x	x	x	x
Web and Desktop Application	x	x	x	x	x		x	x	x	x
UP112 Portal	x	x	x	x			x	x	x	
EMS		x			x	x			x	x
MDM						x	x			x
Inventory Management S/w						x	x			
Human Resource Mgt S/w										x
Biometric Attendance										x
Patrol Mgt System		x		x	x		x			x
Fleet Management Solution				x	x		x			x
GIS Application		x								
GIS Map Data		x					x			
GIS Map Geo-Fencing Process		x					x			
GIS Data Capturing Mobile Application		x					x			
LBS (Location Based Services)	x	x								
Auto Arrive	x	x	x	x	x		x			
Geo Fencing of PRVs		x			x		x			
Vehicle Tracking System		x			x		x			x
PRV Location Tracking by Citizen		x					x			
ELS/ALS	x	x								
Identity Management Software (IMS)										x

Data type details (non exhaustive list)

Data Types	Details						
Caller Details	Caller No	Operator	Location	Address	Mobile Number	Event Type	Event Details
Location	LBS Location of Caller	Location of PRV					
Event Information	Event Type	Event Details	Event Severity	Event Location			
Dispatch Related Details	PRV	Latitude and Longitude	Time Stamping	Relevant RMO	Relevant ES		
Fleet Related Data	Vehicle Number	Vehicle Type (2W/4W)	Last Service Date	Next Service Date	Deployment Date	Tagged Fleet Staff	List of Available in fleet components
Staff Details	Tagged vehicle number	Staff Name	Deployment Date	Last Training Date	Next Training Date	Last Type of Training	Next Training
Closure	ATR	Disposition code	Event closure location	Recommended changes in details of event			
Hardware Details	Hardware Id	Hardware Type	Hardware Location	Hardware Utilization	Hardware Uptime		
Staff Details	Name	PNO Number	Date of joining	Location	Training	Role	
PRV Details	PRV Id	Procurement date	Deployment Date	Last Service Date	Next Service Date	Location	Tagged Staff
Feedback	Citizen Feedback Details						
HRMS	Resource Name	Resource Deployment Date	Role	Resource Designation	Biometric Details		

ii. Note: There might be applications not mentioned in summary but MSI has to ensure that all the applications are well integrated in compliance with best industry practise of data modelling and data warehousing. These data may

include flat files, logs or data from other agencies integrated with UP112 during the course of time (defined under clause 4.27.10).

g. Data warehousing and Analytics component

i. The data warehousing platform should have the capability to handle incremental load at various frequencies (daily, monthly, real time etc.)

ii. The data warehousing platform should have the ability to understand, map and define rules for migration from different sources.

iii. The proposed solution should have data quality and data profiling capacities.

iv. Data cleansing techniques should be included to clean data at all levels.

v. The tool should be capable to handle Extraction, Transformation and Loading (ETL) of both structured and unstructured data from various data sources.

vi. The data warehousing landscape should be capable of handling large volumes of data.

vii. The proposed solution should create a single source of truth by integrating disparate data from multiple sources thus this single source of truth shall be useful for data analysis.

viii. The proposed solution should have the capability of enterprise grade ETL operations from a large array of traditional and non-traditional data sources and should have high performance transformation capabilities.

ix. The proposed solution should allow for connectivity with proposed database. Compatibility to operating system(s) proposed in the solution is must.

h. Securing Data at Rest

The security for the transactional data stores should be ensured by vertical partitioning of the data in different shards to maintains its security and sanity

i. Data governance

MSI shall provision for a solution required for governance and meta data management which shall perform the tasks like (but not limited to) organize, monitor, track data sets, user roles and access definitions.

i. It shall also allow to define the security and privacy policies and provide security and compliance reports to ITECCS.

ii. Data governance model should be adaptable for managing the quality, consistency, reliability, usability, security, data integrity and availability of the solution. Framework could be suggested along the broad areas highlighted below:

1. Data quality
2. Data ownership
3. Data integrity
4. Security and privacy

5. Metadata management
6. Data integration

iii. MSI shall be required to perform Master Data Management (MDM) for ITECCS system throughout the tenure of the project. Some of the key requirements for MDM (but not limited to):
   1. Create a master and maintain a single source of truth data as data may be ingested from multiple sources. This would require reconciliation/ resolution of differences in attributes for both master and transactional data
   2. Maintain masters for reporting and analytics
   3. Shall be capable of resolving multiple instances of the same entity with attribute variations into a single entity using defined resolution rules. The resolution rules can be both probabilistic and deterministic to resolve

j. Backup and archival management
   i. MSI shall implement solution for backup and archival of ITECCS data. The policies shall be finalized by the MSI in consultation with ITECCS. The storage policies of MSI shall be finalized prior to installation and commissioning of the backup and archival solution.
   ii. MSI shall be responsible for managing and monitoring the performance of periodic backups, testing of data backups and adherence to retention policies
   iii. MSI shall ensure that real-time monitoring, log maintenance and reporting of backup status on regular basis. MSI shall ensure availability of administrators and other resources as required for successful and prompt backup as per define policies
   iv. In case of any failure in the backup process, MSI shall ensure prompt resolution to the problems as per defined SLAs
   v. Any media management tasks required for successful management of backups shall be undertaken by MSI including but not limited to tagging, cross referencing, storing, logging, testing, and vaulting in fireproof cabinets (as per requirement of ITECCS)
   vi. MSI shall also provide 24x7 support for file and volume restoration requests at the Data Centres
   vii. The proposed Backup Appliance/ *solution* shall have built-in data security component against ransomware, malicious threats, and attacks *either as a built-in component or add-on using suitable security solution.*

k. Database Security Solution
   i. The solution should be able to protect the database from all threat vectors to meet regulatory compliance requirements. It should be able to provide visibility into all database activity, including from across the network, from local users logged into the server itself, and even from inside the database itself via stored procedures or triggers.

ii. The solution should be able to discover all the supported database in the environment and have the ability to identify sensitive information contained in them
iii. The solution should have the ability to monitor database activities from users connecting through encrypted connections.
iv. The solution should support applications which have pooled connections. The original IP address and username should be monitored.

l. Data Leakage Prevention (DLP)

i. The solution deployed for DLP should have the ability to identify
    a. Data-in-motion
    b. Data-in-use
    c. Data at rest
ii. The solution should support scanning of the database(s).
iii. In case of emergency issues related to infrastructure (Hardware, Software) remote access to the components may be provided only after due approval from UP112. Such access shall be used only for the purpose of accessing logs and not for any application related data. MSI will monitor such remote access and certify no access /leakage of data to any remote location.

m. Data Integrity

Data in transit (from external systems or between internal systems) or data at rest must be protected from tampering. The risk may be from both external users and internal users (such as database administrators) who are always close to the data. NexGen UP112 shall ensure to validate integrity using the checksum and digital signature validations before processing the data. To handle the risks of data being tampered by the internal users such as DBA who have access to data, the envisaged system shall be designed with the below principles

n. Data Confidentiality

To ensure data is securely accessed only by required teams and applications, the following principles are to be adhered

i. All the databases must be accessed by individual user accounts and user accounts cannot be shared by multiple persons or as a team-based accounts. All accounts should uniquely identify individuals and access to be provided to limited/authorised users only. The access policy shall be finalised in consultation with UP112 Leadership team.
ii. All the databases/systems must be integrated with the Identity Access Management system for centralised control. This should also enable disabling of user accounts when a person leaves the organisation.

iii. For reporting purposes, the data must be anonymised (e.g., user level id and details are to be masked - mobile number can be stored as a hash value etc.) before publishing to the BI reporting system.
   a. Any ID must be stored by a Universally Unique Identifier (UUID) value that cannot be easily guessed.
   b. The mapping of such critical IDs can be stored as master information in main databases.

iv. Sensitive data stored in the database tables must be encrypted so that database administrators do not have direct access to this information for misuse.

v. Encryption must be done on similar lines of data integrity. However, to ensure no significant performance loss, the Hardware Security Modules (HSMs) must be used to encrypt and decrypt the data while persisting and reading the data.
   a. All applications reading the data must use the common persistence modules designed for each subject area to abstract the implementation complexity and expose the solution as a re-usable component.
   b. The keys used to encrypt the data shall be critical information that must be protected at all times.
   c. The column type for all encrypt able columns must be sized large enough to store the encrypted information. Additionally, the column type is set to string type and persistence module for each of the databases must ensure to do the required translation from string to appropriate data type.

4.27.6 Network Architecture requirements

UP112 communicates with the DC, DRC, OMCs, PRVs and field locations like DCRs, commiserates and other offices using available connectivity and connected through:

- MPLS network including Internet network
- SIM based GSM network
- RF network

The **Current Network** is MPLS based comprises of One Data Centre at Lucknow and Disaster Recovery Location in Bangalore 126 Remote Police Station across state of UP, two OMC Locations of Ghaziabad and Prayagraj. Additionally, there are 4800 PRV (Police Response Vehicles) 2/4 Wheelers.

The network is based on high availability solution comprising of

i. Dual Cloud MPLS Network reaching out at DC, DR, Operational Mirroring Centre (OMC) and Remote Sites

ii. Dual Internet Network terminating at Data Centre and Disaster Recovery Location

iii. Multiple National Long-Distance Point to Point Links for Operation redundancy and data replication activities.

iv. Dual Customer Premise Equipment Hardware at OMC, Data Centre

v. Single CPE at Remote Sites

vi. Lan Redundancy at Data Centre and Disaster

vii. Mesh architecture configured in both MPLS cloud which means any location talk to any site directly.

viii. Routing Protocol: Routers at site running BGP with Airtel and Vodafone MPLS

ix. Active Failover at All Remote Routers are configured

x. The Current Technology used are –
   - MPLS, Internet and National Long-Distance links (for Point to Point)
   - Mesh architecture configured in both MPLS cloud which means any location talk to any
   - Routing Protocol: Routers at site running BGP with Airtel and Voda MPLS
   - All the Routers have been configured in the Active Failover configurations.

xi. Data Centre, Lucknow: The current MPLS Dual Router (Cisco ASR 1006). The MPLS Infrastructure is currently deployed is on Dual Core with dual fiber last mile. The Infrastructure is currently deployed is on Dual Core with dual fiber last

xii. The two internet The Core switch deployed are on Dual redundancy. The access switch is connected in tandem to the Core switch.

xiii. OMC (Operational Mirroring Centre) Location: The locations important to handle the Citizen Distress Calls during overflow scenario of Data Centre and at the disaster situation. There are two OMC Location i.e. Ghaziabad and Prayagraj. The current MPLS Dual Router deployed is Cisco/ISR4451/K9. The MPLS Infrastructure is currently deployed is on Dual Core with dual fiber last mile.

xiv. Remote Sites/District Control Room: The current network has two last miles. Both the last miles are predominantly on wireless terminating on single Router 2911.

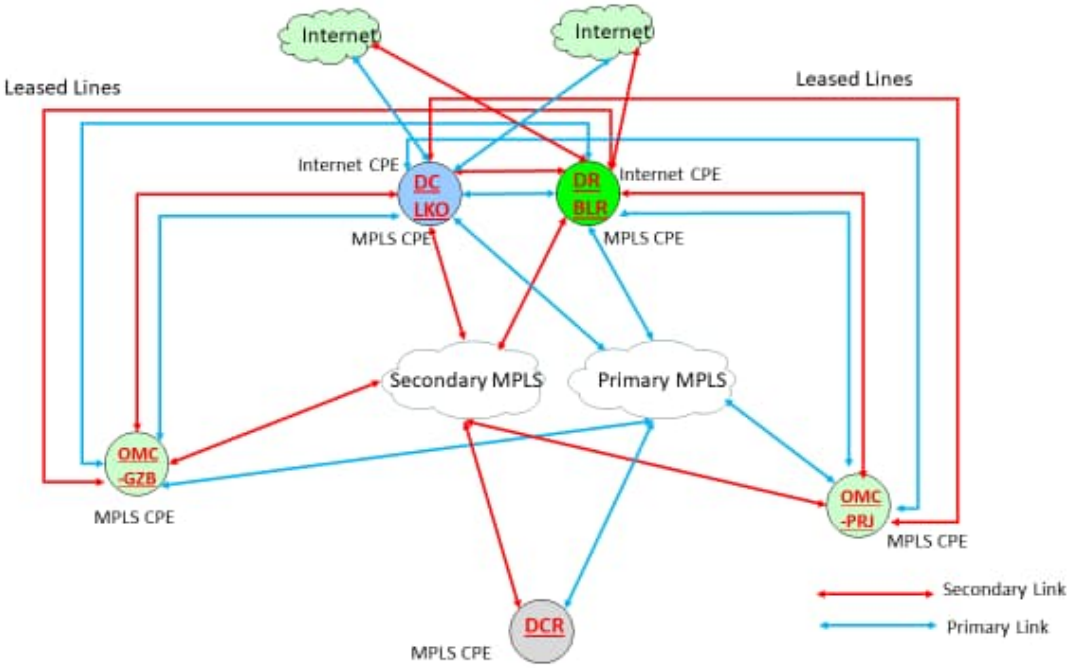
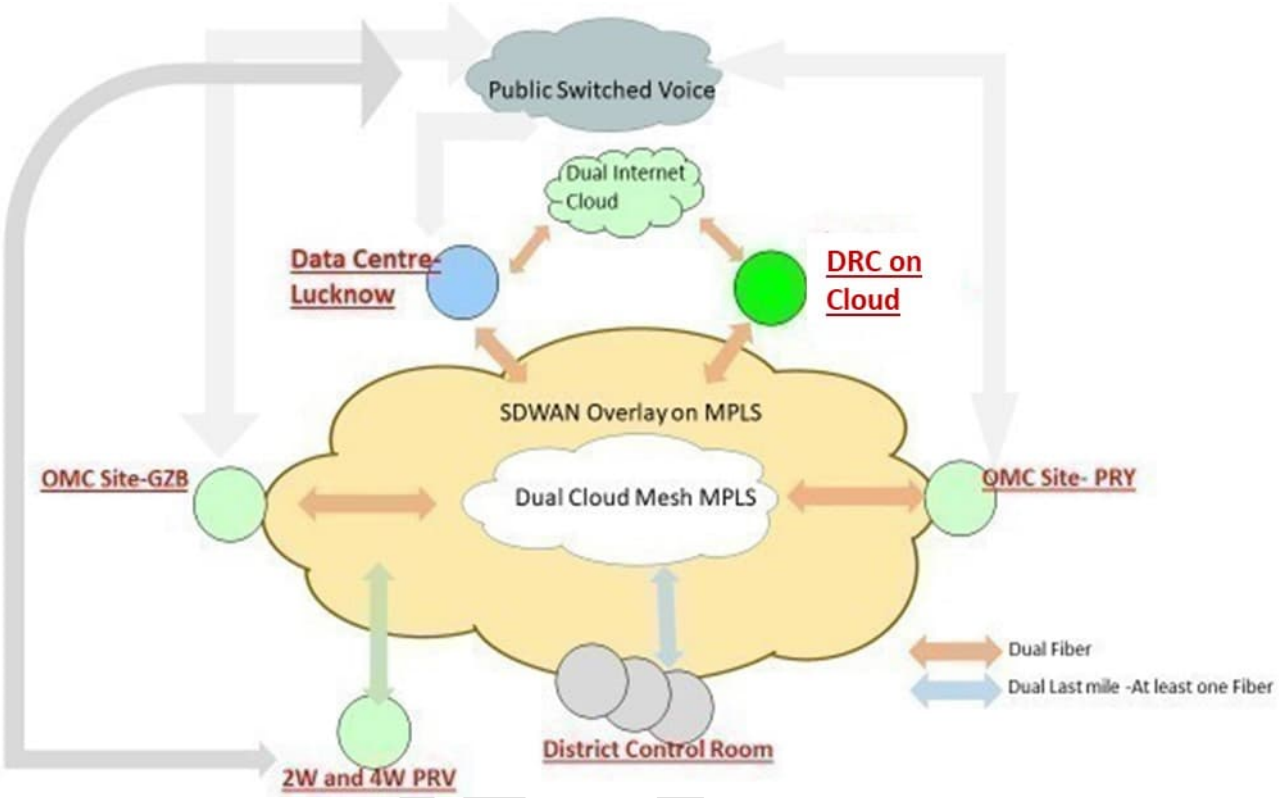


Figure:

xv. NexGen UP112 require MSI to connect all command centre in Lucknow, 2 OMCs and 129 field locations including Districts Control rooms and commiserates, other Police Units like 18 ranges of police station, 8 police zones of state, will be provided bandwidth over MPLS as primary and secondary connectivity for bandwidth.

xvi. NexGen UP112 require MSI to migrate the current MPLS based network Infrastructure to SDWAN bases network infrastructure to enable the business services from the latest technology solutions and reap following benefits

1. End to End SDWAN managed services and ownership of Wide Area Network including bandwidth and hardware.
2. Enable redundancy among WAN connections, automatically failing over to alternate path if the during failure of primary network. Use load balancing across multiple connections to improve application and network performance.
3. Application based routing and policies with real time enforcement of application SLAs.
4. Its key features include network abstraction, WAN virtualization, policy-driven centralized management, and elastic traffic management.
5. Simplified management, better network visibility



6. A comprehensive solution for the Supply, Installation, Configuration Integration, Implementation, Back lining with OEM and Telecom Service Provider, Testing, Maintenance, Management, Co-ordination, Uptime/SLA, and Facility Management of ITECCS Network with migration to SDWAN solution as per the technical specifications mentioned in Section 9 of the RFP and locations mentioned in the Section 9 of RFP for a period of project as per department requirement.
7. The entire current MPLS needs to be Migrated to SDWAN based network.
8. The underlay network will be the mix of MPLS, NLD across the sites of DC, DR, OMC and DCR locations.
9. The bandwidth requirement has been indicated in the Section 7
10. DC, DR, OMC location all the bandwidth to be provided from both the telecom service providers on fibre only.
11. DCRs and commiserates should have at least one bandwidth port out of Dual Port should be deployed on Fiber Ring network with path diversity of each fiber leg.
12. The bandwidth delivered should be from two different service provider network and there should not be sharing of the underlying Infrastructure e.g., Fiber, Hardware, Duct etc.
13. The Service provider should submit the fiber route diagram of the last mile om map from the customer location to the nearest Point of Presence showing the ring diversity of the bandwidth provided.
14. The Right of Way of the fiber laying has to be owned by the telecom Service Provider.

15. The SDWAN Edge devices to be integrated seamlessly with the bandwidth preferably on fiber port for reliability except for the case of wireless network port delivery.
16. Procurement, Installation, Commissioning, testing, monitoring and maintenance of new Routers and migration to SDWAN solution.
17. All the components of proposed SD-WAN Solution shall be compatible with on-premises and cloud.
18. In the proposed SD WAN solution, the WAN path selection should be dynamically selected based on the policy set from the Central controller placed at DC/DRC.
19. In the proposed SD WAN solution, the WAN path selection at the locations should be based on the real time analytics of the WAN Links Capacity & Quality (Packet loss, Latency & Jitter).
20. The MSI has to do the work of Design, supply, installation & maintenance of a comprehensive SD WAN (Software Define Wide Area Network) solution and seamless integration with the entire Network including hardware and software. SD WAN Solution needs to be implemented across Data Centre Primary Site, Disaster recovery site DRC, OMC Sites, DCRs, commiserates and other field locations
21. MSI should ensure proposed solution should be primarily able to provide aggregation of network links, load balancing of traffic, prioritizing of application over the network links, implementation of QoS per tunnel on the fly, discover network traffic with application-level insight with deep packet visibility and analyse and report on application usage and anomalies and prioritizing a specific application traffic over a link. It should be able to manage network congestion by optimizing application-level traffic and should provide monitoring capabilities on an ongoing basis and also be able to provide end user response time metrics.
22. Supply, installation, testing, commissioning, managing, and monitoring of SDWAN Network equipment's by upgrade / new procurement i.e., SDWAN Routers/Controllers/Central devices etc complying with the technical specifications given in section 9 along with all required licenses, accessories etc. and necessary documentation
23. Upgrade/ new purchase with configuration and Integration of SDWAN Routers with other IT/Network Devices/Servers/LAN/WAN along with migration to SDWAN solution as per the technical specifications mentioned in Section 9 of the RFP.
24. The proposed SD WAN solution should be able to load balance across multiple links simultaneously and leverage the secondary link for spill-over if the bandwidth required for one session exceeds the available bandwidth on the best link. This lets high bandwidth applications have as much bandwidth as they need to perform optimally.
25. The proposed SD WAN solution for real time applications like Voice and Video application experience optimization control session disconnection. It should also show same for non-real time application without session disconnect.
26. The MSI shall study and understand the existing setup at Data Centre, Disaster Recovery Centre, OMC, DCRs, Commiserates, other field locations and prepare detailed implementation plan for integration to SDWAN solution. The MSI shall create a Unified Project Plan and ensure that integration should be seamless and within

stipulated timelines where none of the services are impacted adversely and adequate skilled resources are available to support 24*7 operations.

27. The SDWAN device provided at UP112 site locations should have the capacity to handle the data traffic in Active-Active mode for all the links terminated into the router while enabling the entire required feature as per the bandwidth requirement in Section 9
28. The number of locations may increase over the time. The solution/technology services will be required to be further extended to increased number of sites across the state.
29. Solution should be scalable and should be configured to integrate centralized management console for SD-WAN solution irrespective of number of controllers, orchestrator/manager, analytics, or any other Head end devices installed to match project scalability requirement. Further the existing setup (Devices/Servers/LAN/WAN/monitoring tools) should be able to manage using same centralized console with offering all required features including but not limited to Zero Touch Provisioning, Centralized updates, Patch, and configuration management.
30. The MSI shall be responsible for configuration and Integration of SDWAN network devices with UPDial112 Devices/ LAN/WAN/monitoring tools.
31. The proposed SD WAN solution should allow for Hub & Spoke, Partial Mesh, full mesh network topology.
32. The proposed SD WAN solution should allow for internet break out at the local at field level, centralized location, remote entity (remote location) based on the application and the policy defined in the Central SD WAN controller.
33. The proposed SDWAN solution should support defining Application Aware policies.
34. The proposed SD WAN solution should continuously check the link flaps, if the link is not stable then put the link in monitor state, once the link is stable for particular time then start sending traffic on that link with QoS features/ bandwidth shaping.
35. The proposed SD WAN solution should support Link failover due to packet loss, Latency, Jitter, link flap & Etc. - without TCP / UDP session failover. If the bandwidth of a single session exceeds that available on any single link, the session must be able to use multiple links simultaneously by distributing the packets across multiple links.
36. The proposed SD WAN solution should recover from link failure - alternate link convergence time without session disconnect. (applications session should not be interrupted during the traffic fail over from one WAN link to Other)
37. The proposed SD WAN solution should be capable of selecting path per traffic type for Voice link, Application link). Department should have option to select from multiple solution options.
38. The proposed SD WAN solution should support seamless application accessibility across DC-DRC during auto failover of WAN links and load balancing
39. The proposed SD WAN solution should support QOS over the encrypted channel
40. The proposed SD WAN solution should be able to select the path based on the link quality (Congestion, latency, loss, and jitter) must be taken into consideration when a data transfer is initiated.

41. The proposed SD WAN solution should have the capability to detect the path MTU (Maximum Transmission Unit) and support all the MTU sizes in the Network.
42. The proposed SD WAN solution should have the ability to “pass through” certain applications/traffic without applying any Quality-of-Service parameters which is of no interest to the administrator.
43. The proposed SD WAN solution must support IPv4 and shall have the capability to support IPv6 Protocols.
44. The proposed SD WAN solution must be able to allocate a maximum bandwidth usage cap to each class of traffic.
45. The proposed SD WAN solution should be able to define Guaranteed Bandwidth base on different criteria
46. The proposed SD WAN solution during the failure on one link, the critical traffic should automatically migrate to the other Service Provider Link without any manual intervention and without session disconnect. QoS also should maintain during the failure of the WAN link.
47. SD WAN solution, the tunnel creation should be automatic & dynamic without any manual configuration on the edges and the controller.
48. Those MSIs who qualify in the Technical evaluation shall be asked to conduct the PoC to demonstrate the features/functionalities mentioned in this RFP,
49. The MSIs shall ensure that solution should support all the existing applications of UPDial112 and also any other new applications which department may implement in future.
50. The MSI shall coordinate with the existing service provider and all other stakeholders for smooth migration and setting up of new routers / upgraded routers with CPE on existing network at locations. The MSI shall coordinate with the existing service provider and all other stakeholders for smooth handover, migration and setting up of existing network devices viz routers, switches, etc. The MSI shall maintain the inventory of all network.

xvii. NexGen UP112 require MSI to provide SIP **channels** for calls landing at 112 centre at Lucknow and OMCs directly from Telecom Service provider. The number of SIP channels from different telecom given in Section 9

a. For redundancy on SIP channels at UP112 Lucknow centre and OMC, MSI will provide channels with last mile connectivity on different media (Copper/Fiber and RF). Required Telecom Service Provider services for various help lines needs to be activated and configured for SIP channels.
b. The SIP channels will be procured from Telecom Service Providers as per their load as per estimated load in Section 9 and they will be providing redundancy of SIP channels to Analogue and CUG mobiles lines as per Section 9. in case of failure of SIP channels
c. Distribution including inbound and outbound channels are as per Section 9.

xviii. NexGen UP112 require MSI to provide **SIM services** by Secure SIM of APN/ e-SIM hat will be installed in PRVs MDT, Mobile phones, GPS devices and transferring feeds of vehicle mounted cameras and body worn cameras. This will establish connectivity from UP112 centre, OMCs and PRVs

a. MSI to provide SIM services for GSM network to provide data connection at MDT to receive information about event
b. Similarly, SIM services would enable mobile phones to connect for data, calls, and SMS services
c. SIM services would be used to track the PRV through GPS devices fitted therein
d. MSI to conduct assessment of various locations for availability of GPRS/GSM network by different vendors available in UP. Based on this assessment and approval from UP112.
e. MSI to procure SIM cards for MDT, GPS and Mobile, possibly all from different telecom service providers
f. MSI will have to change backend service provider of SIM, if network is poor for SIM in that area.
g. MSI should have excess SIM card in spare
h. MSI to adhere that bills of SIM to be paid timely to avoid disruption in services
i. MSI to ensure unlimited data plans of 4G/5G connectivity
j. SMS through SIMs enable a computer to send and receive SMS text messages to PRVs and supervisory officer, even it would be used for feedback purpose
k. Provide redundant connectivity in UP112 from different modes (such as Fibre and RF) and also two different routes so that failure of one should not impact other.

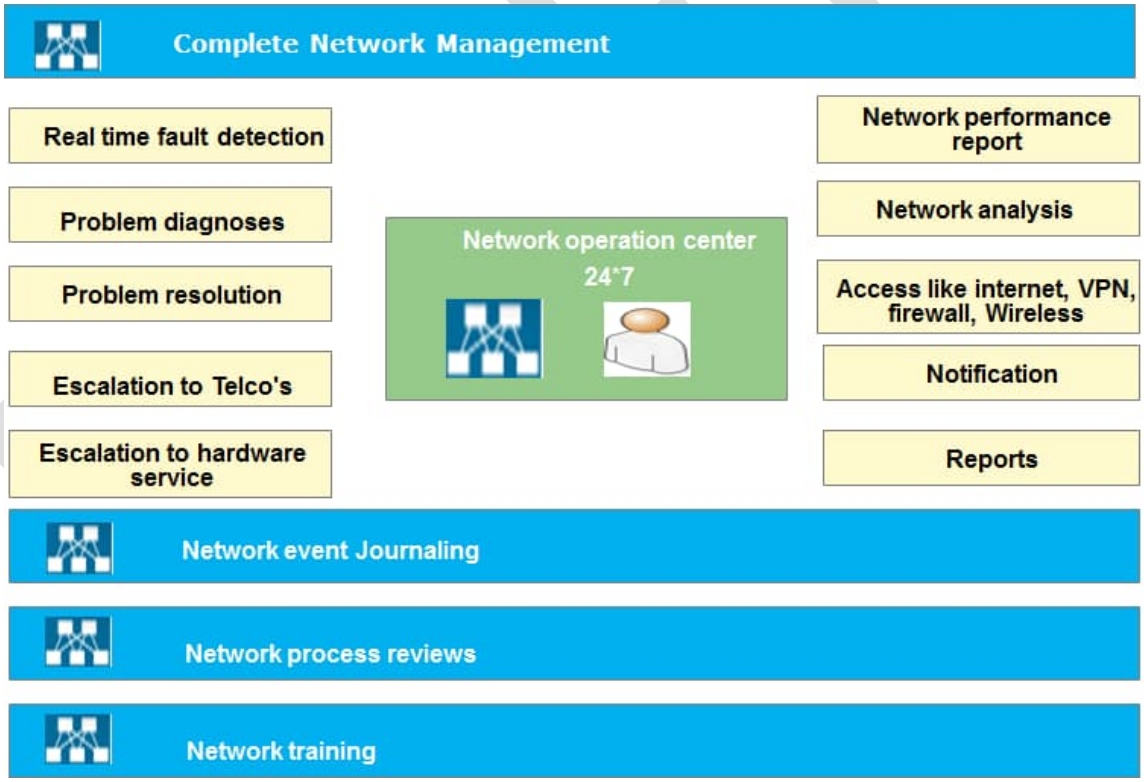
xix. NexGen UP112 require MSI to provide **ROIP (radio over Internet Protocol)** services using Radio frequency network**.** Radio Frequency devices will be integrated with UP112 Command centre, Lucknow and OMCs application connected equipment present in PRVs is wirelessly connected to the RADIO Services in broadcast mode over RF.

a. Host the radio application at UP112 command centre, OMCs, DC, and DRC
b. Solution should any source to multicast
c. Host the radio console web application at UP112 command centre and OMCs
d. Configure the city level radio frequencies in radio server through ports
e. ROIP hardware and software and other relevant components will be provided in 78 districts control rooms commisonarates UPUP112 command centre , 2 OMCs
f. Each PRV will be provided with VHF wireless device for RF communication
g. MSI will provide batteries, required antennas and mast for static as well as handheld devices
h. MSI will ensure that all consumables of Wireless communication like battery will
i. include replaceable warranty
j. MSI has to ensure that all Wireless equipment including VHF sets, batteries, antennas to keep in spare for replacement or sudden demand.
k. The radio devices provider should have AIP (Agreement in principles)
l. Radio devices will be connected in range of deployed frequencies at that particular area.

m. MSI to purchase wireless sets having Dealer Possession License (DPL) is issued to the prospective dealers and distributors of wireless products
n. Wireless (VHF) network from UP112 command centre as well as OMCs to vehicles as additional asset over Telecom Service Provider links

xx. For managing the Networking issues a **Network Operation centre (NOC)** need to be established by MSI and below are the functionalities of NOC but not limited to-

a. The NOC will analyse network problems, perform troubleshooting, communicate with various state site technicians, and track problems through resolution. The key objective of the NOC is to ensure the health and availability of components and services. When necessary, NOC will escalate problems to the appropriate stakeholders. For emergency conditions, such as a power failure of the NOC, procedures will have to be in place to immediately contact technicians to remedy the problem.
b. The indicative representation for the NOC with required minimum features:



c. MSI should develop services catalogue for NOC and get a sign off on the same from GoUP.
d. Primary responsibilities of NOC personnel will include but not limited to:

- Network monitoring and management
- Resolution Management including incident and problem management
- Service level management

- Service Continuity and Availability Management
- Reporting
- Root Cause Analysis
- Remediation plans
- SLA monitoring

e. Features of NOC

- Incident Management based on resource workload, incident Category etc.
- Creates service request or incident tickets when new request will come from state call centres
- Tracking and reporting of all contractual SLAs in an automated way.
- Updating knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.
- The NOC will escalate issues in a hierarchical manner, so if an issue is not resolved in a specific time frame, the next level is informed to speed up problem remediation.

f. MSI to ensure the services to be provided through NOC-Indicative list of services that have to be provided through the NOC are mentioned below.

- Monitoring, Management and Reporting with Enterprise Management System (EMS)- The EMS system should be provided for the regular monitoring, management and reporting of the ICT infrastructure of the project assets in the Data centre, DR Site, Operations Centre as well as State Locations. It should be noted that the activities performed by the MSI will be under the supervision of UP112. All active infrastructure components of the solution should be configured in the EMS system. The EMS or UPS monitoring tool should provision for monitoring the health status of the UPS and allied power systems incorporated in the solution. Accordingly, the UPS so provisioned should lend themselves to be monitored by the EMS/ UPS monitoring tool. The EMS provisioned would be required to be configured to calculate SLA parameters and generate SLA violations on request.

g. Following functionalities are desired by use of such EMS tools:

- Availability Monitoring, Management and Reporting
- Performance Monitoring, Management and Reporting
- Helpdesk Monitoring, Management and Reporting
- Traffic Analysis
- Asset Management
- Incident Management and RCA reporting.
- Change and Configuration management.
- SLA monitoring and management.

I. Monitoring and Management: Availability - Monitoring, Management and Reporting This part of the specification should ensure the monitoring, management, and reporting parameters of availability like discovery, configuration, faults, service levels etc. including but not limited to the following:

a. The proposed system must support multiple types of discovery like IP range discovery – including built-in support for IPv6, Seed router-based discovery and discovery whenever new devices are added with capability to exclude specific devices
b. The proposed system must support exclusion of specific IP addresses or IP address ranges.
c. The system should provide discovery and inventory of physical network devices like Layer-2 and Layer-3 switches, Routers and other IP devices and should provide mapping of LAN and WAN connectivity.
d. The discovery should be able to identify and model of the ICT asset.
e. The proposed system must provide a detailed asset report, organized by vendor name and device, listing all ports for all devices. The proposed system must provide sufficient reports that identify unused ports in the managed network infrastructure that can be reclaimed and reallocated. The proposed system must also intelligently determine which ports are operationally dormant.
f. The proposed system must determine device availability and should exclude outages from the availability calculation with an option to indicate the reason.
g. The proposed system should provide out of the box root cause analysis.
h. The proposed system must include the ability to monitor and visualize a virtualized system infrastructure by discovering and monitoring virtual machines and providing ability to depict the logical relationships between virtual servers and virtual machines.
i. The proposed solution must detect virtual server and virtual machine configuration changes and automatically update topology and should raise alarm when VM migrations happen between hosts.
j. The proposed solution must have the ability to collect data from the virtual systems without solely relying on SNMP.
k. The proposed solution must support an architecture that can be extended to support multiple virtualization platforms and technologies.

II. Reporting

a. The proposed system should provide sufficient reports pertaining to asset and change management, alarms, and availability of critical network resources as well as network response times for critical links.
b. The proposed system should be able to monitor compliance and enforce change control policies within the diverse infrastructure by providing data and tools to run compliance reports, track and remediate violations, and view history of changes.
c. **Performance - Monitoring, Management and Reporting**: The proposed performance management system shall integrate **network, server and database performance** information and alarms in a single console and provide a reporting interface for network components.
d. The Network Performance Management console must provide a consistent report generation interface from a single central console.
e. This central console should also provide all required network performance reports (including latency, threshold violations, packet errors, availability, bandwidth utilization etc.) for the network infrastructure. The proposed system shall identify over-and under-utilized links and assist in maximizing the utilization of current resources

f. The proposed system should enable complete customization flexibility of performance reports for network devices and monitored servers.
g. The proposed system should provide an integrated performance view for all the managed systems and networks along with the various threshold violations alarms in them.
h. The proposed system must provide the following reports as part of the base performance monitoring product out-of-the-box to help network operators quickly identify device problems quickly. The following charts like mentioned below should be available for routers: Backplane Utilization, Buffer Create Failures, Buffer Hits, Buffer Misses, Buffer Utilization, Bus Drops, CPU Utilization, Fan Status, Free Memory, Memory Utilization, Packets by Protocol, and Packets out etc.
i. The Proposed Performance Management must provide charts for Health Reports like:
j. Availability Chart, Average Health Index Chart, Average Network Volume and Call Volume Charts, Avg. Response Chart Bandwidth Utilization Chart, Latency Chart, Network Interface Utilization Chart etc.
k. The proposed system should be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits.

III. Network Performance Monitoring, Management and Reporting: Monitoring and Management

a. The System should have all the capabilities of a Network Management System which shall provide Real time network monitoring and Measurement offend-to-end Network performance and availability to define service levels and further improve upon them.
b. The tool should provide a live exceptions list displaying the various health and threshold exceptions that are occurring in the managed infrastructure.
c. The tool should have the capability to configure different polling speeds for different devices in the managed infrastructure with capability to poll critical devices
d. The proposed system should use intelligent alarm algorithms to learn the behaviour of the network infrastructure components over a period of time
e. The proposed system should be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements like Capture running and start up configuration, Upload configuration etc.
f. The proposed system must able to perform real-time or scheduled capture of device configurations. It should also provide features to capture view and upload network device configuration.
g. The proposed system must be able to store historical device configurations captured in the database and thereby enable comparison of current device configuration against a previously captured configuration as well as compare the current configuration against any user-defined standard baseline configuration policy.
h. The proposed tool should display configuration changes differences in GUI within central Console. Also, this should be able to identify which user has made changes or modifications to device configurations using the Interface.

IV. Application Performance Monitoring, Management and Reporting: Monitoring and Management

a. The proposed solution should proactively monitor all user transactions for any web-application hosted; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes
b. The proposed solution should determine if the cause of performance issues is inside the application, in connected back-end systems or at the network layer.
c. The proposed solution should correlate performance data from HTTP Servers (external requests) with internal application performance data
d. The proposed solution should see response times based on different call parameters. For example, the proposed solution should be able to provide CPU utilization metrics
e. The proposed Solution must be able to correlate Application changes (code and configuration files) with change in Application performance.
f. The proposed solution should allow data to be seen only by those with a need to know and limit access by user roles
g. The proposed solution should measure the end users' experiences based on transactions
h. The proposed solution should give visibility into user experience without the need to install agents on user desktops.
i. The solution should be deployable as an appliance-based system or software-based system acting as a passive listener on the network thus inducing zero overhead on the network and application layer.
j. The proposed solution must be able to provide the ability to detect and alert which exact end users experience HTTP error codes such as 404 errors or errors coming from the web application.
k. The proposed system must be able to detect user impacting defects and anomalies and reports them in real-time for Slow Response Time, Fast Response time, Low Throughput, Partial Response, Missing component within transaction
l. The proposed system must be able to instantly identify whether performance problems like slow response times are within or outside the data centre without having to rely on network monitoring tools.
m. The proposed system must be able to provide trend analysis reports and compare the user experience over time by identifying transactions whose performance or count has deteriorated over time.
n. The proposed SD WAN solution should monitor in Real time WAN Link Condition over the period of time and but not limited to
o. Packet Loss over the customized time period and real time
p. Jitter over the customized time period and real time
q. Link Errors over the customized time period and real time
r. Bandwidth Utilization over the customized time period and real time
s. Application utilization from bandwidth over the customized time period and real time
t. User (i.e., end user IP) utilization from bandwidth over the customized time period and real time
u. The proposed SD WAN solution should have web GUI console to manage the devices without limiting any functionality.

v. The proposed SD WAN solution should support role-based administration that can be linked to groups of WAN Virtualization solution. Depending on their assigned roles, administrators may have read-only or read-write
w. The proposed SD WAN solution shall support monitoring using SNMP latest version with backward compatibility.
x. The proposed SD WAN solution should provide role-based access control or multiple users. Roles that facilitate separation of duties.
y. The proposed SD WAN solution should support user / password management capabilities.

V. Systems and Database Performance Monitoring, Management and Reporting: Monitoring and Management

a. The proposed system should address management challenges by providing centralized management across physical and virtual systems
b. The proposed system should be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable, using agents on the servers to be monitored.
c. It should be possible to configure the operating system monitoring agents to monitor based on user-defined thresholds for warning or critical states and escalate events to event console of enterprise management system.
d. It should also be able to monitor various operating system parameters depending on the operating system being monitored yet offer a similar interface for viewing the agents and setting thresholds.
e. The proposed solution should support monitoring Processors, File Systems, Log Files, System Processes, and Memory etc.
f. The proposed tool should provide Process and NT Service Monitoring wherein if critical application processes or services fail, administrators are immediately alerted and processes and services are automatically re-started
g. The proposed tool should be able to provide Log File Monitoring which enables administrator to watch system logs and text log files by specifying messages to watch for. When matching messages gets logged, the proposed tool should notify administrators and enable to take action like sending an email.
h. The proposed database performance management system shall integrate network, server and database performance management systems and provide the view of the performance state in a single console.
i. It should be able to automate monitoring, data collection and analysis of performance from single point.
j. It should also provide the ability to set thresholds and send notifications when an event occurs, enabling database administrators (DBAs) to quickly trace and resolve performance-related bottlenecks.
k. The Monitoring tool should support database performance agents for performance reporting of standard RDBMS like Oracle, MS-SQL, Sybase and DB2.
l. The Performance Monitoring tool should provide you the ability to easily collect and report specific information, including information not limiting to: Buffer cache hit ratio, Locks and Global Locks, Table spaces etc.
m. The proposed system must provide Performance Management and Reporting — Provides real-time and historical performance of physical and virtual environments enabling custom ITECCS gain valuable insights of a given virtual container of the relative

performance of a given Virtual Machine compared to other Virtual Machines, and of the relative performance of groups of Virtual Machines.

n. Role based Access — Enables role-based management by defining access privileges according to the role of the user.
o. The proposed Virtual Performance Management system must integrate latest virtualization technologies

VI. Helpdesk - Monitoring, Management and Reporting

a. The proposed helpdesk system must provide flexibility of logging, viewing, updating, and closing incident manually via web interface.
b. The proposed helpdesk system must support ITIL processes like request management, problem management, configuration management and change order management with out-of-the-box templates for various ITIL service support processes.
c. Each incident must be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.
d. The proposed helpdesk system must be able to provide flexibility of incident assignment based on the workload, category, location etc.
e. Each escalation policy must allow easy definition on multiple escalation levels and notification to different personnel via window GUI or console with no or minimum programming.
f. The proposed helpdesk system must provide grouping access on different security knowledge articles for different group of users.
g. The proposed helpdesk system must have an updateable knowledge base for tech al analysis and further help end-users to search solutions for previously solved issues.
h. The proposed helpdesk system must support tracking of SLA (service level agreements) for call requests within the help desk through service types.
i. The proposed helpdesk system must be capable of assigning call requests to tech al staff manually as well as automatically based on predefined rules, and should support notification and escalation over email, web etc.
j. The proposed helpdesk system must integrate tightly with the Knowledge tools and Configuration Management Database (CMDB) and should be accessible from the same login window.
k. It should support remote management for end-user & allow analysts to do the desktop sharing for any system located anywhere using embedded OS remote control facility on analyst desktop and update the analysis status under EMS - helpdesk, monitoring, and reporting system, just connected to internet.
l. It should allow IT team to create solution and make them available on the end – user login window for the most common requests.

VII. Traffic analysis

a. The proposed system should enable the Data centre to centrally manage user access privileges and allow deploying baseline security polices so that the right people have access to the right information. It should proactively secure access to data and applications located on Linux, UNIX, and Windows system servers throughout the enterprise.
b. The traffic analysis system provides Network Fault and Performance Management System

c. The solution should be of the type passive monitoring without a need to install any probe or collector for data collection.
d. The solution must provide the following metrics:
e. The proposed solution must keep historical rate and protocol data for a minimum of 3 months (most recent) in its current long term operating database.
f. The proposed solution must be able to monitor and report on unique protocols per day and display utilization data and baselines for each protocol individually by interface.
g. The proposed solution must keep and report on unique hosts and conversations per day for each monitored interface.
h. All custom reports from the long-term database must support the ability to be run manually or scheduled to run automatically at user selectable intervals.
i. All reports should be generated and displayed directly by the system from a common interface.
j. The system should allow via API for Excel to download data to generate reports.
k. The system must be able to restrict views and access for defined users to specific routers, interfaces, and reports.
l. The user must be able to generate reports from the long-term database based on specific thresholds defined by the user where the threshold can be compared to rate, utilization, or volume of every monitored interface as a filter for inclusion in the report.
m. Search for any traffic using a specific configurable destination port, or port range
n. The overview page must include an email function that provides a GUI driven method for emailing the page in PDF format as well as for scheduling the email of this page at regular intervals without user intervention to one or more recipients.
o. The proposed system must be capable of sending alerts via SNMP trap. Alerts should the having the following configurable parameters:
p. The ability to choose any protocol, interface, or group of interfaces, ToS, rate, volume, utilization, time filters (i.e., business hours) over a specified threshold being monitored by the system.
q. The system must provide the ability to group interfaces into functional groups based on any user criteria. The grouping function must allow users to create group names and add interfaces into that grouping for reporting purposes. Once created, these groups must be available for selection within custom reports as a mechanism to include multiple interfaces without individual selection for inclusion.
r. The system must support interface specific report generation for every monitored interface in the network. It must provide menu or GUI driven access from the main system page that allows users to select from the automatically generated interface list and navigate to interface specific information.
s. This page should display a graph representing the total number of flows that the data was derived from. It must represent flows for the selected period of time, for this interface.
t. The user must be able to easily change the data type of the main interface view from protocol specific to a single graphical representation of utilization over multiple points in a 24-hour day as compared to all other similar points in the days in that month.
u. The monthly view must provide a graphical representation of the level of utilization for each fifteen-minute interval of each day of the month.

VIII. Asset Management

a. Ability to provide inventory of hardware and software applications on end-user desktops, MDTs, Radio devices etc. including information on processor, memory, OS, mouse, keyboard, etc. through agents installed on them
b. Ability to have reporting capabilities; provide predefined reports and ability to create customized reports on data in the inventory database. Report results could be displayed as lists or graphs
c. Ability to provide the facility to collect custom information from desktops
d. Ability to provide facility to recognize custom applications on desktops
e. Facility for the administrator to register a new application to the detectable application list using certain identification criteria. Should enable the new application to be detected automatically next time the inventory is scanned
f. Facility for User self-registration.
g. Ability to support configuration management functionality using which standardization of configuration can be achieved of all the desktops
h. Software metering should be supported to audit and control software usage. Should support offline and online metering.
i. Ability to support dynamic grouping of enabling assets to be grouped dynamically based on some pre-defined criteria e.g., a group should be able to display how many and which computers has a specific application installed. As and when a new computer gets the new application installed it should dynamically add to the group
j. Ability to use the query tool to identify specific instances of concern like policy violation (presence of prohibited programs or games and old versions, etc.), inventory changes (memory change, etc.) and accordingly it could perform several actions as reply. These actions could be (a) sending a mail, (b) writing to files, sound an alarm (c) message to scroll on monitor screen if the administrator, etc.
k. Facility to track changes by maintaining history of an asset
l. Ability to have web-based console
m. The proposed Asset Management solution should provide comprehensive and end -to-end management of all the components for each service including Network, Systems and Application infrastructure.

Note: It is mandatory that all the modules for the proposed EMS Solution should provide out-of-the-box and seamless integration capabilities. MSI must provide the specifications and numbers for all necessary Hardware, OS, and DB (if any) which is required for an EMS to operate effectively.

IX. Incident Management and RCA Reporting

a. An information security incident is an event (or chain of events) that compromises the confidentiality, integrity, or availability of information. All information security incidents that affect the information or systems of the enterprise (including malicious attacks, abuse, or misuse of systems by staff, loss of power or communications services and errors by users or computer staff) should be dealt with in accordance with a documented information security incident management process.
b. Incidents should be categorized and prioritized. While prior prioritizing incidents the impact and urgency of the incident must be taken into consideration.
c. It should be ensured that the incident database is integrated with Known Error Database (KeDB), Configuration Management Database (CMDB). These details should be accessible to relevant personnel as and when needed.

d. Testing should be performed to ensure that recovery action is complete and that the service has been fully restored.
e. The MSI should keep the end users informed of the progress of their reported incident.
f. When the incident has been resolved, it should be ensured that the service desk records of the resolution steps are updated, and confirm that the action taken has been agreed to by the end user. Also, unresolved incidents (known errors and workarounds) should be recorded and reported to provide information for effective problem management.
g. Information security incidents and weaknesses associated with information systems should be communicated in a manner allowing timely corrective action to be taken.
h. The MSI should conduct regular reviews on performance of incident management activities against documented Key Performance Indicators (KPI's).
i. The incident management activities should be carried out by the MSI in such a way that an incident is resolved within the agreed time schedule.
j. Root Cause Analysis (RCA) should be conducted by the MSI. The system installed should enable root cause analysis.
k. Controls related to incident management need to be implemented and each implemented control should have a documentary evidence to substantiate and demonstrate effective implementation.

X. Change and Configuration Management

a. Change and configuration management will be governed by the change management and configuration management policy of state. The policy will be shared with the successful MSI.
b. Change management provides information on changes and enables better control of changes to reduce errors and disruption in services.
c. All changes should be initiated using change management process; and a Request for Change (RFC) should be created. All requests for change should be evaluated to determine the impact on business processes and IT services, and to assess whether change will adversely affect the operational environment and introduce unacceptable risk.
d. The MSI shall ensure that all changes are logged, prior prioritized, categorized, assessed, authorized, planned, and scheduled to track and report all changes.
e. Ensure review of changes for effectiveness and take actions agreed with interested parties. Requests for change should be analysed at planned intervals to detect trends. The results and conclusions drawn from the analysis should be recorded and reviewed to identify opportunities for improvement.
f. Controls related to change management need to be implemented and each implemented control should have a documentary evidence to substantiate and demonstrate effective implementation.
g. The roles and responsibilities of the management should include review and approval of the implementation of change management policies, processes, and procedures.
h. A configuration management database should be established which stores unique information about each type Configuration Item CI or group of CIs.
i. The Configuration Management Database (CMDB) should be managed such that it ensures its reliability and accuracy including control of update access.
j. The degree of control shall maintain the integrity of services and service components taking into consideration the service requirements and the risks associated with the CI.

k. Corrective actions shall be taken for any deficiencies identified in the audit and shall be reported to the management and process owners.
l. Information from the CMDB shall be provided to the change management process, and the changes to the CI shall be traceable and auditable.
m. A configuration baseline of the attached CI shall be taken before deployment of a release into the live environment. It shall be stored in the safe environment with appropriate access control.
n. Master copies of CI shall be recorded in the CMDB and shall be stored in secure physical or electronic libraries which shall be referenced in the configuration records. This shall be applicable to documentations, licence information, software, and hardware configuration images.

XI. EMS Ability to integrate with other services

The proposed EMS solution must comply with key integration points out of the box as listed below but not limited to:

a. The proposed network management system should integrate with the helpdesk system by updating the Asset with CI information to support viewing history or open issues in helpdesk on the particular managed asset and associate an SLA to the ticket in the helpdesk. The proposed network management system should attach an asset identifier when submitting a helpdesk ticket. In case the asset is not found in the helpdesk database, it should be automatically or manually created prior to submitting the ticket. NMS console must show associated helpdesk ticket number for the alarms that generated those tickets.
b. SLA's violation on monitored end user response time must open a helpdesk incident out of the box.
c. Proposed Application Performance Solution must integrate with Network Fault Monitoring Solution to forward Application Performance Threshold violation alarms in proposed Network Fault Manager Console.
d. The proposed Fault Management Solution must support integration with proposed help desk or trouble ticketing system such that integration should Associates alarms with Service Desk tickets in the following ways:
e. Manually creates tickets when requested by Fault Management GUI operators
f. Automatically creates tickets based on alarm type
g. Provides a link to directly launch a Service Desk view of a particular ticket created by alarm from within the Network Operation console.
h. Maintains the consistency of the following information that is shared between alarm and its associated Service Desk ticket including status of alarms and associated tickets and current assignee assigned to tickets.
i. Helpdesk ticket number created for associated alarm should be visible inside Network Operation Console. It should be integrated in a way that Helpdesk incident can be launched once clicked on ticket number for associated alarm from within Network Operation Console.
j. The proposed virtual performance management system should integrate with proposed Network Management and Performance Management system out of the box.
k. The proposed NMS should provide workflow between the fault and performance management systems including bi-directional and context-sensitive navigation, such as
l. Navigate from the Topology View to At-a-Glance or Trend Reports for any asset

m. Navigate from the Alarm View to At-a-Glance, Trend or Alarm Detail Reports
n. Proposed Performance Management system should feed in discovery from Devices already discovered in Network Management Module without starting discovery process again all together in Performance Management Engine this will reduce effort of having to perform discovery on both Fault and Performance Management Engines. Discovery can be synchronized.

Note:

Successful MSI must use Industry standard EMS tools recognized by analysts to report desired SLAs for availability and performance of Various IT Components including Networks, Systems and OS. Keeping in view the intricacies involved in the installation, configuration and day to day use of various components of Enterprise Management System covered under this document, the proposed EMS solution must involve tools to ensure smooth or seamless integration and out of the box workability of the offered solution.

XII. ICT Assets Hardening

a. All the ICT assets should be hardened as per the Hardening guidelines and industry leading practices.
b. Remove all unauthorised software, utilities, and services.
c. All required logs should be configured and monitored

XIII. Identity Management Services

a. IDM services should have tight integration with Directory service, which acts as exclusive User repository and directory services for the entire infrastructure.
b. IDM should understand the domain schema and have integrations with Devices and applications for Authentication and Authorization services across the network.
c. IDM should have the feature either to publish or accommodate Organization Group policy publishing.
d. The Identity Manager architecture should be an N Tier Architecture to allow portability between Operating systems and Application servers.
e. Solution must be comprehensive with user provisioning, de-provisioning and password management tools
f. Both the User Provisioning and Access Management [SSO and Operating System Access Control] solution must be a part of an integrated “Identity and Access Management” solution. MSI should own the responsibility for the Identity and Access Management Suite. As the current solution involves both provisioning tools and Access Management tools, it is required that tighter integration and ease of administration is available
g. The solution for identity lifecycle management should support Web Services standards
h. Provisioning tool must support and provide business role-based provisioning.
i. IDM solution should take care of Privileged user access management, single sign on, effective governance mechanism on complete User Management life cycle.
j. Network Access Control Service: Network Access Control Service will aim at controlling access to network with policies, including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do. This service will ensure that when a computer connects to the

network, it is not permitted to access anything unless it complies with the ITECCS defined policy, including anti-virus protection level, system update level and configuration.IT Infrastructure at the NOC

k. The MSI has to ensure the proposed NOC services can be operated from NOC.
l. The MSI will provide adequate IT infrastructure for all the persons manning NOC.
m. MSI has to provide required Desktops with OS and other relevant software.
n. MSI has to provide the required network connectivity to operate NOC.

XIV. Service Level Management

a. The proposed service management system should provide a detailed service dashboard view indicating the health of the services they rely on as well as the SLAs.
b. The system should provide an outage summary that gives a high-level health indication for each service as well as the details and root cause of any outage.
c. The system must be capable of managing IT resources in terms of the business services they support, specify and monitor service obligations, and associate users with the services they rely on and related Service or Operational Level Agreements. Presently, services shall include E-mail, Internet Access, Intranet, and other services hosted.
d. The Service Level Agreements (SLAs) definition facility must support defining a set of one or more service that specify the Service obligations stipulated in an SLA contract for a particular time period (weekly, monthly, and so on).
e. SLA violation alarms must be generated to notify whenever an agreement is violated or is in danger of being violated.
f. The system must provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In addition, the capability to exempt any service outage from impacting an SLA must be available.
g. The reports supported must include one that monitors service availability (including Mean Time to Repair (MTTR), Mean Time between Failure (MTBF), and Maximum Outage Time thresholds) and the other that monitors service transaction response time.
h. The system must provide a historical reporting facility that will allow for the generation of on-demand and scheduled reports of Service-related metrics with capabilities for customization of the report presentation.
i. The system should provide for defining service policies like Service Condition High\Low Sensitivity, Port Status High\Low Sensitivity should be provided out of the box.
j. The system should display option on Services, Customer, SLA's, SLA templates. The customer definition option should allow associating a service or an SLA with a customer.
k. The system should enable generation of reports based on time period selection. It should show absolute results as also percentage-based results.

4.27.7 Application Architecture requirements

MSI has to ensure that applications can be easily modified to respond quickly to the changing business needs, as well as to the rapidly evolving information technologies available to support those need and MSI also need to ensure that all the application should follow the application architecture requirements

a. In order to ensure good application performance and efficient usage of network bandwidth, MSI should emphasise that the system shall utilize scripting technologies effectively which will reduce the number of transactions with the main server and thus reduce the overall bandwidth requirements
b. Designed system shall use web services to implement service-oriented architecture. A major focus of Web services is to make functional building blocks accessible over standard Internet protocols that are independent from platforms and programming languages.
c. System shall provide a browser/ application-based user interface supported by al iOS, Window, Android etc.
d. MSI should ensure that the applications shall be platform neutral
e. All the applications shall be compatible to cloud hosting
f. System shall be designed so that business rules control access to data- In the applications, data would be created, used, and managed by the application component that automate the business processes
g. System shall adopt coding standards in all languages on all platforms that make debugging and maintenance easier
h. The code providing input and output to the user interface would be designed to support a wide range of interfaces

Definition of Options for NexGen UP112 -

- **Upgrade-** This means upgradation of the existing Software/Applications used by UP112 complying with defined specifications as per annexure 9.31.
- **New -** This means providing new Software/Applications complying to required specification as per annexure 9.31.

The details of Applications are presented below with its criticality type and Existing OEM details-

Note- All the application provided initially, its upgrade and any other new application added by MSI shall be compatible to the cloud environment.

S. No.	Applications Category	Applications	Criticality	Existing OEM	Option for NexGen UP112
1	Contact Center Solution	IP PBX	Critical	Avaya	Upgrade
		IP Phone software / Soft phone	Critical	Avaya	Upgrade
		Outbound Dialler software	Critical	Avaya	Upgrade
		Automatic Call Distribution (ACD)	Critical	Avaya	Upgrade
		Call Telephony Integration (CTI)	Critical	Avaya	Upgrade
		Voice recording and Quality monitoring	Critical	Harmony	Upgrade
		Contact Centre Reporting System	Critical	Avaya	Upgrade
		Number Masking	Critical	New	New

S. No.	Applications Category	Applications	Criticality	Existing OEM	Option for NexGen UP112
		Multimedia System	Critical	Avaya	Upgrade
2	Computer Aided Dispatch (CAD)	Web CAD Application	Critical	Intergraph	Upgrade
		Mobile CAD Application	Critical	Intergraph	Upgrade
		Police Station Module	Critical	Intergraph	Upgrade
3	Supervisory and Monitoring	Mobile Application for Police officials	Critical	Intergraph	Upgrade
		Web/Desktop Applications for Police officials	Critical	Intergraph	Upgrade/New
		UP112 Citizen Portal	Critical	Microsoft	Upgrade/New
		Enterprise management System (EMS)	Critical	Microsoft+Solarwinds+Symphony	New
		Mobility Device management (MDM)	Critical	New	New
		Inventory Management Software	Non-Critical	Microsoft	Upgrade/New
		Human Resource Management Software	Non-Critical	Microsoft	Upgrade/New
		Biometric Attendance	Non-Critical	Idemia-Morpho	Upgrade/New
		Patrol Management System	Non-Critical	Intergraph	Upgrade/New
		Fleet Management Solution	Non-Critical	New	New
4	Maps and Location Identification	GIS Application	Critical	Here	Upgrade/New
		GIS Map Data	Critical	Here	Upgrade/New
		GIS Map Geo-Fencing Application	Critical	Here	Upgrade/New
		GIS Data Capturing Mobile Application	Non-Critical	Here	Upgrade/New
		Location Based Services (LBS)	Critical	Pert Telecom iLocator	Upgrade/New
		Vehicle Tracking System	Critical	Intergraph	Upgrade/New
		PRV Location Tracking by Citizen	Critical	New	New
		ELS/ALS (Emergency/Advanced Location Services)	Critical	New	New
5	Other Application	Video Conferencing	Non-Critical	Polycom	Upgrade/New
		Document Management System (DMS)	Critical	Microsoft	New
		Directory Services	Critical	Microsoft	New
		Identity Management Software (IMS)	Critical	Microsoft	New

S. No.	Applications Category	Applications	Criticality	Existing OEM	Option for NexGen UP112
		Chatbot	Non-Critical	New	New
		E-Learning	Non-Critical	Microsoft	New
		Backup Software	Critical	Hpe	Upgrade/New
		SMS Gateway	Critical	Airtel	Upgrade/New
		Business Intelligence	Non-Critical	Intergraph	New
		Video Management Software (VMS)	Critical	New	New

Following are the key features of the required applications while details are provided in technical specifications as per FRS document

a. Contact centre Solution

It includes features for caller interface exchanges, call monitoring, and call routing systems. The contact centre solution is the backbone for telephony of command centres and application is being widely used for telephony interfaces by all the contact centres staff. The following components are integrated features of contact centre solution:

i. IP PBX

1. IP PBX is a software-based appliance that transfer calls received on SIP channels to the IP network
2. The software identifies the correct location and automatically route the calls to the respective UP112 officers
3. All outbound calls from the UP112 gets routed to SIP channels through IP PBX system
4. Provision to broadcast “Greeting Message” whenever a call is received on the system
5. Current status and proposed feature for the application

ii. IP Phone software / Soft phone

1. System will allow the officers to log into the IP phone through the software and integrate it in the backend with IPBX for call forwarding
2. Incoming and outgoing call flash on the screen of CAD communication officer as well, from where it can be attended

iii. Outbound Dialler software

1. The software will be used for the making outbound calls from the officers to return missed call, call in case of SMS, email, or other input sources
2. Feedback calls: The outbound dialler software will have a feature to make calls to the caller whose complaints as per system have been closed. The feedback connected through the ACD with the available communication officer

3. Conference facility: This facility will be used in situations wherein the officer makes a conference call with the caller and the field officer from police to connect both on same call for more clarification.

4. The outbound calls system should be able to optimally utilize outbound desk CO. Thus, communication officer must be engaged only once the call gets connected with citizen. The ring time or the call connect time shall not get wasted for a communication officer.

iv. Automatic Call Distribution (ACD)

1. Routing of the calls to UP112 centre and the available officer shall be carried out by ACD
2. ACD employ a rule-based routing strategy
3. ACD enable to identify available officers and transfer the call accordingly
4. In an event of all officers being engaged, critical calls shall be diverted to the nearby officer based on the rule engine
5. Call routing to the officers will be based on the “longest idle basis”
6. ACD will seamlessly integrate with IP PBX system

v. Call Telephony Integration (CTI)

1. CTI allows interaction between telephone and a computer
2. CTI runs on a server and acts as a common interface for integration of all the deployed software applications
3. CTI functionality will support relevant screen pop-ups on the officers’ screen on the basis of call location detection
4. CTI will pass events details and changes in communication officers’ status and as well as details incoming calls to the computer applications

vi. Voice recording and Quality monitoring

1. The voice recording shall happen for all incoming and outgoing calls
2. System will store voice recording of entire conversation between caller and communication officer both for incoming call and outgoing call even when calls are transferred from one centre to another Control room of the UP State
3. Voice recording of all the calls is maintained at the DC/DR for a period of 5 years. One-month live call data also be maintained post which it is archived. Critical data is flagged even after archival on SAN based suitable accessible storage. This help in post event analysis and if required for judicial purposes
4. System is designed such that unauthorized person cannot modify/ move/ delete any voice recordings
5. Authorized personnel from UP112 able to access the recordings as required by them

6. System enables search for the voice recordings through various fields and filters such as date, time, caller name, location, case file number, officer etc.

vii. Contact Centre Reporting System

1. Reporting system has a provision to provide the Contact centre reports like call handling, Average handle time of the call etc.
2. System enables to export the report the report in different kind of format like pdf, text, Xls etc.
3. The officers at UP112 HQs shall have access to the Contact Centre dashboards at their laptops, tablets, or mobiles.

viii. Number Masking

1. At times, the mobile numbers of PRV staff get shared with citizens of the state, and then, even after the close of the event, citizens communicate with PRV staff directly. This situation creates 2 issues:
    - The system has exited the loop. the communications are beyond the scope of the UP112 system.
    - As per SOP, PRVs should not cater to any event or issue that hasn't been allocated to them, but at times, PRV staff have responded to these direct requests.
2. Thus, to ensure that the UP112 system is always on loop and that no direct links are established between citizens and PRV staff, all number masking applications would be required.
3. Call masking solutions would ensure end-to-end data protection through virtual number calling. The call will be placed on the server, and a virtual number will be displayed to the citizen who can answer the call.
4. All the calls from PRV staff to citizen and citizen to PRV staff shall be recorded and available. The recording shall be available for 15 days.

ix. Multimedia System

1. Multimedia System act as an interface to receive inputs from various sources such as SMS, email, chats etc. and convert the input to CAD format
2. It sends notifications to the screen of the identified CAD Officer
3. System enables to detect the location from the GPS coordinates received from mobile application, IoT, panic button of vehicles etc.
4. System has the capability to register the mobile applications/ IoT/ devices/ panic buttons etc. before the data can be received from the same

b. CAD Application

All incoming emergency and non-emergency calls or data messages attended by CO through the front-end system are CAD. CAD systems have various fields for inputs such as name, address, contact number, incident type, incident location, caller location, priority of incident, type of emergency response required, etc. and would also

have pre-populated information from the location detection (call or IP or latitude-longitude) or subscription details. After entering the details from the input source (call or SMS or email or mobile application or chat or WhatsApp or other), the officer creates a case with a unique id and passes on cases for dispatch as per the standard operating procedure. The CAD software has the capability to run multiple other features and its heartbeat application throughout the entire ERSS. Some of the new features

Auto Arrive

1. System should automatically arrive the PRV when reached close to the event location
2. No additional cost for Geo tagging and Auto arrive, only need customization in CAD application

Geo Fencing of PRVs

PRVs are usually allocated to a thana boundary/ boundaries. It is seen that PRV crosses their allocated jurisdiction. In order to monitor their movement as per defined route, it is recommended that their routes are predefined, and any violation should be in form of auto alerts.

i. Computer Aided Dispatch (CAD) Application

1. Communication/Event Supervisors enable to access the CAD application with proper identification of username/ login
2. CAD system receives case in form of call/SMS/Chat/Social Media/Mobile app SOS etc. which would include details of person in distress, location details, incident type, officers' comments and other details captured from the person.
3. System assists communication officer to see the case details and should have functionality to categorize the case and mark it for to take further action
4. System assists the dispatch module to locate the nearest available vehicles and also facilitates correct directions to the identified by vehicle to reach the incident spot in minimum time
5. AVLS (automatic Vehicle locating system) utilize both GPS and GSM technologies to track vehicle at any time and at any location. It will also help in gathering information about the distance travelled by the vehicle
6. GIS coordinates of the person in distress (in case longitude/ latitude received by CRM) and emergency response vehicles would be displayed on the screen of the Dispatch Supervisor
7. Information from the CAD system is passed on to the identified MDT device
8. System capable of capturing information such as time of allocating the case to vehicle, officers present in the vehicle etc.
9. CAD system have monitor displays of which one display will be for CAD application and the second display for GIS application

10. Event Supervisor module of the CAD system provide overriding rights to the supervisor. Supervisor would be able to define position of the emergency vehicles, define VIP movement, rallies etc.
11. Event Supervisor able to define the master's for the CAD system such as dispatch zones, vehicles, shifts, skills, events etc.

ii. Mobile CAD application

1. The mobile CAD application installed in the MDT and Mobile devices issued to the PRVs for sharing event related information
2. Mobile CAD Application shall receive the notification of the case detail which is sent by dispatch
3. The application shares the current location of the vehicle to DC through a Web API configured in concerned mobile devices
4. Status and proposed feature for the application

c. Supervisory and Monitoring

i. Mobile Application for Senior Officers, Police Station Officers and Field staff (Supervisory App)

1. To monitor the activities of all cases received in UP112, a mobile app is developed and installed for field officer to monitor event related information on mobile handset
2. Officer can monitor the activity and location of PRV for the events in their jurisdiction and can perform appropriate action on requirement basis
3. Field staff also have role-based access to this mobile application for monitoring and supervision of PRVs under his purview
4. This application shall get the event related data on real time basis
5. The application shall be able to provide the call recording of communication between caller and communication officer but only on request basis
6. The call recording feature shall be available up to SP and above level

ii. Web and Desktop Application for Monitoring - Police officials

1. Web application over MPLS network available to monitor the activities by Field officer in their jurisdiction.
2. Officer can monitor the activity and location of PRV for the events and can perform appropriate action on requirement basis
3. Current status and proposed feature for the application

iii. UP112 Portal (Citizen Portal)

1. There will be UP112 portal for both internal and public domain users
2. UP112 Portal is website built on web-based application where Department publish any kind of updates related to their services of UP112
3. UP112 internet portal shall be used to provide feedback, history of the cases etc. – Not available

4. UP112 internet portal shall be used to display any kind of news, event and update which are published by Department of Home
5. In the next stage the content requires to be updated on regular basis

iv. Enterprise Management System (EMS)

1. It is envisaged that the entire IT infrastructure of including servers and devices at all locations (centre, state, and field) and network shall be managed through this solution.
2. The EMS solution deployed on all the SNMP devices such as desktops / servers / networking equipment to be monitored.
3. EMS is used to automate and monitor SLAs and generate the log of any defaults.
4. All the SNMP devices will be listed in asset management part of the EMS tool.

v. Mobility Device management (MDM)

1. All MDT, mobile phones, tablets, GPS devices even radio sets would be monitored through MDM health including its availability, performance and usage would be continuously monitored.
2. AVLS would also be monitored via MDM
3. MDT would have various status like available, away, on case, unavailable etc. to let dispatcher know the current availability of MDT vehicle
4. Remote management shall be available i.e., complete control of MDT can be taken
5. Simultaneous TEXT MSG push (bulk SMS) to MDT by MDM would be available
6. Remote console to be available to view all such devices centrally
7. Automated Live GPS location of MDT should be available

vi. Inventory Management Software

1. All the non-IT assets such as Table, chairs, PRV in fleet equipment etc. shall be labelled with RFID tag and all the districts and HQ would be provided with RFID reader.
2. This would ease the stock checking and tracking of assets at central level.
3. BAR Code generation to be available, inventory license limitation shall not be there to capture centrally
4. Inventory check to be done by MSI to support the department. However, stock inventory under Inventory application to be managed by department with the help of MSI.
5. Task of Feeding data in Inventory management software shall be in the scope of MSI

vii. Human Resource Management Software

Solution facilitates in enabling effective monitoring and supervision of staff. This covers the electronic supervision and measurement of the following indicative personnel processes and transactions related to:

1. Time and attendance
2. Payment
3. Leave management
4. Travel management of staff
5. Transportation
6. Transfer/promotion of outsourced staff
7. Rewards and recognition received
8. Training conducted
9. Code violations if any
10. Complete life cycle of personnel from selection, evaluation to exit
11. Grievance redressal

viii. Biometric Attendance

1. Centralized biometric attendance system for UP112 and two OMCs
2. In next stage, centralized facial recognition will be integrated with attendance software on MDT as a part of HRMS to capture the attendance of PRV staff
3. Reporting System, encryption facility will be there for biometrics solution
4. Registration of PRV staff on Biometric (Facial recognition system) shall be done at DCR level

ix. Patrol Management System

The Patrol Management System enables us to define, assign and monitor the routes, allocation, and utilization of resources. A Patrol Management application also be installed on MDTs for managing the Patrol related activities of the PRVs. The application will cover the following:

1. Define landmarks
2. Define routes
3. Add/Update details of personnel available
4. Send and Receive patrols
5. Reports/MIS
6. This application shall also be able to capture details of arrests and seizures (if made) during patrols.

x. Fleet Management Solution

Fleet management solutions would digitize and improve complete NexGen UP112's fleet management operation, key areas of operation would include:

1. **Maintenance planning:** A digitized schedule would help ensure PRV to receive routine maintenance and enable PRV staff to spot and remedy

excessive wear and tear before it becomes a major issue. This, in turn, would reduce vehicle downtime and maintenance costs.

2. **DVIR**: Digital Vehicle Inspection Reports (DVIR) would enable drivers to report vehicle and maintenance issues quickly and efficiently. Calling attention to problem areas in real-time with photo upload capabilities would help to keep vehicles on the road by eliminating unexpected downtime.

3. Fuel Utilization tracking with the data available at fuel providing agencies

4. **Driver Behaviour:** Getting real-time PRV pilot behaviour data and the automatic creation of driver risk profile will help fleet managers to identify drivers who are at high risk. Fleet management systems would also create driver safety league tables that can be used for safe driving incentive programs.

5. MDT will also have an application for PRV management that shall be used by the field staff for supervision of PRV operations and maintenance e.g., refuelling of vehicles, submission of bills, logging the odometer readings at the time of PRV handover-takeover for patrol vehicle mileage validation, periodic inspection reports, and code violations if any etc. This application shall interact with the central BI-Reporting and Analytics system for monitoring and supervision by the ITECCS officials.

6. These types of tracking will make fleet managers task far more manageable, as they will act as a single source to gain real-time visibility into the status of the entire fleet. It will also make easier to transfer information across business — especially when your fleet management software is integrated with other applications used across the UP112 operation.

d. Maps and Location Identification

i. GIS Application

The representation for GIS application architecture is comprehend GIS application deployed at DC, DRC and UP112 and field level devices. Majorly 3 components are involved to implement GIS functionality i.e., GIS MAP, GIS MAP DATA and GIS Server.

1. GIS MAP is a base layer on which GIS map data rendering GIS MAP with data of multiple point of interest (PoIs) in form of latitude and longitude

2. GIS Server render the caller / Vehicle location and identify the GIS map and GIS map data and will send to the event supervisor desktop and to MDT devices

3. MDT and concerned users share the location in form of latitude and longitude at DC where GIS server with GIS data is configured.

ii. GIS Map Data

GIS maps of high precision, comprehensive and detailed with roads, house and building level data shall be available.

iii. GIS Map Geo-Fencing Application

Geo-fencing application is installed on GIS desktop. Personnel with geo-fencing support person create the boundary of the UP-state areas including Police boundaries up to Police stations level, cities, districts etc. This is enriched for more than 50 layers including Police boundaries, road network etc.

iv. GIS Data Capturing Mobile Application

GIS Data capture mobile application is used to collect the field location data of different areas in the state. Once the data is stored, the officer will then push the data to the Data centre GIS database through the mobile application.

v. Location Based Services (LBS)

1. Location detection from connectivity of Gateway Mobile Location Centre (GMLC)/ Home location register (HLR)
2. LBS will be integrated with Telecom Service Provider GMLC/HLR data base to get precise information
3. For getting precise information about location, Location Based Service (LBS) may be used
4. Availability of SDR is a challenge that will be taken care in next stage of project

vi. Vehicle Tracking System

A vehicle tracking system combines the use of automatic vehicle location in individual vehicles with software that collects these fleet data for a comprehensive picture of vehicle locations. Modern vehicle tracking systems commonly use GPS for locating the vehicle. Vehicle information can be viewed on electronic maps via the Internet or specialized software. During NexGenUP112 we are expecting to get auto alerts at CAD for high-speed driving of PRVs. Thus, for PRVs not tagged to an event shall not be allowed to use PRV rashly.

vii. PRV Location Tracking by Citizen

Citizen would be able to track movement of PRV assigned to cater event reported by him. PRV location tracking facility shall be available to citizens of UP state of respective event. Post assignment of a PRV to an event, the citizen who registered the event would receive a message with LINK to track his PRV this link would be LIVE till PRV arrives the location of reported event. The PRV tracking shall have feature to show Expected Time of Arrival (ETA) of PRV to Citizens.

viii. Emergency Location System/Advance Location System (ELS/ALS)

1. **Leveraging Advanced Mobile Location (AML) for smart phones location detection:**
   Advanced Mobile Location (AML) shall be leveraged to identify location of callers calling through smart phones (Android/iOS). The location is derived from the location data of the phone (GNSS, Wi-Fi). Therefore, it helps identify location with much better accuracy and reduces dependency on telecom operators' network. The availability of ELS/ALS is subject to support from respective service provider.

2. **Location Based Mass Population Alert:**
   Location based Mass Population Alert system can help department communicate with a targeted audience based on their location either through SMS or voice call. It can be used to send warning for floods in vulnerable areas, to counter rumours that are being spread in specific location to incite mobs, to provide traffic related updates in particular parts of the city etc.

3. **Location identification for requests received through WhatsApp or SMS**
   This shall be used to identify location of victims who have communicated over WhatsApp or SMS. It will help increase the reach without over-burdening the system.

4. **Satellite based location tracking of PRVs in remote areas**
   We propose satellite-based location tracking of PRV which are in those areas where telecom network connectivity is either very poor or no connectivity. Satellite based tracking will be done using GPS device that will be placed on the PRVs which will continuously provide the location of the vehicle without depending on the telecom operators.

e. Other Required Applications

i. Video Conferencing

1. Video conferencing shall be more comprehending in the next stage of project enabling 78 districts Control room, Commissionerate's, 78 SP/SSP's and Commissionerate's offices, OMCs, headquarters in Lucknow and all PRVs connect on VC through a single software using the existing infrastructure upgrade
2. Video conferencing will strengthen district SP/SSPs and commiserates to videoconference with PRVs and with the other units connected on same MPLS network, at a time 10% of the total user defined in section 9 Annexure- 25 "Quantifiable Specification Standards of The Service BOQ" can be part of a single call
3. New feature like Logged in user in conference can also share the private text message through the software as well
4. Additional feature like meeting via other Video Conference service provider such as Google Meet and Teams shall be available
5. Also, Auto camera focus feature (eagle eye) during VC shall be available

6. Feasibility to have video call with PRV staff either on MDT or on Mobile shall be available

ii. Document Management System (DMS)

1. DMS will have new functionality to manage documents with updated version and categorization of the documents with proper indexing
2. DMS would have a provision to detect the user roles and permission and show the relevant functionality to the user as per requirement
3. New functionalities need to be added such as File movement and Letter movement shall be available

iii. Directory Services

1. Directory services would have a provision to create, update and modify the LDAP (Lightweight Directory Access Protocol) directory
2. It would have a provision to integrate with the Identity and access management
3. It would be used to define the roles and permission of different kind of users in the system
4. Directory services would have proper integrations with DNS, DHCP, Email and other infrastructure components and services.

iv. Identity Management Software (IMS)

1. System shall be able to identify and authorize and authenticate the user and would allow access to the applications and database based on the user identity.
2. Identity and access management system would be able to identify the rights available with the user in terms of viewing, addition, deletion, modification of the data and generation of various reports through MIS.
3. The system shall have log data facility for the users which are logging in the system, log out time with IP address etc.
4. It would be possible to revoke the rights of users
5. Privilege access/identity management tool shall be available

v. Chatbot

1. Emergency/ SoS from Citizen can be captured with the help of chatbot
2. Feedback from citizens of state shall be automated via use of chatbot

vi. e-Learning

1. e-Learning capabilities are required to enhance self and anytime learning of the users of Emergency Response system located all across the State
2. Interactive modules even video content would be available in English, Hindi
3. Changes in the training modules of e-Learning will be handled centrally
4. Attendance capturing is not available in the current application
5. Module and lesson tracking is not available to be upgraded in next stage
6. Attendance capturing shall be available with HRMS

vii. Backup Software

1. Backup software is used and allow users to create multiple copies and versions of important digital information.
2. Backup software protect data in case of an accidents, user mistakes, natural disasters, and equipment failure happen.
3. The backup software solution allows creating tape clone facility after the backup process.
4. The backup solution support integration of backup and restore with hardware cloning and snapshot features into the GUI, eliminating the traditional need to write user scripts

viii. SMS Gateway

1. SMS Gateway enable a computer to send and receive SMS text messages to and from a SMS capable device over the global telecommunications network.
2. It allows sending & Receiving Bulk SMS with easy-to-use web portal, Comprehensive APIs, plugins & More.
3. Automate texting in minutes by sending and receiving SMS.
4. The SMS Gateway provides the common service of SMS to the Police officials, citizens and PRVs

ix. Business Intelligence (BI)

UP112 has envisaged a solution that will help the organization to predict crime trends across the state based on past data. The envisaged analytics solution will help the department to streamline its operations and plan better resource deployment. The indicative list of functionalities is listed below-

1. Data Integration / Data Quality Enhancement
2. Crime Anticipation for Optimal Resource Deployment
3. Emergency Call Trends
4. Call Forecasting
5. Analyse Call Trends and Discover Patterns
6. Locality profiling
7. Search and Discovery

x. Video Management software (VMS)

The Video management software (VMS) will be used at centralized location in NexGen UP112 for Vehicle mounted cameras. Below is the minimum functionality supported by VMS but not limited to-

1. Collects video from cameras and other sources
2. Records / stores that video to a storage device
3. Provides an interface to both view the live video, and access recorded videos

4.27.8 Hardware for UP112

1. All of the IT hardware installed at DC, DRC, OMCs, Contact Centres, PRVs, DCRs have been accessed on the basis of re-utilization of the existing hardware to the maximum possible so that they are able to perform to similar standards in the NexGen UP112 with

uninterrupted services. More than 10,000 units of hardware, including PRVs hardware, have already been installed in the field and headquarters.

2. MSI may use the existing UP112 video walls for monitoring emergencies and related MIS.
3. For training purpose, the UP112 Lucknow is equipped with training rooms in terms of projector, screens, speakers etc. MSI has to ensure the replacement, upgradation, and maintenance of the system
4. MSI has to take care of the operation of Contact Centre and supporting centres which will have all necessary IT infrastructure like multi-screen desktops, printers, copiers, UPS etc.
5. MSI has to take care of the surveillance and access control system covering the entire building complex for monitoring activities
6. The approach opted by MSI is to best utilise the available hardware that is currently supported by the OEM, i.e., not fall under the category of "End of support" (EOS) which is duly opted for this project.
7. MSI has to replace all the items before 6 months of EOS as in below mentioned table of clause 4.27.8.
8. MSI has to ensure the Preventive Maintenance of all the hardware as per the schedule mentioned in section 9 annexure 30 and the same shall be monitored, reviewed, and integrated with Enterprise Management System (EMS).
9. All the consumables for hardware details as per section 9 annexure 29 need to provide by MSI
10. Below is the complete list of existing products either to be replaced or added as new ones or to be discontinued as per the requirements of project.

Definition of Options for NexGen UP112 -

- **Upgrade-** This means upgradation of the solution as per the specification mentioned in annexure xx. In case it requires a new solution to be proposed to meet the specification, the MSI shall provide the same.
- **Maintain and New**- Maintain means providing and managing the AMC of the existing solution till the EOS as per table below. New means new solution to be provided as per specification mentioned in annexure 9.1 before 6 Months of End of support (EOS)
- **New-** This means providing new Solution as per specification mentioned in anexxure 9.1

No Change- This means no change in the solution.

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
DC								
1	Biometric	1	Morpho	MA Sigma Multi	2028	Non-Critical	Biometrics Installed outside DC to avoid unauthorized access of DC	No Change

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
2	SAN Storage	1	HPe	HP 3PAR 8400	May-26	Critical	1. Required for storing the data 2. Existing system has 187 TB capacity out of which 26 TB space is available for usage	Maintain and New
3	VTL	1	HPe	HPE StoreOnce 5500	Dec-24	Critical	1. Virtual tape Library (VTL) advanced model Disk to Disk(D2D) Required for cold storing the data 2. Existing system has 250 TB capacity out of which 175 TB space is available for usage	Maintain and New
4	Voice gateway	8	Avaya	Avaya	Dec 27	Critical	Voice gateway is used to connect the enterprise VoIP network with the telecommunications	

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
							provider, using a number of different connectivity methods, such as PSTN, ISDN and SIP	
5	Database server	9	Cisco	UCS B200M4	Feb-24	Critical	Database server is used for database storage and retrieval	Maintain and New
6	Blade chassis	7	Cisco	UCS 5108	Dec-28	Critical	Hardware module where multiple servers can be hosted	New
7	Rack	8	Rittal	DKPS	Dec 27	Critical	Used for storing network equipment's such as server, storage, switches etc.	No Change
8	Blade Server-2 CPU	29	Cisco	UCS B200M4	Feb-24	Critical	Server for hosting multiple applications	Maintain and New
9	Blade server-4 CPU	8	Cisco	UCS B420M4	Feb-24	Critical	Server for hosting multiple applications	Maintain and New
10	Load Balancer	2	Array	APV 2600	Mar-23	Critical	Load balancer is device before servers which routes client requests across all servers in a manner that maximizes	New

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
							speed and capacity utilization and ensures that no one server is overworked, which could degrade performance. Two Sets of Link and Server Load Balancers are required for NexGen UP112	
11	200 kVA UPS	3	Hitachi	I4	2028	Critical	1. Backup source for powering up DC 2. Only 272 battery banks are required 3. Minimum 2 hrs battery backup is required	Upgrade and New New Only battery need to be replaced
12	Core Switch	2	Cisco	Cisco Nexus 7000	Feb-27	Critical	core switch is a high-capacity switch placed within the backbone or physical core of a network	Maintain and New
13	Managed Access Switch-24 ports	8	Cisco	Cisco 2960-X	Oct-27	Critical	Access switch is an interface that interacts with end devices	Maintain and New
14	SAN Switch	2	Hpe	HP SN Series	May-26	Critical	This will be used to	Maintain and New

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
							connect servers with SAN storage	
15	Aggregation Switch	2	Cisco	Nexus 56xx	Aug-26	Critical	Aggregation switch combines multiple networks connections	Maintain and New
16	Internet Router	2	Cisco	ISR 4000	Dec-27	Critical	1. This device is located at a network boundary and enables an internal network to connect to external networks 2. Upgrade to SDWAN for utilization of both TSP connectivity in parallel and for better monitoring	Maintain and New
17	Core router	2	Cisco	ASR 1006	Dec-27	Critical	1. This device communicates between the internet and the devices in DC that connect to the internet	Maintain and New

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
							2. Upgrade to SDWAN for utilization of both TSP connectivity in parallel and for better monitoring	
18	Web Application Firewall	2	Array	AWF 3500	Dec-22	Critical	A web application firewall is a specific form of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service	New
19	NexGen Firewall	2	Cisco	ASA 5585-X	Sep-25	Critical	A next-generation firewall (NGFW) is a security appliance that processes network traffic and applies rules to block potentially dangerous traffic	Maintain and New
20	Security Incident and Event Management	1	HPe	HP ArcSight ESM	Dec 27	Critical	This is used for identifying, monitoring, recording and analysing cybersecurity	Maintain and New

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
							events or incidents within a real-time IT environment	
21	Data Leakage Prevention (DLP)	2	Websense	DLP	2023	Critical	This software detects potential data breaches and prevents them by monitoring, detecting, and blocking sensitive data while in use (endpoint actions), in motion (network traffic), and at rest (data storage	New
22	Network Access Control (NAC)	2	Cisco	SNS-3515-K9	Jun-24	Critical	Network Access Control (NAC) is an approach to computer security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authenticatio	Maintain and New

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
							n and network security enforcement	
25	Host Based Intrusion Prevention System (HIPS)	2	Trend Micro	Deep Security	2028	Critical	The host intrusion prevention system blocks the activity and notifies the potential victims so they can take proper action against a threat actor or virus that tries to change the operating system. In NexGen UP112 HIPS will be part of IPS along with NIPS as part of Software.	New
26	Global Load balancer	2			New addition	Critical	Global server load balancing distributes the Internet traffic amongst a large number of connected servers in the DC	New
DRC (To be hosted on cloud in NexGen UP112 from existing on premises setup)								
1	SAN Storage	1	HPe	HP 3PAR 8400	May-26	Critical	1. Virtual tape Library (VTL) Required	Migration to Cloud

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
							for cold storing the data 2. Existing system has 134 TB capacity out of which 66 TB space is available for usage	
2	VTL	1	HPe	HPE StoreOnce 5500	Dec-24	Critical	1. Virtual tape Library (VTL) Required for cold storing the data 2. Existing system has 200 TB capacity out of which 100 TB space is available for usage	Migration to Cloud
3	Database server	4	Cisco	UCS B200M4	Feb-24	Critical	Database server is used for database storage and retrieval	Migration to Cloud
4	Blade chassis	5	Cisco	UCS 5108	Dec-28	Critical	Hardware module where multiple servers can be hosted	Migration to Cloud
5	Rack	8	Rittal	DKPS	Dec-28	Critical	Used for storing network equipment's	Migration to Cloud

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
							such as server, storage, switches etc.	
6	Blade server-2 CPU	19	Cisco	UCS B200M4	Feb-24	Critical	Server for hosting multiple applications	Migration to Cloud
7	Blade server-4 CPU	4	Cisco	UCS B420M4	Feb-24	Critical	Server for hosting multiple applications	Migration to Cloud
8	Load Balancer	2	Array	APV 2600	Mar-23	Critical	This is a device before servers which routes client requests across all servers in a manner that maximizes speed and capacity utilization and ensures that no one server is overworked, which could degrade performance	Migration to Cloud
9	Core Switch	2	Cisco	Cisco Nexus 7000	Feb-27	Critical	core switch is a high-capacity switch placed within the backbone or physical core of a network	Migration to Cloud
10	SAN Switch	2	HPe	HP SN Series	May-26	Critical	This will be used to connect servers with SAN storage	Migration to Cloud

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
11	Aggregation Switch	2	Cisco	Nexus 56xx	Aug-26	Critical	Aggregation switch combines multiple networks connections	Migration to Cloud
12	Internet Router	2	Cisco	ISR 4000	Dec-27	Critical	1. This device is located at a network boundary and enables an internal network to connect to external networks 2. Upgrade to SDWAN for utilization of both TSP connectivity in parallel and for better monitoring	Migration to Cloud
13	Core router	2	Cisco	ASR 1006	Dec-27	Critical	1. This device communicates between the internet and the devices in DC that connect to the internet 2. Upgrade to SDWAN for	Migration to Cloud

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
							utilization of both TSP connectivity in parallel and for better monitoring	
14	Web Application Firewall	2	Array	AWF 3500	Dec-22	Critical	A web application firewall is a specific form of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service	Migration to Cloud
15	NexGen Firewall	2	Cisco	ASA 5585-X	Sep-25	Critical	A next-generation firewall (NGFW) is a security appliance that processes network traffic and applies rules to block potentially dangerous traffic	Migration to Cloud
16	Security Incident and Event Management	1	HPe	HP ArcSight ESM	Dec 27	Critical	This is used for identifying, monitoring, recording and analysing cybersecurity events or incidents within a real-	Migration to Cloud

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
							time IT environment	
17	Data Leakage Prevention (DLP)	1	Websense	DLP	2023	Critical	This software detects potential data breaches and prevents them by monitoring, detecting, and blocking sensitive data while in use (endpoint actions), in motion (network traffic), and at rest (data storage	Migration to Cloud
18	Network Access Control (NAC)	2	Cisco	SNS-3515-K9	Jun-24	Critical	Network Access Control (NAC) is an approach to computer security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and	Migration to Cloud

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
							network security enforcement	
19	Host Based Intrusion Prevention System (HIPS)	1	Trend Micro	Deep Security	2028	Critical	The host intrusion prevention system blocks the activity and notifies the potential victims so they can take proper action against a threat actor or virus that tries to change the operating system	Migration to Cloud
UP112 Contact centre								
1	Biometric	17	Morpho	MA Sigma Multi	2028	Non-Critical	Biometric device placed in UP112 building for access and attendance purpose	No Change
2	Desktops including Hindi Keypad on Keyboard with two monitors	199	HP	HP ProDesk 600 G2 Small Form Factor Business PC	Feb-23	Critical	This device is used by Communication officers for creating events	New
3	Desktops including Hindi Keypad on Keyboar	200	HP	HP ProDesk 600 G2 Small Form Factor Business PC	Feb-23	Critical	This device is used by Dispatch Officers/District Supervisor	New

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
	d with triple monitors						for monitoring and event dispatch	
4	Desktops including Hindi Keypad on Keyboard with single monitor	233	HP	HP ProDesk 600 G2cSmall Form Factor Business PC	Feb-23	Critical	This device I used for other office works	New
5	Desktop Thin client including Hindi Keypad on Keyboard	10	HP	HP t628 Thin Client	Oct, 2023	Critical	This device is used for data centre monitoring	New
6	IP Phones with Headset	671	Avaya	9641G	2028	Critical	This device for COs, DOs and other staff for call taking	IP Phone- No Change Headset-New Y Jack Headset-New
7	Laptop	35	HP	HP Probook 450 G3	Dec-21	Non-Critical	For officers and other related staff	New
8	Printer, scanner, and copier (multi-function	10	HP	HP LaserJet Pro MFP M427fdn	Dec, 2028	Non-Critical	For printing, scanning etc.	No change
9	Heavy Duty printer	9	Ricoh	MPC 2003SP	Dec-22	Non-Critical	For printing, scanning etc.	New
10	Laser jet printer	10	HP	HP LaserJet Pro 400 M403dn	Dec, 2028	Non-Critical	For printing	No change
11	Paper shedder	5	GBC	Shred Master	Dec-22	Non-Critical	For disposal for documents	New
12	3 Conference room with equipment of capacity 15 people							

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
13	Training/ Video Conference equip	3	Extron	XPA 1002	Dec-28	Non-Critical	VC equipment's for training purpose	Upgrade
14	Control System	3	Extron	IP CP PRO 550	Dec-28	Non-Critical	VC equipment's for training purpose	Upgrade
15	2 Conference rooms with equipment of capacity 10 people							
I	Display device	2	Panasonic	TH 80LFB70W	Dec-22	Non-Critical	For viewing purpose in Conference room.	MSI may continue using the same device provided extended maintenance can be availed, if not bidder has to provide equivalent or higher model
ii	Audio System	2	Extron	XPA 1002	Dec-28	Non-Critical	VC equipment's for training purpose	Upgrade
iii	Control System	2	Extron	IP CP PRO 550	Dec-28	Non-Critical	VC equipment's for training purpose	Upgrade
16	2 Conference rooms with equipment of capacity 8 people							
I	Display device	2	Panasonic	TH 80LFB70W	Dec-22	Non-Critical	For viewing purpose in Conference room.	MSI may continue using the same device provided extended maintenance can be availed, if not bidder has to provide equivalent or higher model
ii	Audio System	2	Extron	XPA 1002	Dec-28	Non-Critical	VC equipment's for training purpose	Upgrade
iii	Control System	2	Extron	IP CP PRO 550	Dec-28	Non-Critical	VC equipment's	Upgrade

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
							for training purpose	
17	3 Conference room with equipment of capacity 20 people							
I	Display device	3	Panasonic	TH 80LFB70W	Dec-22	Non-Critical	For viewing purpose in Conference room.	MSI may continue using the same device provided extended maintenance can be availed, if not bidder has to provide equivalent or higher model
ii	Audio System	3	Extron	XPA 1002	Dec-28	Non-Critical	VC equipment's for training purpose	Upgrade
iii	Control System	3	Extron	IP CP PRO 550	Dec-28	Non-Critical	VC equipment's for training purpose	Upgrade
18	1 Meeting room with equipment of capacity 30 people							
I	Display device	1	Panasonic	TH 80LFB70W	Dec-22	Non-Critical	For viewing purpose in Conference room.	MSI may continue using the same device provided extended maintenance can be availed, if not bidder has to provide equivalent or higher model
ii	Audio System	1	Extron	XPA 1002	Dec-28	Non-Critical	VC equipment's for training purpose	Upgrade
iii	Control System	1	Extron	IP CP PRO 550	Dec-28	Non-Critical	VC equipment's for training purpose	Upgrade
19	2 Board rooms with equipment of capacity 30 people							
I	Display device	2	Panasonic	TH 80LFB70W	Dec-22	Non-Critical	For viewing purpose in	MSI may continue using

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
							Conference room.	the same device provided extended maintenance can be availed, if not bidder has to provide equivalent or higher model
Ii	Audio System	2	Extron	XPA 1002	Dec-28	Non-Critical	VC equipment's for training purpose	Upgrade
Iii	Control System	2	Extron	IP CP PRO 550	Dec-28	Non-Critical	VC equipment's for training purpose	Upgrade
20	2 training rooms with equipment of capacity 25 people							
I	Screen	2	Milan	Leolite Motorized 10'X8'	Dec-28	Non-Critical		No Change
Ii	Projector	2	Panasonic	PT VX 415 NZ	Dec-22	Non-Critical	Projector for training purpose	New
Iii	Audio system	2	Extron	XPA 1002	Dec-28	Non-Critical	Audio equipment for training purpose	Upgrade
Iv	Lapel Microphone	2	Mipro	ACT 311	Dec-28	Non-Critical	Microphone for training purpose	No Change
21	2 training rooms with equipment of capacity 50 people							
I	Screen	2	Milan	Leolite Motorized 12'X10'	Dec-28	Non-Critical	For viewing purpose in training room.	No Change
Ii	Projector	2	Panasonic	PT VX 415 NZ	Dec-22	Non-Critical	Projector for training purpose	New
Iii	Audio system	2	Extron	XPA 1002	Dec-28	Non-Critical	Audio equipment for training purpose	Upgrade
Iv	Lapel Microphone	2	Mipro	ACT 311	Dec-28	Non-Critical	Microphone for training purpose	Upgrade

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
22	1 Training rooms with equipment of capacity 50 people (35 Dos live training room)							
I	Screen	1	Milan	Leolite Motorized 12'X10'	Dec-28	Non-Critical	For viewing purpose in training room.	No Change
Ii	Projector	1	Panasonic	PT VX 415 NZ	Dec-22	Non-Critical	Projector for training purpose	New
Iii	Audio system	1	Extron	XPA 1002	Dec-28	Non-Critical	Audio equipment for training purpose	Upgrade
Iv	Lapel Microphone	1	Mipro	ACT 311	Dec-28	Non-Critical	Microphone for training purpose	No Change
23	Streaming Solution Device	1	Polycom	Group700	Dec-28	Non-Critical	This device is used for streaming the Video and Audio for Video conferencing purpose	Upgrade
24	Desktops with triple monitors	35	HP	HP ProDesk 600 G2 Small Form Factor Business PC	Feb-23	Non-Critical	This device is used by Dispatch Officers/District Supervisor for training purpose	New
25	IP Phones with Headset	35	Avaya	9641G	2028	Critical	This device is used by Dispatch Officers/District Supervisor for training purpose	IP Phone- No Change Headset-New Y Jack Headset-New
26	Tabletop microphone	35	Shure	MX 392/C	Dec-28	Non-Critical	This device is used by Dispatch Officers/District Supervisor for training purpose	No Change

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
27	VHF static radio device	29	Motorola	XiR M8668	Dec-22	Critical	This device is used by Dispatch Officers/District Supervisor for training purpose	New
28	Access Switch	2	Cisco	Cisco 2960-X	Oct-27	Critical	This device is used by Dispatch Officers/District Supervisor for training purpose	Maintain and New
29	MDT	1	Panasonic	FZ-B2	Dec-22	Critical	This device is used by Dispatch Officers/District Supervisor for training purpose	New
30	1 training rooms with equipment of capacity 100 people							
I	Screen	1	Milan	Loeolite Motorized 12'X10'	Dec-28	Non-Critical	For viewing purpose in training room.	No Change
Ii	Projector	1	Panasonic	PT VX 415 NZ	Dec-22	Non-Critical	Projector for training purpose	New
Iii	Audio System	1	Extron	XPA 1002	Dec-28	Non-Critical	Audio equipment for training purpose	Upgrade
Iv	Lapel Microphone	1	Mipro	ACT 311	Dec-28	Non-Critical	Microphone for training purpose	Upgrade
31	1 Training rooms with equipment of capacity 100 people (75 Cos live training room)							
I	Screen	1	Milan	Loeolite Motorized 12'X10'	Dec-28	Non-Critical	For viewing purpose in training room.	No Change
Ii	Projector	1	Panasonic	PT VX 415 NZ	Dec-22	Non-Critical	Projector for training purpose	New

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
Iii	Audio System	1	Extron	XPA 1002	Dec-28	Non-Critical	Audio equipment for training purpose	Upgrade
Iv	Lapel Microphone	1	Mipro	ACT 311	Dec-28	Non-Critical	Microphone for training purpose	No Change
32	Access Switch	4	Cisco	Cisco 2960-X	Oct-27	Critical	Access switch is an interface that interacts with end devices	Maintain and New
33	Tabletop microphone	75	Shure	MX 392/C	Dec-28	Non-Critical	Tabletop microphone for conferencing or meeting room	No Change
34	Streaming Solution Device	1	Polycom	Group700	Dec-28	Non-Critical	This device is used for streaming the Video and Audio for Video conferencing purpose	Upgrade
35	Desktops with double monitors	75	HP	HP ProDesk 600 G2 Small Form Factor Business PC	02-02-2023	Critical	This device is used by Communication officers for training purpose	New
36	IP Phones with Headset	75	Avaya	9641G	2028	Critical	This device is used by Communication officers for training purpose	IP Phone- No Change Headset-New Y Jack Headset-New
37	Video Conference equipment for 15 locations	15	Polycom	RealPresence Collaboration Server 1800 (MCU) Group 700 (end points)	Dec-28	Non-Critical	This device is used by Communication officers for training purpose	Upgrade
38	Digital light processi	3	Barco	MVL 721	Dec-28	Critical	Video wall in Cos room for	No Change

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
	ng (DLP) video wall						monitoring purpose	
39	Radio Gateway	1	Turbonet	ROIP-300DS	Dec-22	Non-Critical	This device is used by Communication officers for training purpose	New
40	VHF static radio device	29	Motorola	XiR M8668	Sep-21	Critical	This device is used by Communication officers for training purpose	New
41	Battery of VHF Static device	29	Exide	Power safe plus	Dec-22	Critical	This device is used by Communication officers for training purpose	New
42	lattice Mast and antenna for VHF static set	1	NA	NA	Discontinued	Non-Critical	This device is used by Communication officers for training purpose	New
43	Network Rack	2	Rittal	DKPS	Dec-28	Critical	Hosting Network equipment's of contact centre room	No Change
44	Managed Access Switch-24 ports	36	Cisco	Cisco 2960-X	Oct-27	Critical	Access switch is an interface that interacts with end devices	Maintain and New
45	Interactive Screen for EOC	2	Panasonic	TH 80LFB70W	Dec-22	Non-Critical	Interactive Screen for EOC.	MSI may continue using the same device provided extended maintenance can be availed, if not bidder has to provide equivalent or higher model

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
46	Tablets	24			New Addition	Non-Critical	Tablets for HQ officers	New
47	Dome camera	80	Honeywell	H4D3PRV2	Dec-28	Critical	Indoor cameras placed inside the building for surveillance	No Change
48	Bullet Camera	18	Honeywell	HBD3PR2	Dec-28	Critical	outdoor cameras placed in outdoor for surveillance	No Change
49	PTZ Camera	2	Honeywell	CALPSD1AI18WP CALIPSD1AI18WW	Dec-28	Critical	These cameras are used for 360-degree surveillance of the premises	No Change
50	24 Channel NVR	3	Honeywell	CALNVR8024B	Dec-28	Critical	Network video recorder with storage for viewing live and recorded videos	No Change
				OMC				
1	Desktops including Hindi Keypad on Keyboard with two monitors	58	HP	HP ProDesk 600 G2 Small Form Factor Business PC	Feb-23	Critical	This device is used by Communication officers for creating events in OMCs	New
2	Desktops including Hindi Keypad on Keyboard with triple monitors	32	HP	HP ProDesk 600 G2 Small Form Factor Business PC	Feb-23	Critical	This device is used by Dispatch Officers/District Supervisor for monitoring and event	New

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
							dispatch in OMCs	
3	Laptop	16	HP	HP Probook 450 G3	Dec-21	Non-Critical	For officers and other related staff	New
4	IP Phones with Headset	106	Avaya	9641G	2028	Critical	This device for COs, DOs and other staff for call taking in OMCs	IP Phone- No Change Headset-New Y Jack Headset-New
5	Printer, scanner and copier(multi-function)	4	HP	HP LaserJet Pro MFP M427fdn	Dec, 2028	Non-Critical	For printing, scanning etc.	No change
6	Laser jet printer	4	HP	HP LaserJet Pro 400 M403dn	Dec, 2028	Non-Critical	For printing, scanning etc.	No change
7	Heavy Duty printer	2	Ricoh	MPC 2003SP	Dec-22	Non-Critical	For printing, scanning etc.	New
8	Battery of VHF Static Device	58	Exide	Powersafe plus	Dec-22	Critical	Battery for VHF device	New
9	VHF static radio device	58	Motorola	XiR M8668	Sep-21	Critical	This device is meant for emergency communication between UP112 to DRC, UP112 to PRVs and DRC to PRVs	New
10	Lattice Mast and antenna for VHF static set	2	NA	NA	Discontinued	Non-Critical	For setting up Clear LOS between two points	New
11	Radio Gateway	2	Turbonet	ROIP-300DS	Dec-22	Non-Critical	It is the interface between two radio devices	New

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
12	2 Meeting rooms with equipment of capacity 20 people							
i	Display device	2	Panasonic	TH 80LFB70W	Dec-22	Non-Critical	For viewing purpose in Conference room.	MSI may continue using the same device provided extended maintenance can be availed, if not bidder has to provide equivalent or higher model
ii	Audio System	2	Extron	XPA 1002	Dec-28	Non-Critical	VC equipment's for training purpose	Upgrade
iii	Control System	2	Extron	IP CP PRO 550	Dec-28	Non-Critical	VC equipment's for training purpose	Upgrade
iv	Video Conferencing at 6Mbs	2	POLYCOM	Group 700	Dec-28	Non-Critical	Video conferencing system	Upgrade
13	Printer, scanner and copier(multi-function)	2	HP	HP LaserJet Pro MFP M427fdn	Dec, 2028	Non-Critical	For printing, scanning etc.	No change
14	Network Rack	2	Rittal	DKPS	Dec-28	Critical	For hosting network equipment	No Change
15	Managed Access Switch 24 ports	8	Cisco	Cisco 2960-X	Oct-27	Critical	Access switch is an interface that interacts with end devices	Maintain and New
16	Intranet Router - 500Mbps	4	Cisco	ISR 4400	Dec-27	Critical	1. This device is located at a network boundary and enables an internal network to	Maintain and New

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
							connect to external networks 2. Upgrade to SDWAN for utilization of both TSP connectivity in parallel and for better monitoring	
17	UPS 20 kVA	4	Hitachi	I4	2028	Critical	1. Backup power supply in OMCs 2. Only 120 battery banks are required 3. Minimum 2 hrs battery backup is required	Upgrade- SNMP card need to be added New-Battery only
18	Biometric	6	Morpho	MA Sigma Multi	2028	Non-Critical	This device will be used for access and attendance purpose in OMCs	No Change
19	Dome camera	16	Honey well	H4D3PRV2	Dec-28	Critical	Indoor cameras placed inside the building for surveillance	No Change
20	16 Channel NVR	2	Honey well	CALNVR2016B	Dec-28	Critical	Network video recorder with storage for	No Change

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
							viewing live and recorded videos	
21	Auto-phase sequence corrector in OMCs	2	NA		New addition	Non-Critical	This unit will prevent equipment stopping intermittently due to improper sequence of the incoming three stage power	New
22	Voltage control stabilization at OMCs	2	NA		New addition	Non-Critical	This device will do voltage correction from over and under voltage conditions	New
Field Hardware								
1	Desktops including Hindi Keypad on Keyboard with single monitor	201	HP	HP ProDesk 600 G2cSmall Form Factor Business PC	Feb-23	Critical	For officers and other related staff in District	New
2	Laptop	26	HP	HP Probook 450 G3	Dec-21	Critical	For officers and other related staff in District	New
3	Mobile Data Terminal Devices (MDT) minimum 7 inches screen	3275	Panasonic	FZ-B2	Dec-22	Critical	Given to 4W PRVs for accessing the information	New
4	Mobile Data Terminal Devices	1600	Zebra	TC 75X - Falcon	2023	Critical	Given to 2W PRVs for accessing	New

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
	(MDT) minimum 5 inches screen						the information	
5	Mobile Data Terminal Devices (MDT) minimum 7 inches screen (Fire Services)	280	Panasonic	FZ-B2	Dec-22	Critical	Given to 4W Fire PRVs for accessing the information	New
6	Mobile Data Terminal Devices (MDT) 5 inches screen (Fire Services)	380	Zebra	TC 75X - Falcon	2023	Critical	Given to 2W Fire PRVs for accessing the information	New
7	UPS 1 kVA	129	Hitachi	IP11-1	Dec-22	Critical	1. For Power backup in Districts 2. Only 272 battery banks are required 3. Minimum 2 hrs battery backup is required	New
8	Network Rack	130	Rittal	DKPS	NA	Critical	Hosting Network equipment of Districts	No Change
9	IP Phones with Headset	151	Avaya	9641G	2028	Critical		IP Phone- No Change Headset-New Y Jack Headset-New

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
10	VHF 4W antenna	3200	Motorola	XiR M8668	NA	Critical	Antenna for radio sets	New
11	Lattice Mast and antenna for VHF static set	129	NA	NA	Discontinued	Non-Critical	For setting up Clear LOS between two points	New
12	VHF static radio device	3326	Motorola	XiR M8668	Sep-21	Critical	This device is meant for emergency communication between UP112 to DRC, UP112 to PRVs and DRC to PRVs	New
13	Battery of VHF Handheld Radio Device and Charger of Battery pack	1600	Motorola	PMNN4463A	Dec-22	Critical	Battery for VHF device	New
14	VHF Handheld radio device	1600	Motorola	XiR P8668	Mar-23	Critical	Radio Handsets	New
15	Radio Gateway	129	Turbonet	ROIP-300DS	Dec-22	Non-Critical	It is the interface between two radio devices	New
16	Managed Access Switch 24 Ports	129	Cisco	Cisco 2960-X	Oct-27	Critical	Access switch is an interface that interacts with end devices	Maintain and New
17	Intranet Router 20Mbps	129	Cisco	C2911	Dec-22	Critical	1. This device is located at a network boundary and enables an internal network to	Maintain and New

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
							connect to external networks 2. Upgrade to SDWAN for utilization of both TSP connectivity in parallel and for better monitoring	
18	GPS Devices	6,600	New Procurement		New addition	Critical	This will be provided to all PRVs and this provides geolocation and time information to a GPS receiver anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites	New
19	Body worn Cameras	6,600	New Procurement		New addition	Critical	These are small cameras which can be clipped onto a police officer's uniform or worn as a headset and turned on to record video and audio of law	New

Sl.	Description	Existing Qty.	Existing OEM	Existing Model	EOS	Criticality	Details	Option for NexGen UP112
							enforcement encounters with the public	
20	Vehicle Mounted Cameras	668	New Procurement		New addition	Critical	PTZ camera mounted on the top of specially identified PRVs for surveillance purpose	New
21	RFID reader and tags	78 location	New Procurement		New addition	Non-Critical	This will be used for asset monitoring purpose; readers will be installed at each district and all the items which require monitoring will have RFID tags.	New

4.27.9 Cloud Service Requirement

Functional requirement of Cloud Service-

1. Virtual Machines and Compute Requirements-

a. The service shall be available online, on-demand and dynamically scalable up or down per request for service from the end users (The Client) with two factor authentications via the SSL through a web browser
b. Service shall provide auto-scalable, redundant, dynamic computing capabilities of virtual machines
c. Service shall allow users to securely and remotely load applications and data onto the computing or virtual machine instance from the SSL VPN clients only as against the public internet
d. Configuration and Management of the Virtual machine shall be enabled via a Web browser over SSL VPN/Secure tunnel as against the public internet

e. In case of suspension of a running VM, the VM shall still be available for reactivation for reasonable time without having to reinstall or reconfigure the VM for the Client solution. In case of suspension beyond a reasonable time, all the data within it shall be immediately deleted / destroyed and certify the VM and data destruction to the Client as per stipulations and shall ensure that the data cannot be forensically recovered.
f. The MSI shall ensure that VMs receive OS patching, health checking, Systematic Attack Detection, and backup functions.
g. Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network
h. CPU (Central Processing Unit) - CPU options shall be provided as follows:
i. A minimum equivalent CPU processor speed of 2.3GHz shall be provided.
j. The CPU shall support 64-bit operations
k. Provide hardware or software based virtual load balancer Services (VLBS) through a secure, hardened, redundant CSP Managed Virtual Load Balancer platform.
l. Provide hardware or software based virtual load balancing as a service to provide stateful failover and enable Customers to distribute traffic load across multiple servers.
m. Virtual Machines offered should be with the latest generation processor offered by the processor OEM.
n. Physical core to vCPU ratio should not be more than 1:2 for all proposed Virtual Machines
o. Ability to automatically increase/scale the number of Instances/VMs during demand spikes to maintain performance (i.e., 'scale-out')
p. Cloud service architecture should be in such a way that avoids VM outages or downtime when the provider is performing any kind of hardware or service maintenance at the host level
q. Required Operating System should be offered along with the Virtual Machines and should support external licenses by various OEMs.The OS offered should come with continuous updates and upgrades for the entire contract duration.
r. CSP should have capability to provide dedicated hosts in its native Cloud Infrastructure in India, which allows usage of existing third-party software license
s. The cloud environment in DRC shall be in active mode so that if DC fails, automatically the traffic gets switch over to DRC.

2. Storage Requirement

a. The service shall be available online, on-demand, and dynamically scalable up or down per request for service from the end users with two factor authentications via the SSL through a web browser.
b. Service shall provide scalable, redundant, dynamic storage
c. There shall not be any additional costs associated with data transfer over and above the ordinary bandwidth charges, or for bulk transfer for The Client.
d. For all volumes pertaining to production VMs, Solid State Device (SSD) based Block Storage should be offered with support of minimum 100 IOPS to maximum 16000 IOPS with 250 MB/S per volume

e. Block Storage with minimum monthly uptime of 99.99% or higher (as published in the CSP's Public Portal)
f. Object storage should be replicated across multiple DC's for better resiliency and should be designed for 99.99% availability.
g. Support complete eradication of data such that it is no longer readable or accessible by unauthorized users and/or third parties.
h. Offer server-side encryption of data 'at-rest', i.e., data stored on volumes and snapshots
i. Offer object storage tiering capability, i.e. the ability to recommend transitioning an object between object storage classes based on its frequency of access
j. All the data of VTL and SAN storage will be replicated on the cloud environment.

3. Database Requirement

a. For all Database instances, Solution should be offered with CSP's native Managed Relational Database as a Service with the following features
    I. CSP should be able to offer managed relational database service in the cloud for example: MySQL, PostgreSQL, SQL Server
    II. Support synchronous replication and automatic failover of a primary database to a standby database copy in a separate physical data centre to improve data redundancy
    III. Offer encryption of data 'at-rest' and 'in-transit'
    IV. Support the creation of on-demand (i.e., user-initiated) point-in-time copies (snapshots) and the restoration of a database instance using one of these copies
    V. Support vertically scaling the database instance (vCPU / Memory / Storage)
    VI. Support automated database backups
    VII. Minimum monthly uptime of 99.95% or higher (as published in the CSP's Public Portal)

4. VPC/Networking/Hybrid Connectivity requirement

a. Provide a virtual local area network (LAN) infrastructure and static IP addresses of non-internet routable addresses.
b. Ability to deploy VMs in multiple security zones, as required for the project, defined by network isolation layers.
c. Provide private connectivity between the Client's network and CSP's Data Centre facilities (Direct Connection/Express Route)
d. Provide infrastructure that allows to provide an external ipv6 address termination for applications hosted on Cloud
e. The data centre and disaster recovery centre facilities (where applicable) should support connection to the wide area network through high bandwidth links of appropriate capacity to take care of the needs of various types of user entities. Provision has to be made for segregation of access path among various user categories.

f. CSP shall have the capability to provide adequate bandwidth between Primary Data Centre and Disaster Recovery Centre for data replication purpose.
g. Support network level redundancy through MPLS links from two different service providers, alternate routing paths facilitated at ISP backbone (MPLS), redundant network devices etc.

4.27.10 Migration Strategy

a. Migration of Hardware

MSI to ensure the migration of existing hardware to latest hardware. One of the possible approaches can be that primary servers shall remain active while the secondary servers shall be turned off and can be replaced with the new hardware.

The existing system shall be migrated to the next generation technology with upgrades to latest security and safety features. The data of the existing system shall also be migrated from the existing operating environment to new operating environment.

b. Migration of Data

Data migration is a one-time process of transferring the existing data from one system to another; it includes various steps which are as follows: -

i. Identification
ii. Preparation
iii. Extracting
iv. Transforming (If required)
v. Storing
vi. Verification

Data replication is the periodic copying of data from a data source on one platform to a destination on another, while data integration combines data from disparate sources in a data warehouse destination or analysis tool.

The data at the last stage of UP112 operations must be retained as per archival policy. Various types of the data available with UP112 are textual, Voice, Image, Backup files, logs. These data must be migrated to new hardware and software to make it available to the user in NexGen UP112.

MSI to ensure that the data generated in Phase 1 and during NexGen shall be available on cloud. Thus, MSI to ensure timely migration of past data and regular scheduled replication of data to cloud. The data of UP112 shall be replicated in cloud environment on real time and structure of data sets should be same as that in DC. The cloud should be available in active mode.

c. Migration to cloud (Migration of all applications from on premise infrastructure to MEITY empaneled CSP (Cloud Service Provider))

Application and Infrastructure Discovery & Portfolio Analysis:

i. Formulate a baseline of the department's technical environment including inventory of both applications and infrastructure. This should also include development/testing environments in addition to the production environment.
ii. Document the technical details of the applications including technical architecture, integration with external solutions, underlying technologies / platforms, and underlying software. For each of the applications, capture the logical and physical deployment architecture providing the details of various architectural components (e.g., load balancer, firewall).
iii. For all the applications identify their dependencies on other components and services. Create a dependency tree that highlights all the different parts of the applications and identify their upward and downstream dependencies to other applications.

d. Migration of Software

The existing software of UP112 will be migrated to the latest available versions/upgrades to ensure the efficiency of the NexGen UP112. The software will be installed in a testing environment to check its performance and compatibility with the new/existing hardware. The software migration process refers to moving from one release level to a newer release. The process shall involve installing a new version of Tools and a new version of an existing Software applications.

Following software shall be migrated to the latest available NexGen versions (list not exhaustive): -

i. Operating Systems
ii. Firewall
iii. Antivirus
iv. Contact Centre Solution
v. Core CAD Application
vi. Database Management Software
vii. End User Applications

4.27.11 Integration with Other Agencies

With the objective of providing prompt integrated emergency response for public safety and security to all citizens anytime, anywhere in state of Uttar Pradesh, promoting ease of doing business, achieving excellence in service delivery and for effective governance, ITECCS is planning to integrate NexGen UP112 with various external agencies. The purpose of integrating with different agencies is to develop a mechanism to strengthen public safety as and when required as per information is received regarding allied agencies connected with UP112.

The objectives of integration with other regulators includes the following:

i. Seamless data exchange (including bulk data, structured and un-structured data exchange) and data verification for service delivery, data analytics, enforcement, etc.
ii. Improve inter-departmental efficiency and communication
iii. Provide better quality, efficient and prompt emergency services to citizens of state

Currently ITECCS is integrated with multiple government agencies at various levels that is integration is at:

a. Voice and Data Transfer i.e., event details transfer, call transfer level, voice recording transfer ***– L1 integration***
    1 In an L1 integration to-and-fro event related data sharing shall be possible between both the agencies event using API level integration
    2 An event can be logged at any of the end and can be shared
    3 Call can be exchanged between both the agencies
    4 UI would be common at both the ends

b. Data Sharing i.e., Event Details Sharing ***– L2 Integration***
    1 In an L2 integration to-and-fro event related data sharing shall be possible between both the agencies event using API level integration
    2 An event can be logged at any of the end and can be shared in defined format.
    3 Call transfer is not under this scope of work

c. Call taking of respective agency at ITECCS HQ ***– L3 Integration***

    1 An agency will deploy its resource at 112 HQ and their resource will use our infrastructure for call taking and event logging
    2 Data sharing with respective agencies using API level integration if the agency has infrastructure to support the data sharing

d. Receiving calls of respective agencies and logging data on respective platform ***– L4 Integration***
    1 No physical integration would exist between systems the communication officers of UP112 would entertain the calls for respective agency and log data to their respective web portals

Following is the list of possible indicative integrations (non-exhaustive list). MSI has to ensure that the system is flexible enough to ensure seamless integration with any agency.

a. GRP (L1 Integration)

Initially for integration between UP112 and GRP, 83 MDTs were provided to 65 GRP stations, which report to 6 SRP control rooms (Prayagraj, Kanpur, Agra, Meerut, Gorakhpur, and Lucknow). These control rooms are also provided with 6 RoIP terminals, whereas 1 terminal is provided at GRP HQ.

Thus, proposed integration architecture would be:

i. The created event will be directly transferred to the MDT of GRP and, parallelly, to the SRP terminal situated at the SRP control rooms as per jurisdiction. (Presently, events are routed through SRP terminal to the MDT of GRP PS). This event can be monitored at GRP HQ level as well.
ii. SMS will be directed through GRP MDT to the person travelling as per the roaster on a particular train. Additional UI would be integrated with the mobile responder and duty roaster, and an employee at the roaster would be directed with an SMS from GRP MDT regarding the incident in the train.

iii. SMS will be dispatched to the officers as per their jurisdiction according to SOP.
iv. An acknowledgement SMS will be sent to the caller.
v. SMS will be dispatched to the officers as per their jurisdiction according to SOP.
vi. SRP control room (6) employees can also be facilitated to immediately transfer the information to beat employees similar to GRP Thana.
vii. Action taken report provided by the beat party will be added to the event chronology.
viii. Feedback from citizens is shared with GRP.
ix. Also mapping of GRP boundary would be done on 112 maps.

b. Railway Protection Force (L1 Integration)

Integration with RPF can be considered for better emergency services to citizens on move. RPF control room can be fully integrated with UP112 HQ for exchange of audio and events related information like GRP

c. UPSRTC (Uttar Pradesh State Road Transport Corporation) (L2 Integration)

We have already established an API level integration with panic buttons devices installed in UPSRTC's 50 pink busses. Thus, for UPSRTC related triggers (SOS messages), dispatch section was taking actions as per designed SOP.

This integration was functional, and some events were created for triggers generated by panic buttons installed in the transport buses.

Thus, proposed integration architecture would be:

i. As per current information, 50 pink buses, 200 new roadway buses, and 12,000 old buses are to be added on their state tracking platform as per MORTH guidelines.
ii. All the panic triggers would land at UPSRTC platform and only the filtered one would be transferred to 112 for action related to Police intervention with details of information like bus number, driver and staff information, and map information.
iii. In an event of police intervention, PRV will communicate with the UPSRTC command and control centre. Medical, fire, and other assistance if required, the information from UP112 would be disseminated to the respective allied agencies.

d. 181 Women Helpline (L3 Integration)

As per MoU of services integration, dedicated channels and dedicated staff is provided for 181 related calls.

Thus, as per integration architecture:

i. There are 10 counselling staff, 04 team leaders and 2 Sub inspectors for feedback are involved in the 181
ii. Any Calls made by distress Caller to 181 – Women Helpline will be answered by Communication Officers at 112 and an event will be created.
iii. This Event is transferred over CAD to the concerned 181 officers in UP112 building
iv. This Event will also be dispatched simultaneously to the Supervisory terminal installed at 181 officers placed at 112 Building
v. 181 officers further counsel the victim and coordinate with one stop centre in district

vi. Event chronology is being maintained by counsellors.

e. 1090 Women Power Line (Women and Child Security Organisation) (L1 Integration)

Currently, we have established robust API level integration between 112 and 1090. Training has been provided to call takers at both the units. The communication officer records the 1090 event and sends it to the 1090 via the dedicated software level portal. Further, 1090 takes action on the same. In the same manner, 1090 records and sends the action pertaining to 112 intervention over API.

The proposed integration architecture would enable:

i. Centralized call taking for 1090 through 112 and only response-related activities can be performed by 1090, citizens would have a single number to call for all types of emergencies/counselling cells.
ii. If the above centralized call taking is not possible, then location detection, i.e., the LBS platform can be shared with 1090 along with POIs and layers of GIS maps so that a better location of the distressed caller can be detected and responded promptly. Later action taken and feedback can be shared with UP112 system
iii. SMS facility to Women related specific cases to 1090 official and citizen as well.
iv. Supervisor app facility to 1090 officials
v. Single button conference call between 1090/ caller/ call taker/ dispatcher/ PRV
vi. Truly seamless communication with dispatch officers for 1090 related calls till PRV reaches to victim

f. Safe Cities (L1 Integration)

As part of the Lucknow safe city project, it is already provisioned to create an interface of WPL1090 and UP112 platforms. There are other safe cities coming up in the state of Uttar Pradesh under Women and child safety.

Thus, proposed integration architecture would be:

In safe city, woman needs emergency of 112 and WPL1090 as well. Safe City ISCR operator will forward the call to UP112 along with the caller and event details. At UP112, communication officer will use the details forwarded by ISCR or can gather more details (if required) which are necessary for further action. Accordingly, UP112 communication officer will create an events and Dispatch Supervisor will assign the nearest police response vehicle (PRV) for further action. Even the location of cameras in the safe city will be plotted on the MAP of 112 as geo-coded. In future as per requirement the video of ISCR cameras can be seen by supervisors/ dispatchers at UP112

The steps involved in the process for integration are as follows:

i. Step 1- Distress woman calls ISCR Safe City helpline number. The operator at Safe City will access the case and decide whether the case shall be taken up at UP112 level.

ii. Step 2- The operator will access the case and create an event which will include all the required information of the women caller.
iii. Step 3- After gathering all the required information the operator at ISCR will forward the event to the UP112 for quick emergency response.
iv. Step 4- Dispatch Supervisor at UP112 will access the case and gather more information from the victim/caller (if required).
v. Step 5- After gathering Dispatch Supervisor assigns the event to nearest police response vehicle for quick emergency response. A message consisting information about PRV, contact no. and event details will be forwarded to the victim/caller along with a call from assigned PRV.
vi. Step 6- After taking the necessary actions as per SOP, UP112 will close the event and ATR is filled by the PRV and the same will be forwarded to ISCR for records.

g. Smart Cities (L2 Integration)

Smart city will be integrated like safe cities for events generated through Panic buttons/ SoS in the smart cities, further forwarded as a part of Command-and-control room of Smart city. In future viewing facility of CCTV cameras of Smart city would be available on geo-tagged map of UP112 through on-demand facility for supervision.

h. 101 Fire Services (L2 Integration)

Currently, 518 MDTs has been provided to fire department. These MDTs have been distributed across all fire stations of state.

Thus, as per current design:

i. Call taking takes place at UP112 HQ by COs
ii. Event Creation on CAD of UP112
iii. Dispatch by UP112
iv. Event details are shared with fire department via provided MDTs
v. Event Closer at MDT (provided by 112 to Fire department)
vi. Feedback for events to be obtained by UP112's communication officers
vii. Data Analysis on fire related events is performed by UP112

There have been challenges in this integration as MDTs are busy and events are being tagged to different fire stations. Also, challenges related to capacity building of fire employees, MDT usability, map navigation, supervision & monitoring issues by Fire staff etc.

Thus, proposed integration architecture would be:

i. There are around 284 fire stations and 1100 fire brigades in the state.
ii. The calls will land on 112 and, further, based on event classification, will be sent to the respective mobiles of the fire station. The fire station mobile will have the same count as the number of vehicles in the particular fire station. Approximately 1,100 mobile shall be present, and one event on each mobile is assigned to a specific fire station. If multiple vehicles are allotted to an event, but Fire RFP will bring one mobile with them at event location.

iii. All the vehicles would be fitted with GPS so that their movements can be tracked centrally.

iv. For supervision and better coordination, every district fire headquarters should have one MPLS connection, say 75 locations so that events can be easily tracked and monitored by the District Fire staff.

v. All the fire events registered at 112 should be taken for ATR and feedback as well.

i. 108 Medical Services (L1)

A two-way communication API level integration is well established and all 108 Master System Integrator dispatches vehicles on the request of 112. System is already working in an established software level connection.

Mapping of hospitals and ambulance locations in the map with calling facility to hospitals.

j. Cyber Helpline 1930 (L4 Integration)

The 1930 helpline was launched by the National Cybercrime Reporting Portal which comes under the Ministry of Home Affairs. There is as website provides a web page enabling victims of financial cyber fraud to feed details related to banking transactions and freeze the bank account to which the money is transferred. If the victim calls 112 and reports about such cyber frauds the same is being captured by communication officer in the National cybercrime reporting portal and acknowledgement number is transferred to victim.

k. 112 SOS Mobile App (L2 Integration)

The 112 SOS Mobile App is a part of the Emergency Response Support System (ERSS), a Govt of India initiative is already integrated with UP112 for registering the panic initiated by distress caller.

l. Expressway authorities (L1 Integration)

Express ways such as NHAI (National Highway Authority of India) – 1033, UPEIDA (Uttar Pradesh Expressways Industrial Development Authority), and YEIDA (Yamuna Expressways Industrial Development Authority) Express Way has their command and control centres running on their own for any emergency related to road security and surveillance. All such expressway command and controls will be integrated over API with 112 system for sharing the information regarding any distress information received at 112 where intervention of expressway authority is required and vice versa.

m. UPHP (Uttar Pradesh Highway Police) (L1 Integration)

UPHP has 50 vehicles and would be integrated for better coordination and supervision for vehicle tracking, information dissemination on highways from UP112. All the events as per devised SOP shall be transferred to UPHP vehicles for assistance. They would be also in beneficial for accidents on highways where special excavation equipment would be required. The financial may be borne by UPHP for establishing integration with UP112 with inventories like MDT, MDT software and connectivity

n. Disaster Management (L1 Integration)

The disaster management is integrated with 112 and SDMA control room has similar setup of system and CAD terminals. In future their software would be integrated on API with ours so

that in case of any emergency, event can be transmitted over system from both the parties. Even their inventories would be shared with UP112. Similar integration for other units like SDRF.

o. Uttar Pradesh Metro Rail Corporation (L2 Integration)

Uttar Pradesh Metro Rail Corporation has currently four projects Lucknow, Agra, Gorakhpur, and Kanpur Metro. All upcoming metro compartments are coming up with panic buttons which will be connected to their command room. All such panics where Police intervention is required would be forwarded from command room of Metro to 112 and such events recorded for metro related events will be transferred to Metro command room.

p. CRIS (Centre for Railway Information Systems) (L2 Integration)

The Summarized protocols for handling railway Emergency Calls at UP112:

i. Emergency calls would cover security, Safety, and medical issues by 139 helplines of railway on their own

ii. The extreme emergency calls shall be forwarded from UP112 only if it has taken place on train or Railway Stations or other Railway territory.

iii. Calls related to Railways general inquiry etc. would not be handled by UP112 nor would they be transferred from UP112 to Railways helpline 139

For smooth functioning of the system, Railways to ensure the following:

i. Call received through 112 may be given high priority at 139

ii. All emergency contact numbers of zone/division provided for the purpose remain operational 24*7 to attend any call made in emergency situation with Sanchar portal at UP112

iii. There may be occasions when incident would have taken place in some other zone/division but 112 call handling agents being not familiar with Indian Railways demarcation of Zone/division system. Such call or taken up the matter with some other Zone/division which does not have jurisdiction on the place where incident has taken place actually. E.g., Lucknow falls in NR Zone, however,112 caller may take up with NER. In such a case, taking into consideration the gravity of situation, call receiving Zone/division should ensure immediate appropriate action instead of passing on to the railways under who jurisdiction, the incident falls. Concerned railway shall certainly come forward in due course for action needed in the situation.

iv. Zonal railways should ensure that all information related to incident is timely fed in SIMS portal Safety Information Management System (SIMS).

v. Objective is to integrate SIMS with UP112 portal over API so that emergencies can be timely transferred

q. CM Helpline (L2 Integration)

CM helpline is integrated with 112 for transferring the events manually, now API level integration is envisioned so that all enquiry related to CM helpline can be registered and forwarded to CM helpline and all first responder intervention related events would be captured and forwarded to UP112.

r. UP COP Integration (Application Integration)

UP COP application shall be integrated with UP 112, this includes integration of Chatbot application of UP112 on UP COP application and this will act as an interface of Citizen with UP 112. Any related developments, coding, support, customization needs to be done, will be under scope of MSI.

s. CCTNS Integration

Police station Module of UP112 shall be available to CCTNS team of technical services and any other police unit on need and request basis.

t. Link Integration

112 has established channels which any business institution can use to send alarm triggers to UP112 so that 112 can send a PRV. UP112 will register the locations and will assign an identification number. Business Institution's command center will receive and process the alarm triggers. The ones requiring police assistance will be forwarded to the 112 Contact Center. A PRV will be dispatched accordingly. Thus, to make state more business conducive functionalities of LINK Project shall be integrated with UP112 core system.

4.28 Human Resource

UP112 project would require provisioning of dedicated manpower at various locations having different skill sets to provide support during entire project duration. The details of the manpower needed are described henceforth.

4.28.1 Technical Manpower

In order to effectively manage the entire operations and performance of the project a pool of technical resources are required in two different phases of the project i.e.,

1. Implementation and Migration Phase: In this phase, the MSI shall provide services for design, customization, installation, commissioning, integration & migration for emergency response system (UP112 ERSS). Duration of this phase shall be 5 months from the date of acceptance of LOI by MSI.

2. Operation and Maintenance Phase: In this phase, MSI shall be responsible for operations and maintenance of entire technology solution for the contract period. This shall start after Implementation phase. Duration of this phase shall be 60 months after the Implementation phase of UP112 Project.

I. MSI shall provide adequate number of personnel each responsible for a specific role within the project. MSI must provide clear definition of the role and responsibility of each individual personnel.

II. MSI shall have a defined hierarchy and reporting structure for various teams that shall be part of the project.

III. Changes in number of Manpower resources will have to be approved by GoUP.

IV. Appointment/replacement of manpower deployment will have to be approved by the competent authority at UP112.

Note:

- Initial appointment assessment shall be evaluated by MSI in presence of the dedicated team of officials and consulting body at UP112.
- Any mid-term changes in employment of the resources shall be approved by the dedicated team of officials and consulting body at UP112.

V. The MSI shall be responsible for compliance of labour laws in respect of the personnel employed by them. The MSI shall be the employer for its workers and the ITECCS will not be held responsible fully or partially for any dispute that may arise between the MSI and its workers. ITECCS as a Principal Employer, bears a “limited responsibility” as per the relevant prevalent laws.

VI. MSI shall be responsible to ensure 100% manpower all days including festive seasons.

VII. The following table provides a list of resource categories and the minimum resource requirements estimated for the different sites. However, MSI shall independently estimate the teams size required to meet the requirements of Service Levels as specified as part of this tender. MSI to bear the financial costing of the resources in case of addition to maintain the SLAs. MSI shall propose qualified personnel with adequate skills levels to manage the infrastructure / components envisaged as part of this project.

Table: Minimum human resource requirement during implementation and migration phase

Technical Manpower: During implementation and migration phase								
#	**Role Description**	**Key Personnel Yes/No**	**Onsite/ Offsite**	**Minimum No. of Resources**	**Deployment**	**Minimum Qualifications**	**Minimum Experience**	**Minimum Certification**
1	Project Director/ Manager	Yes	Onsite	1	100%	(M.Tech / B. Tech/ BE) + MBA (Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢ Minimum 15 years of experience ➢ Working in projects related to implementation of IT with an experience of 5 years or more in project management role leading a team of 40 or more members. ➢ Should have overall experience of 5 or more years in Government projects	PMP/Prince 2
2	Solution Architect (DC, DR)	Yes	Onsite	1	100%	M.Tech/ B.Tech / B.E (Note: M.Tech/ B.Tech/ BE should be from either of the below streams:	➢ Minimum 10 years of experience in infrastructure architecture design, installation, commissioning, and management in such large scale ERSS/ITeS projects in Government or Private sector ➢ Should have experience in implementing at least 3 projects in	Microsoft Certified Systems Engineer (MCSE)/ CCNA (Cisco Certified Network

Technical Manpower: During implementation and migration phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	the proposed tier-II & tier III &/or tier IV DC/DR solutions / architecture	Associate)/ CCNP (Cisco Certified Network Professional) / Cisco Certified Network Professional CCIE (Data centre) Note: Lab attempted Applicable) / TOGAF (Open Group Architecture Framework)
3	Solution Architect (Applications)	Yes	Onsite	1	100%	M.Tech/ B.Tech/ BE/MCA (Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering	➢ Minimum 10 years of experience in Application Development / Solution Architect ➢ Should have experience of more than 5 years as Solution Architect in large projects of similar nature ➢ Should have architected at least two such large scale ERSS/ITeS projects in Government or Private Sector ➢ Should have experience in	TOGAF (Open Group Architecture Framework) / Certified System Architect (CSA)

Technical Manpower: During implementation and migration phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	implementing at least 3 projects in the proposed enterprise/solution architecture	
4	Solution Architect (Network)	Yes	Onsite	1	100%	➢ M.Tech / B. Tech/ BE/MCA (Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢ Minimum 10 years of experience in Network design/solution ➢ Shall have the ability address specialized complex infrastructure and network architectural issues	CCNA/CCNP (R&S or Voice) / CWNA (Certified Wireless Network Administrator (CWNA) /TOGAF/ CCIE (R&S or Voice) (Note: Lab attempted Applicable)

Technical Manpower: During implementation and migration phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
5	Solution Architect (Information Security)	Yes	Onsite	1	100%	➢ M.Tech / B.Tech / B.E. / MCA (Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢ Minimum 10 years of experience in managing large scale projects involving Information Security/ Cyber Security ➢ Should have experience in design and implementation of Information Security policy for complex and large scale IT application deployments ➢ Should have done assignments involving assessment of information security policies and should be able to identify areas of improvements in the information security architecture ➢ Should have specialization on a range of solutions, including, but not limited to, making appropriate use of PKI, intrusion detection or prevention, VPN, single sign-on, firewalls, and all elements of network-level security.	CISA (Certified Information Systems Auditor)/ ISO27001/ CCIE (Security) Note: Lab attempted Applicable)/ TOGAF

Technical Manpower: During implementation and migration phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deploy ment	Minimum Qualifications	Minimum Experience	Minimum Certification
6	Database Architect or Modeler	Yes	Onsite	2	100%	M.Tech or B.Tech/B.E/ MSc.(Computer Science or IT) / MCA (Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢Minimum 10 years of experience in managing Technology project from Database perspective ➢ Should have experience in implementing the proposed database solution and relevant certification in the proposed database ➢ Should have extensive experience in, creation of schemas, table spaces, define number of users in the database, create user profiles, memory utilization, caching etc ➢ Should have experience in monitoring and maintenance of databases, installation of database software patches, monitoring of database backups, standardization, and implementation of database	DBA Architect level Certification for the proposed database
7	Database Administrator	Yes	Onsite	3	100%	➢ M.Tech / B.Tech/B.E/ MCA (Note: M.Tech/ B.Tech/ BE should be from either of the below streams:	➢ Minimum of 6 years' experience as a database administrator. ➢ A good understanding of the underlying operating system. Knowledge of the physical database design. Ability to perform both database and operating	DBA Administrator level Certification for the proposed database

Technical Manpower: During implementation and migration phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deploy ment	Minimum Qualifications	Minimum Experience	Minimum Certification
						➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	system performance tuning and monitoring. ➢Proficiency with data manipulation languages such as MS SQL, Oracle Database, and Hadoop ➢Programming with experience in handling standby databases preferred.	
8	System Administrator	Yes	Onsite	2	100%	➢ M.Tech / B.Tech/B.E/ MCA (Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication	➢ Minimum 6 years' experience as a system administrator. ➢ Experience in sys admin of RDMB data (MS-SQL, Oracle etc.), sysadmin windows-2008/2012 etc. server, programmer of .NET, SQL, PL/SQL, etc.	Relevant certification - Microsoft Certified Systems Administrator (MCSA)/ Oracle Linux System Administrator (Oracle)

Technical Manpower: During implementation and migration phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						➢ Electronics & Tele-communication)		
9	Network Administrator	Yes	Onsite	2	100%	➢ M.Tech / B.Tech/B.E/ MCA (Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢ Minimum 6 years' experience as a system administrator. ➢ Candidate should be well versed with Routing and Switching devices and technologies like ATM, Frame Relay, MPLS, Wireless, Broadband and Protocol Analysis Tools. ➢ Must have intermediate skills in Information Security technologies like Anti-virus, Firewalls, 2 & 3 factor Authentication, IDS, IPS, Content Filtering, Encryption, VPN, Threat Management and be familiar with Information Security Audit parameters.	CCNA /CCNP (R&S)/CCNP (Voice)/ Checkpoint Certified Security Administrator. (CCSA)/ CWNA
10	Business Analyst	Yes	Onsite	1	100%	➢ M.Tech / B.Tech/B.E	➢ Minimum 5 years' of experience in monitoring-of IT/e- Governance projects with Minimum of 3 years'	

Technical Manpower: During implementation and migration phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						(Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	experience in same role ➢ Should have experience in the complete requirements management cycle using hybrid waterfall and agile methodologies of a large project spanning 2-3 years with multiple releases ➢ Hands on experience with requirement management platforms within the DevOps framework to understand large RFPs, capture user requirements, functional requirements, and software &system requirements, good understanding of ISO and IEEE requirements engineering standards	
11	CAD Expert (from OEM)	Yes	Onsite	3	100%	➢ M.Tech / B.Tech/B.E/ MSc.(Computer Science or IT) / MCA (Note: M.Tech/ B.Tech/ BE should be from either of the below streams:	➢ Minimum 10 years of relevant experience along with minimum of 3 years of working experience in CAD domain	OEM certifications

Technical Manpower: During implementation and migration phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)		
12	GIS Expert (from OEM)	Yes	Onsite	1	100%	➢ M.Tech / B.Tech/B.E/ M.Sc. (Computer Science or IT) / MCA OR Full time Post Graduation degree in Geology / Geo-informatics / Remote Sensing / or related subject (Note: M.Tech/ B.Tech/ BE should be from either of the below streams:	➢ Minimum 8 years of relevant experience of large-scale project involves GIS component	OEM certifications

Technical Manpower: During implementation and migration phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)		
13	Telephony & ACD expert (from OEM)	Yes	Onsite	3	100%	➢ M.Tech / B.Tech/B.E/ M.Sc. (Computer Science or IT)/MCA (Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics	➢ Minimum 10 years of relevant experience	OEM certifications

Technical Manpower: During implementation and migration phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						➢ Electronics & Communication ➢ Electronics & Tele-communication)		
14	Radio over IP specialist (from OEM)	Yes	Onsite	1	100%	➢ M.Tech / B.Tech/B.E M.Sc. (Computer Science or IT)/MCA (Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢ Minimum 10 years of relevant experience	OEM certifications
15	Cloud Architect	Yes	Onsite	1	100%	➢ B. Tech / B.E or MCA with at-least 5 years of experience in at		

Technical Manpower: During implementation and migration phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						least two MEITY empanelled cloud environments ➢ Experience designing, executing, and supporting cloud solutions. ➢ Experience in Cloud Migration ➢ Experience in Implementing DevOps Pipelines Experience in Cloud based Version Control applications Excellent knowledge of cloud computing technologies and current computing trends		
16	Monitoring centre configuration and customization expert	Yes	Onsite	1	100%	➢ M.Tech / B.Tech/B.E/MCA (Note: M.Tech/ B.Tech/ BE should be from either of the below streams:	➢ Minimum 6 years of relevant experience	ITIL Certification

Technical Manpower: During implementation and migration phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)		
17	Application Developers	Yes	Onsite	4	100%	➢ M.Tech / B.Tech/B.E/MCA/ MSc.(Computer Science or IT) (Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics	➢ Minimum 8 years of relevant experience in Application Development (Web/Desktop/mobile) and Database Management. ➢ Familiarity with cloud message APIs and push notifications ➢ Understanding of Google s Android design principles and interface guidelines ➢ Ability to design/develop/support new/existing apps, and perform unit testing and integration testing	Certified Web Professional - Web Developer/ Certified Software Development Professional (CSDP)/ Proposed solution certification (OEM specific)

Technical Manpower: During implementation and migration phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						➢ Electronics & Communication ➢ Electronics & Tele-communication)		
18	Application Tester	Yes	Onsite	2	100%	➢ B.Tech / B.E./ /BCA / MSc.(Computer Science or IT) /B.sc (CS or IT)	➢ Minimum 6 years of relevant experience	Certified Software Tester (CSTE)/ Certified Manager of Software Testing (CMST)/ ISTQB Agile Tester Certification/ /Advanced Level Agile Technical Tester/Certified Software Test Professional Associate

Technical Manpower: During implementation and migration phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
								Level (CSTP-A)
19	Master Trainer	Yes	Onsite	1	100%	➢ (M.Tech/ B.Tech / B.E./ MCA/ MSc. and M.Ed)	➢ Minimum 8 years of relevant experience in conducting training ➢ Experience in corporate HR training would be additional asset.	
20	Documentation Specialist	Yes	Onsite	4	100%	Graduate in any discipline	➢ Minimum 7 years of relevant experience ➢ Relevant experience in Technical and administrative documentation in Government sector. Excellent/Good: Reading, Writing, and Speaking skills in Hindi and English ➢ Experience in formatting documents according to SOP regulatory requirements	
21	GIS Data Support Staff	Yes	Onsite	2	100%	B.Tech/B.E/ MSc.(Computer Science or IT) / BCA OR Full time Post Graduation degree in Geology / Geo-informatics / Remote	➢ Minimum 5 years of relevant experience	OEM certifications

Technical Manpower: During implementation and migration phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						Sensing / or related subject		
22	Geo Fencing Staff	Yes	Onsite	2	100%	B.Tech/B.E/ MSc.(Computer Science or IT) / BCA OR Full time Post Graduation degree in Geology / Geo-informatics / Remote Sensing / or related subject	➢ Minimum 5 years of relevant experience	OEM certifications
23	SOC Expert	Yes	Onsite	2	100%	➢ M.Tech/ B.Tech / B.E/ MCA (Note: Note: M.Tech/B.Tech/BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢	➢ Minimum 7 years of relevant experience in Incident responder, Security investigator, Advanced security analyst, Security engineer/ architect. ➢ Should have knowledge on networking and security	At least one industry leading SIEM product and preferably other leading certifications in security, such as CISA/CISM /CRISC

Technical Manpower: During implementation and migration phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						Electronics & Tele-communication)		
24	VAPT Expert	Yes	Onsite	1	100%	➢ M.Tech /B.Tech/ B.E./ MCA (Note: M.Tech/B.Tech/BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢ Minimum 7 years of relevant experience	Certification in at least one industry leading SIEM product and preferably CEH
25	Data Migration Expert	Yes	Onsite	2	100%	➢ M.tech /B.Tech/ B.E./ MCA (Note: M.Tech/B.Tech/BE should be from either of the below streams:	➢Minimum 10 years of experience ➢Having strong understanding of master data ➢ Experience in multiple implementation/ rollout project	DBA Certification for the proposed database

Technical Manpower: During implementation and migration phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deploy ment	Minimum Qualifications	Minimum Experience	Minimum Certification
						➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	experience specifically working actively on data migration, data mapping, data load testing, and process issue analysis tracing to master data relevant to the issue	
26	IT Security & asset Manager	Yes	Onsite	3	100%	➢ M.tech /B.Tech/ B.E. / MCA (Note: M.Tech/B.Tech/BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢ Minimum 8 years of relevant experience in managing large scale projects involving Information Security/ Cyber Security ➢ Should have experience in design and implementation of Information Security policy for complex and large scale IT application deployments ➢ Should have done assignments involving assessment of information security policies and should be able to identify areas of improvements in the information security architecture ➢ Should have designed information security architectures	➢ Desirable to have Industry standard security certifications on the proposed solution/ ITIL

Technical Manpower: During implementation and migration phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
							for large internet-based applications for safeguarding against security threats, vulnerabilities, cyber and phishing attacks ➢ Should have specialization on a range of solutions, including, but not limited to, making appropriate use of PKI, intrusion detection or prevention, VPN, single sign-on, firewalls, and all elements of network-level security.	
27	ERSS Domain Expert	Yes	Onsite	1	100%	➢ M.tech /B.Tech/ B.E./ MCA (Note: M.Tech/B.Tech/BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢	➢ Minimum 5 years of relevant experience	

Technical Manpower: During implementation and migration phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deploy ment	Minimum Qualifications	Minimum Experience	Minimum Certification
						Electronics & Tele-communication)		
28	District technical Support	No	Onsite	78	100%	➢ B. Tech / B.E. / BCA / M.Sc. (IT) (Note B. Tech /BE should be from either of the below stream: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢ Minimum 3 years' experience in IT Support Roles	
Total				**127**				

Table: Minimum human resource requirement during Operations and Maintenance (O&M) phase

Technical Manpower: During Operation and Maintenance phase								
#	**Role Description**	**Key Personnel Yes/No**	**Onsite/ Offsite**	**Minimum No. of Resources**	**Deployment**	**Minimum Qualifications**	**Minimum Experience**	**Minimum Certification**
1	Project Director/ Manager	Yes	Onsite	1	100%	(M.Tech / B. Tech/ BE) + MBA (Note: M.Tech/B.Tech/BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢ Minimum 15 years of experience ➢ Working in projects related to implementation of IT with an experience of 5 years or more in project management role leading a team of 40 or more members. ➢ Should have overall experience of 5 or more years in Government projects	PMP/Prince 2
2	Solution Architect (DC, DR)	Yes	Onsite	1	25%	M.Tech/ B.Tech / B.E (Note: Note: M.Tech/B.Tech/BE should be from either of the below streams: ➢ Information Technology	➢ Minimum 10 years of experience in infrastructure architecture design, installation, commissioning, and management in such large scale ERSS/ITeS projects in Government or Private	MCSE/ CCNA/CCNP/ CCIE (Data centre) Note: Lab attempted Applicable) / TOGAF

Technical Manpower: During Operation and Maintenance phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	sector ➢ Should have experience in implementing at least 3 projects in the proposed tier-II & tier III &/or tier IV DC/DR solutions / architecture	
3	Solution Architect (Applications)	Yes	Onsite	1	25%	M.Tech/ B.Tech / B.E / MCA Note: M.Tech/B.Tech/BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢ Minimum 10 years of experience in Application Development / Solution Architect ➢ Should have experience of more than 5 years as Solution Architect in large projects of similar nature ➢ Should have architected at least two such large scale ERSS/ITeS projects in Government or Private Sector ➢ Should have experience in implementing at least 3	TOGAF/ Certified System Architect (CSA)

Technical Manpower: During Operation and Maintenance phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
							projects in the proposed enterprise/solution architecture	
4	Solution Architect (Network)	Yes	Onsite	1	25%	➢ M.Tech / B. Tech/ BE/ MCA (M.Tech/B.Tech/BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢ Minimum 10 years of experience in Network design/solution ➢ Shall have the ability address specialized complex infrastructure and network architectural issues	CCNA/CCNP(R&S or Voice) / CWNA/TOGAF/ CCIE (R&S or Voice) Note: Lab attempted Applicable)

Technical Manpower: During Operation and Maintenance phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
5	Solution Architect (Information Security)	Yes	Onsite	1	25%	➢ M.Tech / B.Tech / B.E. / MCA (M.Tech/B.Tech/BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢ Minimum 10 years of experience in managing large scale projects involving Information Security/ Cyber Security ➢ Should have experience in design and implementation of Information Security policy for complex and large scale IT application deployments ➢ Should have done assignments involving assessment of information security policies and should be able to identify areas of improvements in the information security architecture ➢ Should have specialization on a range of solutions, including, but not limited to, making appropriate use of PKI, intrusion detection or prevention, VPN, single	CISA / ISO27001/ CCIE (Security) Note: Lab attempted Applicable)/ TOGAF

Technical Manpower: During Operation and Maintenance phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
							sign-on, firewalls, and all elements of network-level security.	
6	Database Architect or Modeler	Yes	Onsite	1	25%	M.Tech or B.Tech/B.E/ MCA/ MSc.(Computer Science or IT) (M.Tech/B.Tech/BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢Minimum 10 years of experience in managing Technology project from Database perspective ➢ Should have experience in implementing the proposed database solution and relevant certification in the proposed database ➢ Should have extensive experience in, creation of schemas, table spaces, define number of users in the database, create user profiles, memory utilization, caching etc ➢ Should have experience in monitoring and maintenance of databases, installation of database software patches, monitoring of	DBA Certification for the proposed database

Technical Manpower: During Operation and Maintenance phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
							database backups, standardization, and implementation of database	
7	Database Administrator*	Yes	Onsite	4*	100%	➢ M.Tech / B.Tech/B.E/ MCA (Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢ Minimum of 6 years' experience as a database administrator. ➢ A good understanding of the underlying operating system. Knowledge of the physical database design. Ability to perform both database and operating system performance tuning and monitoring. ➢Proficiency with data manipulation languages such as MS SQL, Oracle Database, and Hadoop ➢Programming with experience in handling standby databases preferred.	DBA Certification for the proposed database

Technical Manpower: During Operation and Maintenance phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
8	System Administrator*	Yes	Onsite	4*	100%	➢ M.Tech / B.Tech/B.E/ MCA (Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢ Minimum 6 years' experience as a system administrator. ➢ Experience in sys admin of RDMB data (MS-SQL, Oracle etc.), sysadmin windows-2008/2012 etc. server, programmer of .NET, SQL,PL/SQL, etc.	Relevant certification - Microsoft Certified Systems Administrator (MCSA)/ Oracle Linux System Administrator (Oracle)
9	Network Administrator*	Yes	Onsite	4*	100%	➢ M.Tech / B.Tech/B.E / MCA (Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology	➢ Minimum 6 years' experience as a system administrator. ➢ Candidate should be well versed with Routing and Switching devices and technologies like ATM, Frame Relay, MPLS, Wireless, Broadband and	CCNA /CCNP (R&S)/CCNP (Voice)/CCSA/ CWNA

Technical Manpower: During Operation and Maintenance phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	Protocol Analysis Tools. ➢ Must have intermediate skills in Information Security technologies like Anti-virus, Firewalls, 2 & 3 factor Authentication, IDS, IPS, Content Filtering, Encryption, VPN, Threat Management and be familiar with Information Security Audit parameters.	
10	CAD Expert (from OEM)	Yes	Onsite	1	100%	➢ M.Tech/ B.Tech/ BE/ MCA/ MSc.(Computer Science or IT) (M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢	➢ Minimum 10 years of relevant experience along with minimum of 3 years of working experience in CAD domain	OEM certifications

Technical Manpower: During Operation and Maintenance phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						Electronics & Tele-communication)		
11	GIS Expert (from OEM)	Yes	Onsite	1	50%	M.Tech / B.Tech/B.E/MCA/ MSc.(Computer Science or IT) OR Full time Post Graduation degree in Geology / Geo-informatics / Remote Sensing / or related subject (M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢ Minimum 8 years of relevant experience of large-scale project involve GIS component	OEM certifications
12	Telephony & ACD expert (from OEM)	Yes	Onsite	1	100%	➢ M.Tech / B.Tech/B.E/ MCA/	➢ Minimum 10 years of relevant experience	OEM certifications

Technical Manpower: During Operation and Maintenance phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						MSc.(Computer Science or IT) (Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)		
13	Cloud Architect	Yes	Onsite	1	100%	➢ B. Tech / B.E or MCA with at-least 5 years of experience in at least two MEITY empanelled cloud environments ➢ Experience designing, executing, and		

Technical Manpower: During Operation and Maintenance phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						supporting cloud solutions. ➢ Experience in Cloud Migration ➢ Experience in Implementing DevOps Pipelines ➢ Experience in Cloud based Version Control applications Excellent knowledge of cloud computing technologies and current		
14	Senior Application Developers	Yes	Onsite	2	100%	➢ M.Tech/B.Tech/BE/ MCA/ MSc.(Computer Science or IT) (Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering	➢ Minimum 8 years of relevant experience in Application Development (Web/Desktop/mobile) and Database Management. ➢ Familiarity with cloud message APIs and push notifications ➢ Understanding of Google s Android design principles and interface guidelines ➢ Ability to	Certified Web Professional - Web Developer/ Certified Software Development Professional (CSDP)/ Proposed solution certification (OEM specific)

Technical Manpower: During Operation and Maintenance phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	design/develop/support new/existing apps, and perform unit testing and integration testing	
15	Master Trainer	Yes	Onsite	1	100%	(M.Tech/ B.Tech / B.E./ MCA/ (M.sc. + M.Ed) (Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢ Minimum 8 years of relevant experience in conducting training ➢ Experience in corporate HR training would be additional asset.	
16	GIS Data Support Staff	Yes	Onsite	1	100%	B.Tech/B.E/BCA/ M.Sc. OR Full time Post Graduation degree in Geology / Geo-informatics / Remote	➢ Minimum 5 years of relevant experience	OEM certifications

Technical Manpower: During Operation and Maintenance phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						Sensing / or related subject		
17	SOC Expert*	Yes	Onsite	4*	100%	➢ M.tech/ B.Tech / B.E/ MCA (Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢ Minimum 7 years of relevant experience in Incident responder, Security investigator, Advanced security analyst, Security engineer/ architect. ➢ Should have knowledge on networking and security	At least one industry leading SIEM product and preferably other leading certifications in security, such as CISA/CISM /CRISC
18	VAPT Expert*	Yes	Onsite	4*	100%	➢ M.tech /B.Tech/ B.E./ MCA (Note: M.Tech/ B.Tech/ BE should be from either of the below streams:	➢ Minimum 7 years of relevant experience	Certification in at least one industry leading SIEM product and preferably CEH

Technical Manpower: During Operation and Maintenance phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)		
19	IT Security & asset Manager*	Yes	Onsite	8*	100%	➢ M.tech /B.Tech/ B.E./ MCA (Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢ Minimum 8 years of relevant experience in managing large scale projects involving Information Security/ Cyber Security ➢ Should have experience in design and implementation of Information Security policy for complex and large scale IT application deployments ➢ Should have done assignments involving assessment of information security policies and	➢ Desirable to have Industry standard security certifications on the proposed solution

Technical Manpower: During Operation and Maintenance phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
							should be able to identify areas of improvements in the information security architecture ➢ Should have designed information security architectures for large internet-based applications for safeguarding against security threats, vulnerabilities, cyber and phishing attacks ➢ Should have specialization on a range of solutions, including, but not limited to, making appropriate use of PKI, intrusion detection or prevention, VPN, single sign-on, firewalls, and all elements of network-level security.	
20	IT Helpdesk Staff (2999)*	No	Onsite	12*	100%	➢ B.Tech/ B.E. / BCA	➢ Minimum 3 years' experience in IT Support	

Technical Manpower: During Operation and Maintenance phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
21	DC support Staff*	No	Onsite	4*	100%	➢ B.Tech/ B.E. / BCA/ MCA	➢ Minimum 5 years' experience in IT DC Support	
22	Cloud Architect	No	Onsite	1	100%	➢ B.Tech/ B.E. /BCA/ MCA	➢ Minimum 5 years' experience in cloud support	
23	IT Support staff at Lucknow*	No	Onsite	30*	100%	➢ B.Tech/ B.E. / BCA/B.SC IT	➢ Minimum 5 years' experience in IT Support	
24	IT Support Staff at OMC Ghaziabad*	No	Onsite	6*	100%	➢ B.Tech/ B.E. / BCA/B.SC IT	➢ Minimum 5 years' experience in IT Support	
25	IT Support staff at OMC Prayagraj*	No	Onsite	6*	100%	➢ B.Tech/ B.E. / BCA/B.SC IT	➢ Minimum 5 years' experience in IT Support	
26	Application support staff - Programmer / Designer	Yes	Onsite	2	100%	➢ B.Tech/BE/ MCA/ M.Sc. IT (Note: M.Tech/ B.Tech/ BE should be from either of the below streams: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication	➢ Should have at least 5 years of relevant experience in Designing, development, and support in website management/HRMS management/mobile application management	

Technical Manpower: During Operation and Maintenance phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						➢ Electronics & Tele-communication)		
	Application support staff - Mobile application developer	Yes	Onsite	1	100%	➢ B.Tech/ BE/ MCA/ M.Sc. IT (Note: B.Tech should be from either of the below stream: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)	➢ Should have at least 5 years of relevant experience in Android / iOS development	
	Application support staff - Content writer	Yes	Onsite	1	100%	➢ B.Tech/ BCA/M.Sc.	➢ Minimum 4 years of relevant experience in (Hindi and English content writing)	
27	District technical Support	No	Onsite	78	100%	➢ B.Tech/BE/ BCA/ M.Sc. IT	➢ Minimum 3 years' experience in IT Support Roles	

Technical Manpower: During Operation and Maintenance phase								
#	Role Description	Key Personnel Yes/No	Onsite/ Offsite	Minimum No. of Resources	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
						(Note: B.Tech/BE should be from either of the below stream: ➢ Information Technology ➢ Computer Science and Engineering ➢ Electronics ➢ Electronics & Communication ➢ Electronics & Tele-communication)		
Total				**183**				

*For three shifts in a day.
** The project will require custom reports, customisation, and other updates in the software. This set of resources will do all such changes avoiding requirement of any Change Order for such changes.

4.28.2 Detailed Resources Profile, Roles and Responsibilities

Below mentioned (but not limited to) are the responsibilities of Technical Manpower as per their roles:

Sl.	Role Description	Roles and Responsibilities
1	Project Director/ Manager	➢ Shall be responsible for organizing, planning, directing, and coordinating the project/program effort ➢ Shall be responsible for overall planning and stakeholder management ➢ Shall be responsible for managing the team resources and ensuring their optimum allocation, as desired by UP112

Sl.	Role Description	Roles and Responsibilities
		➢ Shall manage the solution implementation in close coordination with all the solution architects, administrators, experts, support staff, multiple agencies, vendors, project stakeholders etc. ➢ Shall be responsible for organizing, planning, directing, and coordinating with the resources. ➢ Shall have a thorough understanding and knowledge of the principles and methodologies associated with program management, vendor management, quality assurance metrics and techniques, and configuration management tools ➢ Shall be available onsite for full time during project implementation ➢ Shall be the single point of contact for UP112 for all contractual obligations, including those of any subcontractors ➢ Shall not serve in any other capacity.
2	Solution Architect (DC, DR)	➢ To design the Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) that should include but not limited to, data replication strategies between DC and DR, DC-DR connectivity, and failover procedures ➢ To interact with other architects, project management to determine the solution interdependencies and interfacing requirements with DC and DR ➢ To identify improvements areas or upgradation needs in DC-DR services
3	Solution Architect (Applications)	➢ To conceptualize and interpret new architecture designs and requirements into an architecture and design that shall become the blueprint for the solution being created. ➢ For implementing the applications as defined in the application solution being created. ➢ For implementing the applications as defined in the application architecture using appropriate technologies and thereby design secure applications. comprehensive architecture for a software solution and providing strategic direction throughout the development process ➢ To research, analyse and interpret highly complex technical data for comprehension at various organizational levels and provide recommendations ➢ To work with the other consultants in applying solutions to business problems, and place the solutions to the enterprise architecture across all viewpoints
4	Solution Architect (Network)	➢ Responsible for interacting with other project stakeholders, agencies, and solution architects for defining the network requirements for seamless interfacing of all project components

Sl.	Role Description	Roles and Responsibilities
		➢ Responsible for sizing the required Network bandwidth and for Server Load Balancing requirements. ➢ Should have experience in design of network architecture for large scale distributed and heterogeneous environments ➢ Design of network security architecture, including firewall, intrusion detection systems, intrusion prevention systems, encryption, PKI, and key management and would be responsible for defining the integrated security architecture in close coordination with the other system components. ➢ Ownership of installation, configuration and troubleshooting of switches, Routers, Firewalls, and IPS. VLAN configuration etc., Knowledge of Network Protocols
5	Solution Architect (Information Security)	➢ The Information Security Solution Architect shall be responsible for designing information security architectures for the project ➢ Shall serve as a security expert during application development, database design, and network and or platform (operating system) efforts, helping project teams comply with enterprise and IT security policies, industry regulations, and best practices. ➢ Shall contribute to the development and maintenance of the information security strategy
6	Database Architect or Modeler	➢ Shall provide highly specialized technical expertise towards data architecture and data model design, design of data structures, database schemas, including deployment architecture for databases. ➢ Shall own the overall management and administration of database, creation of schemas, table spaces, define number of users in the database, create user profiles, memory utilization, caching etc. ➢ Shall be able to assist in tasks, including, but not limited to, the monitoring and maintenance of databases, installation of database software patches, monitoring of database backups, standardization, and implementation of databases to improve the management of production and test environments, support users by resolving problems with applications' databases ➢ Shall be able to assist in the day-to-day tasks, including, but not limited to, monitoring and allocating volumes, creating, and managing zones, LUN, etc., managing fabric security, analysis of utilization and resources, performance tuning, coordination of system updates or fixes ➢ Shall ensure proper backup and restore, database validity, database consistency and security

Sl.	Role Description	Roles and Responsibilities
		➢ Responsible for successful data migration
7	Database Administrator	➢ To provide highly specialized technical expertise towards administration of Databases ➢ For installation of database, creation of schemas, table spaces, define number of users in the database, create user profiles, memory utilization, caching etc. ➢ To assist in tasks including the monitoring and maintenance of databases, installation of database software patches, monitoring of database backups, standardization, and implementation of databases ➢ To improve the management of production and test environments, support users by resolving problems with applications' databases ➢ To assist in the day-to-day tasks, including, but not limited to, monitoring and allocating volumes, creating, and managing zones, LUN, etc., managing fabric security, analysis of utilization and resources, performance tuning, coordination of system updates or fixes
8	System Administrator	➢ For maintaining the optimum performance of the Emergency Response system ➢ To provide highly specialized technical expertise to handle System Administration challenges for complex and large-scale systems ➢ To assist in the day-to-day tasks, monitoring of system activities, analysis of system utilization and resources, capacity control, performance tuning, coordination of system updates or fixes, adding or deleting users from the system, and generating reports as required. ➢ To ensure the systems security by ensuring usage policies, the systems backup and restore, etc. ➢ To grant access and permission to various users to the system
9	Network Administrator	➢ To provide support for tasks, including, but not limited to installation, setup or configuration, troubleshooting, tuning, diagnostics, and maintenance of networking and related equipment ➢ To coordinate with the other vendors or agencies to resolve all network related issues. (S)He shall have extensive experience in troubleshooting and management of network technologies as described in this tender. ➢ To manage deployment and maintenance of IT Security infrastructure, including, but not limited to, administration of appropriate access protection; system integrity or reliability; audit control; system recovery methods and procedures, prevention of breaches, intrusions, and or system abuses, awareness training, and compliance with IT security policy directives and regulations of GoUP

Sl.	Role Description	Roles and Responsibilities
		➢ (S)He shall have the technical expertise to monitor various devices or tools such as content filtering and blocking, virus protection and vulnerability protection. ➢ To escalate any security breaches and make sure patches are installed in case of threats related to OEM products ➢ (S)He shall maintain an updated knowledge base of all the published security vulnerabilities and virus threats for related software and microcode, including, but not limited to, operating systems, application servers, web servers, databases, security solutions, messaging solutions
10	Business Analyst	➢ Responsible for implementation of Project Governance Systems and Procedures ➢ Planning and Project Management of all transition and scaling activities of requirements. ➢ Responsible for analysis of macro-level inputs from UP112 for scaling ➢ Responsible for managing resources, procurement, forecasting and demand ➢ Management of services in requirements and design and manage cost and process improvement initiatives ➢ Requirement gathering, business analysis and functional testing of proposed Software System ➢ Shall participate in all fortnightly or monthly project meetings and project review meetings
11	CAD Expert (from OEM)	➢ Should be responsible for reviewing and overseeing the implementation of OEM developed CAD system, product design diagrams, documents, test plans and results to ensure the design and delivery of a sound CAD architecture that meets all the Emergency user needs. ➢ Contribution to the efforts of Solution Architects in documenting the CAD product capabilities, participating in formal customer acceptance testing, reviewing potential CAD product enhancements ➢ To work in close conjunction with multiple agencies, project stakeholders, system designers, architects etc. to understand the CAD interfacing requirements and ensure that the CAD system is integrated into the system as a whole ➢ To provide technical assistance and consultant oversight related to the CAD system with overall project implementation including installation, configuration, testing, reporting, migration, and transition etc ➢ To be familiar with the key aspects of emergency call receiving, emergency data message received, processing of information, voice and screen logging and recording, automatic call distribution technologies, network, and call centre operations.

Sl.	Role Description	Roles and Responsibilities
		➢ To provide day-to-day assistance to UP112 in customization and changes as per requirement of UP112 ➢ Organize Train the trainer course (quarterly) ➢ Patching, upgrading and Updation of public facing list of applications on the defined interval
12	GIS Expert (from OEM)	➢ To closely interact with the GoUP, other project stakeholders and the associated agencies to gauge system and interface requirements and accordingly customize and configure the OEM GIS solution followed by assistance in implementation across all the project locations ➢ (S)He would be required to monitor all the OEM GIS databases for accuracy and data integrity. S)He shall possess knowledge about GIS systems specifically deployed for emergency response systems in India ➢ (S)He should be able to develop and implement standards, processes and procedures for data input and maintenance of the respective OEM's GIS system ➢ (S)He shall possess experience of handling complex projects that involved large scale usage of GIS ➢ To have the ability to address the complexities of the project with relation to hardware being deployed at the states to have GIS software ➢ Hands-on training on deployment on similar projects with MDTs ➢ To perform complex spatial data processing including geodatabase management, data collection, detailed editing, reporting etc. ➢ (S)He should provide training and technical assistance to agencies in the use of GIS data and computerized mapping programs
13	Radio over Internet Protocol (ROIP) System Expert (from OEM)	➢ To be responsible for reviewing and overseeing the implementation of OEM developed ROIP system, product design diagrams, documents, test plans and results to ensure the design and delivery of a sound ROIP architecture that meets all the Emergency user needs. ➢ To contribute to the efforts of Solution Architects in documenting the ROIP product capabilities, participating in formal customer acceptance testing, reviewing potential ROIP product enhancements

Sl.	Role Description	Roles and Responsibilities
		➢ To be familiar with the key aspects of radio frequency wireless setup, emergency data message received, processing of information, voice logging and recording, network, and radio wireless operations. ➢ (S)He must possess an in-depth practical working knowledge of public safety call centre operations and technologies. Experience of designing a large scale complex ROIP systems ➢ (S)He would be required to work in close conjunction with multiple agencies, project stakeholders, system designers, architects etc. to understand the ROIP interfacing requirements and ensure that the CAD system is integrated into the system as a whole
14	Telephony & ACD expert (from OEM)	➢ (S)He shall closely work with the solution architects for designing the entire Telephony and ACD system that shall act as the key constituent of the Contact Centre systems ➢ (S)He shall be responsible for configuration, installation and customization of the OEM supplied applications and shall closely work with the administrators and the UP112 for ensuring the acceptance of the same based on the acceptance criteria as defined by UP112 ➢ (S)He should be familiar with the components of a centralized contact centre's infrastructure e.g., Trunk lines, PBX solution etc. and should be able to complement the efforts of Solution Architects and experts from Network and Security Point of View
15	Cloud Architect	➢ (S)He would creates and maintains the cloud computing architecture that all organizations require in order to be flexible as well as adaptable ➢ (S)He ensure cloud security and Conducting migrations of data and applications and other aspects into the cloud, as needed ➢ (S)He should be responsible for Designing the cloud environment from a comprehensive perspective, ensuring that it satisfies all of the department needs. Performing activities such as deployment, maintenance, monitoring, and management inside the cloud framework that has been created.
16	Monitoring centre configuration and customization expert	➢ (S)He should recommend courses of action based on analysis of both existing and emerging internal or external threats to the emergency response applications and deliver reports, briefings, and assessments to the UP112 while facilitating understanding of cyber threat entities and environments. ➢ (S)He should be able to configuration and customization in the deployed components of SOC or NOC

Sl.	Role Description	Roles and Responsibilities
		➢ (S)he should be able to provide technical investigative support to other Law Enforcement Agencies or any other stakeholders as required
17	Senior Application Developers	➢ (S)He shall Work closely with analysts, solution architects, database designers and UP112to customize the ER applications as planned ➢ (S)He shall gather business requirements and develop specifications for the ER applications ➢ (S)He shall produce the detailed specifications and writing the program codes ➢ (S)He shall unit-test the software work-products in controlled, real situations before going live ➢ (S)He shall be responsible for preparation of training manuals for users. (S)He shall assist the System administrators in maintaining the systems once they are up and running
18	Application tester	Application tester shall be responsible: ➢ Developing and executing software test plans ➢ Identify and facilitate issue resolution with functional and technical groups ➢ Work closely with the systems, database administrators and application support staff to efficiently test the incremental changes being made to the applications that are a part of the overall ER solution landscape ➢ To work with the Documentation Specialist for documenting the test results and reporting them to the senior management
19	Master Trainer	➢ (S)He shall coordinate with the Project Manager and GoUP to plan the training calendar for all the project stakeholders ➢ (S)He shall organize the required qualified resources for the identified training courses. ➢ (S)He shall have expertise in the usage and training of all the Emergency Response solution components viz. LBS, CTI, Identity Management, IP PBX, Reporting, Recording, ACD, Case Record Management, Dialler, EMS, AVLS, and GIS etc. ➢ (S) He shall also be responsible for giving “Train the Trainer” training to identified personnel at each state who shall then be responsible for providing the Refresher courses through classroom or e-Learning training modules as shall be prepared by the MSI ➢ (S)He shall be responsible for designing the training materials. (S)He shall ensure proper conduct of training sessions and also ensure continuous training sessions are organized for the officers. ➢ (S)He shall ensure collection and collation of Trainee Feedback for all training sessions

Sl.	Role Description	Roles and Responsibilities
20	Documentation Specialist	➢ (S)He shall assist the Solution Architects, administrators, Developers, QA staff, Trainers etc. in clearly articulating and documenting the artefacts that are created by them during Implementation as well as Post-Implementation phase
21	GIS Data Support Staff	➢ Responsible for collecting the GIS data at filed level and assist the police official to push the data to central server at DC and DRC
22	Geo Fencing Staff	Responsible for doing the geo-fencing on map for each city in the guidance of police officials
23	SOC Expert*	➢ Should be responsible for 24 X 7 monitoring basis with onsite personnel ➢ Should be responsible for reporting of security alerts and incidents ➢ Should be responsible for capturing data from all devices on real time basis The Main Duties and Responsibilities of SOC Experts a) Investigate all suspicious activities b) Maintain secure monitoring tools c) Review and report on all cybersecurity processes d) Keep all security programs and resources up to date. e) For reporting of security alerts and incidents. f) For detecting internal and external attacks on UP112 infrastructure. g) For capturing data from all devices on real time basis. h) For providing security reports to UP112 or any other agency on daily, weekly, monthly, quarterly, and yearly basis (when required) i) Assist in conducting security audits j) Compliance to security policy and any policy defined by cert-in
24	VAPT Expert*	➢ Should have prior experience of working with standards such as ISO 27001, ISO 20000, COBIT framework, ITIL. ➢ Should have understanding of applicable laws, regulatory requirements, and frameworks. Should possess good IT auditing skills coupled with characteristics like reliability, pro-activeness, and attentiveness. ➢ Should have comprehensive knowledge on regular network scanning, firewall logging, penetration testing and related domains.

Sl.	Role Description	Roles and Responsibilities
		➢ Should be capable of analysing network scans and pen test results, firewall logs or vulnerability scan results to find anomalies that suggest a malware attack or other malicious event has taken advantage of security vulnerability or could possibly do so. ➢ Should be capable of performing rigorous analysis to identify and ascertain vulnerabilities, risks, and threats. Should be able to test customized patching solutions. ➢ Manage the compliance efforts of all internal and outsourced functions that have one or more information security-related responsibilities, to ensure that IT security compliance efforts are consistent
25	Data Migration Expert	➢ Create a project plan for the migration process, including mapping risks and potential impacts ➢ Undertake an audit of existing data ➢ Cleanse data as necessary to remove the potential for issues with data migration ➢ Test the system after the migration process ➢ Find and fix any outstanding faults or issues with migrated data ➢ Document the processes undertaken, any issues, and fixes that have been deployed ➢ Develop best practice standards and protocols for data migration.
26	IT Security & asset Manager*	IT Security and Asset Managers shall be responsible ➢ All required audit and detailed reports ➢ Meeting the governance compliance and security principles ➢ To oversee, direct and enhance the operational functions to Security Operations Centre (SOC) to detect, analyse and respond to advanced and emerging cyber threats etc.
27	ERSS Domain Expert	• Short-term and Long-term strategic planning of the organizations, processes, and solutions • Audit of IT, non-IT and fleet Infrastructure –monitoring the deployment of IT, non-IT and fleet infrastructure at various locations including Data centre and Disaster recovery centre as per the BOQ specified. • Develop framework for project Monitoring & Evaluation (M&E). • Should have experience of Security appliances like firewall, HSMS, server security etc. • Prepare and submit quarterly progress reports for project management including identification of bottlenecks, causes of potential bottlenecks in project implementation, and providing specific recommendations.

Sl.	Role Description	Roles and Responsibilities
		• Manage projects and related specific activities within given constraints of time, budget, and quality. • Ensure scope, schedule and costs are reasonable and achievable. • Ensure all project documentation is updated and conveyed to relevant stakeholders on time. • Integrate self into client environment to effectively lead project team building positive professional relationships with clients and associates. • Define objectives, requirements, and assumptions necessary to structure management project. • Plan, schedule, and control activities to full fill identified objectives applying technical, theoretical, and managerial skills to satisfy project requirements. • Ensure alignment on project goals and deliverables. • Ensure risks have appropriate mitigation and contingency plans.
28	IT Helpdesk Staff (2999)*	➢ IT Helpdesk staff shall be the dedicated personnel for UP112 responsible for handling all IT related problems. ➢ Responsible for creating the issues tickets and providing immediate solution physically or remotely (if possible). ➢ Responsible for first level diagnosis and troubleshooting of the problems relating to network, IP phones, applications, OS, Internet Explorer, Open Office, messaging solutions, Anti-virus, etc. ➢ To monitor and respond quickly and effectively to requests received through the IT helpdesk
29	DC support Staff*	➢ DC Support staff shall be deployed at the Data centre to address any exigencies whenever they arise. ➢ Responsible to ensure the reliability and availability of the Data Centre ➢ Responsible to address the challenges with the servers, storage, software, and networking equipment that constitute a data centre ➢ Support staff should be conversant with the key architectural and design parameters of a DC e.g., Rack, Cooling, Power Distribution, Generator, Availability and Reliability, Physical Infrastructure Management, Fire Protection methods, General Design considerations etc. and should be able to come up with solutions or should be aware of complete escalation procedures for resolving the issues that may surface in the Data Centre
30	DR Support Staff* NOTE: The deployment of DR	➢ DR Support staff shall be deployed at the Disaster recovery centre to address any exigencies whenever they arise. ➢ Responsible to ensure the reliability and availability of the Data Centre

Sl.	Role Description	Roles and Responsibilities
	Support Staff will depend on whether MSI propose to cloud/co-located DR site	➢ Responsible to address the challenges with the servers, storage, software, and networking equipment that constitute a data centre ➢ Support staff should be conversant with the key architectural and design parameters of a DRC e.g., Rack, Cooling, Power Distribution, Generator, Availability and Reliability, Physical Infrastructure Management, Fire Protection methods, General Design considerations etc. and should be able to come up with solutions or should be aware of complete escalation procedures for resolving the issues that may surface in the Data Centre
31	IT Support staff at Lucknow*	➢ Responsible for first level diagnosis and troubleshooting the problems related to hardware and software installed at the office locations ➢ Troubleshooting of MDT, Radio devices, Desktop, Network and Telephony and other software deployed etc.
32	IT Support Staff at OMC Ghaziabad*	➢ Responsible for first level diagnosis and troubleshooting the problems related to hardware and software installed at the office locations ➢ Troubleshooting of MDT, Radio devices, Desktop, Network and Telephony and other software deployed etc.
33	IT Support staff at OMC Prayagraj*	➢ Responsible for first level diagnosis and troubleshooting the problems related to hardware and software installed at the office locations ➢ Troubleshooting of MDT, Radio devices, Desktop, Network and Telephony and other software deployed etc.
34	Application support staff - Programmer / Designer	➢ Developing and executing software test plans ➢ Identify and facilitate issue resolution with functional and technical groups ➢ Work closely with the systems, database administrators and application support staff to efficiently test the incremental changes being made to the applications that are a part of the overall ER solution landscape ➢ To work with the Documentation Specialist for documenting the test results and reporting them to the senior management
35	Application support staff -	➢ Support the entire application lifecycle (concept, design, test, release, and support) ➢ Produce fully functional mobile applications writing clean code ➢ Gather specific requirements and suggest solutions

Sl.	Role Description	Roles and Responsibilities
	Mobile application developer	➢ Write unit and UI tests to identify malfunctions ➢ Troubleshoot and debug to optimize performance ➢ Design interfaces to improve user experience ➢ Assist with Product development team to plan new features ➢ Ensure new and legacy applications meet quality standards ➢ Research and suggest new mobile products, applications, and protocols ➢ Stay up to date with new technology trends
36	Application support staff - Content writer	Application support staff shall be responsible: a) For content updating over the UP112 website, portal, e-learning b) Troubleshooting any issues related to the website, HRMS or any other application c) Any customization required in websites, HRMS or others
37	District technical Support	a) Ensure entry of Human resource and assets related information in HRMS/Asset/Inventory management portal. b) District technical support staff shall be designated at each district and Commissionerate to resolve the problems arising at the filed locations relating to Hardware, software, IT equipment, CAD etc. c) Responsible for first level diagnosis and troubleshooting the problems relating to network, IP phones, applications, OS, Internet Explorer, Open Office, messaging solutions, Anti-virus, MDTs, applications etc.

4.28.3 Contact Centre Resources

Contact Centre Operation is most crucial part of UP112. Contact centre manpower plays a vital role in the entire UP112 ERSS set up, as these officers collects the primary information and create the event. UP112 is having a centralized contact centre established at Lucknow. Contact centre at Lucknow being assisted through two Operations Mirroring Centres (OMCs) at Prayagraj and Ghaziabad with 15% capacity each. Prayagraj and Ghaziabad being used as back-up operational mirror centres for Lucknow.

Manpower at Contact centre comprise of:

1. Communication Officer (CO)
2. Communication Officer Monitoring staff

a. Communication Officers (CO)

Entire contact centre shall be managed by professional and trained women staff called as "Communication officers" who would be efficient and trained to handle calls of distressed citizens. CO comprises of outsourced manpower. Trained women Communication Officers (COs) who would be the first level contact for the callers.

- Further Communication officers are divided into following categories:
  a. **Inbound voice CO:** CO who would be attending the calls landing through landline phone or mobile phones on the toll-free emergency number i.e.,112 or any other emergency no. (to be integrated/added in coming future).

  b. **Inbound non-voice CO:** CO who would be managing the non-voice services such as SMS, email, IoT, panic buttons, VoIP, messengers etc. Non-voice CO would create event for the received message with available details.

  c. **Outbound Voice CO for Feedback:** CO who would be responsible to call back the citizens. Call backs to happen in case feedback is to be taken from the caller as per the feedback schedule.

  d. **Enquiry Voice CO:** CO who would be attending and managing the voice calls related to any type of enquiry

  e. **Inbound/Outbound for other services:** CO who would be managing the other services integrated with UP112 Savera, SIS/Link Cell, Calls from other/border States, WPL-1090, Internal contacts (5001 & 2872), WCD-181, Cyber Desk-1930 etc.

1.1. Existing load assessment:

Following are the existing process comprising contact centre human resources:

a. Inbound Voice calls:

These COs attend voice calls landing over 112 through automatic call distributor (ACD).

Based on assessment of call session report (last 6 months) from CMS (communication management system), the shift wise current occupancy of COs is summarized below:

Important factors	Shift 1: 08:00 AM to 04:00 PM	Shift 2: 04:00 PM to 12:00 AM	Shift 3: 12:00 AM to 08:00 AM
Current AHT (Average Handling time)	64 – 67 Sec.	76 – 80 Sec.	59 – 63 Sec.
AHT for actionable calls	170 - 180 Sec.	170 - 180 Sec.	170 - 180 Sec.
AHT for non-actionable calls	22 - 25 Sec.	22 - 25 Sec.	22 - 25 Sec.
Avg. volume of calls	21,000 – 23,000	22,000 – 24,000	7,000 – 8,000
Avg. event count	5,700 - 6,100	7,600 - 8,000	1,800 – 2,000
Avg. engaged Hours	430 - 450	520 - 540	140 -160
Count of COs	137	148	66
Average occupancy	37% - 41%	43% - 47%	25% - 29%

b. Inbound non-voice calls:

All the non-voice communication from the citizen is managed by these desks including social media platform. The following type of desk are in this category:

i. SMS
ii. Citizen Portal
iii. 112 India App
iv. Twitter
v. WhatsApp
vi. Facebook
vii. Instagram
viii. e-Mail

As per assessment of citizen's request raised using above mode, it is observed that only twitter and WhatsApp are popular platforms to connect UP112

UP112	19-Nov-16 to 31-Dec-2021
Twitter	47019
Facebook	389
WhatsApp	45887
SMS	485
E-Mail	219
Citizen Portal	813
112 India App	
Instagram	Nil
Grand Total	**94812**

c. Outbound desks for Feedback

Feedback desks are separately setup to take feedback from citizen. For all non-special dispatch calls, feedback being sought for 50% of these calls randomly. For all special dispatch calls, feedback being sought for 100% of these calls.

The required number of desks for feedback as per the assessment of current workload and estimated workload for next phase is given below:

Factors	Existing	Estimated/ proposed for Next phase
Event Count	15,000 – 16,000	24,000 – 26,000
High Priority Calls *	4,500 – 4,800 (30%)	7,400 – 7,600 (30%)
Normal Priority Calls	10,500 – 11,000 (70%)	17,000 – 18,000 (70%)
Feedback for high priority calls	4,500 – 4,800 (100%)	7,400 – 7,600 (100%)
Feedback for normal priority calls **	6,600 – 6,700 (60%)	17,000 – 18,000 (100%)
Current Contact ability ***	30 %	30%
Total Feedback received	3,200 – 3,500 (30%)	7,400 – 7,600 (30%)
Total non-contactable calls	7,700 – 7,900 (70%)	17,000 – 18,000 (70%)
AHT for feedback calls	140 - 160 Sec.	140 - 160 Sec.
AHT for non-contactable calls	30 Sec.	30 Sec.
Total engaged hours	190 – 220 hours	450 – 470 hours
Occupancy	63%	70%****
Desks	18	36
Seats	18 (1st Shift) 9 (2nd Shift)	36 (1st Shift) 36 (2nd Shift)

Note: **Current ratio of high priority events is expected to be remained same in next phase.*
*** Currently feedback is attempted for 60% of normal priority events.*
**** Current rate of contact means number of calls where citizen receives call and gives feedback.*
***** 70% Occupancy is targeted for next phase to optimise manpower.*

d. Enquiry Desk:

All the enquiry calls are managed by these desks. However, general enquiry is managed by Inbound CO only. For this purpose, access of Sanchar Portal has been provided to each CO desk. In case of further details are requested by the caller, it is transferred to Information Desks. In current phase, only one desk is set up for enquiry. This single desk is insufficient to handle current workload as 700 – 800 enquiry calls are received in UP112 on daily basis. In current setup enquiry desk is used to work as outbound calls desk when idle.

Factors	Current			Proposed/ estimated for next phase		
	Shift - 1	Shift - 2	Shift – 3	Shift - 1	Shift - 2	Shift – 3
Current enquiry calls	700 – 800			1,500-2,000		
Desk/Seats	1	2	1	4	4	2

e. Outbound desks for abandoned calls:

Currently 2 desks are setup to call back for abandoned calls those are dropped after 5 seconds. These calls are significantly low and can be called back by the same Desk through CTI. All disconnected calls shall be called back by outbound desk.

f. Desks for other Services:

UP112 is a unified and fully functional integrated emergency response support system (ERSS) operationalised in Uttar Pradesh. It has been integrated with other helpdesks like SDRF, FIRE, 1090, medical etc., It has been noted that 1090 women power line and cybercrime are the major services which requires a significant desk.

Based on the current assessment of call load it is analysed that future workload is expected to increase, hence a dedicated team shall be continued to respond to the calls from other sources, thus the desks requirement for NexGen UP112 is assessed and shown below:

Factors	Current			Proposed/ estimated for next phase		
	Shift - 1	Shift - 2	Shift – 3	Shift - 1	Shift - 2	Shift – 3
Savera	2	2	2	-	-	-
SIS/Link Project	2	2	2	1	1	1
Calls from other/border States	1	1	1	1	1	1
1090/5001/2872	5	5	5	3	3	2
181 -WCD	6	6	6	4	4	2
Cyber Desk-1930	20	20	10	20	20	20
Total	**36**	**36**	**26**	**29**	**29**	**16**

i. Savera desk is used for senior citizen registration, so that priority can be given if any emergency calls received from these numbers. Only 13 and 51 registrations have been done by these desks in the month of Jan'22 and Feb'22 respectively.
ii. SIS/Link desks are setup to receive emergency calls from Jeweller shop/Banks/financial institutions, etc., These are sensitive calls and needs to be responded on time to prevent a financial damage/physical injury etc. Current call volume is very low i.e., 69 & 68 in the month of Jan'22 & Feb'22.
iii. Desk for attending calls from other States: This desk is for attending calls from other neighbouring states. Current volume of calls is 30 – 40 per day.
iv. Desks for other services (1090/5001/2872): Currently 5 desks are setup to manage calls from other services i.e., 1090, 5001 & 2872. Only 700 – 900 calls (daily) are received by these desks.
v. Desks for attending calls from 181: Currently six number of desks are setup to manage calls from 181. These calls are specifically for women related crime and needs to be continued in separate setup. 1900 – 2000 calls are received with 80 second AHT in single day by these desks.
vi. *Desk for Cybercrime: Cyber Crimes such as (phishing scams, website spoofing, ransomware, malware, IoT Hacking, Child Pornography, Child Sexual Abuse Material, or sexually explicit content on the internet) are increasing with IT adoption. The growth in cybercrime is expected to increase in future hence the current call load is expected to increase in NexGen UP112. In the existing setup twenty desks are allotted with fifty seating capacity to respond to calls related to cybercrime, the activity of CO includes making entry in cybercrime portal on behalf of citizen in case it is required to be registered. This process takes too much time resulting 5 to 6 minutes AHT for these calls.*

1.2. Estimation of workload:

- Impact of changing in call trunking protocols:

  Currently, UP112 is facing network congestion issue which leads to significant call drop at different levels. To address this issue, SIP trunking with increased numbers of channels is proposed. The change in technology may increase call receiving capability of the system and shall allow more citizen to connect with UP112. This will significantly increase current load on CO desk/seats.

- Impact of population growth and public awareness:

The estimated emergency calls are proportional to population. It is anticipated that number of calls will gradually increase in proportion of population growth also it is expected that the by increase in public awareness call would increase significantly. Similarly, event count may also increase in same ratio. The CO desk/seat needs to be provisioned considering growth in call volume as well as event count.

a. Inbound Voice calls:

Based on impact of above factors, the estimation of important factors and the required CO Seat for Inbound Voice calls are given below:

Important factors	Shift 1: 08:00 AM to 04:00 PM	Shift 2: 04:00 PM to 12:00 AM	Shift 3: 12:00 AM to 08:00 AM
Estimated AHT	52 – 56 Sec.	60 – 64 Sec.	50 – 54 Sec.
AHT for actionable calls**	160 - 170 Sec.	160 - 170 Sec.	160 - 170 Sec.
AHT for non-actionable calls ***	22 - 25 Sec.	22 - 25 Sec.	22 - 25 Sec.
Estimated volume of calls ****	53,000 – 54,000	55,000 – 56,000	18,500 – 19,500
Estimated event count *****	10,000 – 10,500	13,000 – 14,000	3,100 – 3,300
Estimated engaged Hours ******	790 - 830	950 - 980	260 - 280
Targeted occupancy *******	70%	70%	70%
Estimated Seats	**162**	**217**	**72**

Note:

** Estimated AHT would drop as increment in non-actionable call volume will be proportionately high than actionable calls.*

*** AHT for actionable call would drop as proposed LBS/ELS would ease address capturing. This may save avg. 10 sec.in probing of event location.*

**** AHT for non-actionable calls may remain same.*

***** 2.5% hike in current call volume is anticipated after SIP trunking.*

***** 60% hike is anticipated in current event count.*

****** 80% hike is anticipated in current engaged hours (Talk time, disposition time, After Call Work - ACW).*

******* CO's occupancy is targeted to 70% in order to optimize manpower resources*

b. Inbound non-voice calls:

Seats estimation as follows:

Medium	Proposed Count*		
	Shift - 1	Shift - 2	Shift – 3
Twitter	1	1	1
Facebook	1	1	1
WhatsApp	1	1	1
SMS	1	1	1
E-Mail	1	1	1
Citizen Portal	1	1	1
Instagram & 112 India app	**0**	**0**	**0**
Total Seat	**6**	**6**	**6**

c. Outbound desks for Feedback:

100% feedback are proposed to be received by feedback desks. The estimated number of desks for feedback as per the assessment of estimated workload for next phase is given below:

Factors	Estimated/ proposed for Next phase
Event Count	24,000 – 26,000
High Priority Calls *	7,400 – 7,600 (30%)
Normal Priority Calls	17,000 – 18,000 (70%)
Feedback for high priority calls	7,400 – 7,600 (100%)
Feedback for normal priority calls **	17,000 – 18,000 (100%)
Current Contact ability ***	30 %
Total Feedback received	7,400 – 7,600 (30%)
Total non-contactable calls	17,000 – 18,000 (70%)
AHT for feedback calls	140 - 160 Sec.
AHT for non-contactable calls	30 Sec.
Total engaged hours	450 – 470 hours
Occupancy	70% ****
Desks	36
Seats	36 (1st Shift) 36 (2nd Shift)

d. Enquiry Desk:

For the next phase, separate outbound desks are proposed only for feedback. Therefore, it is proposed to increase enquiry desk/seats as per below estimation to enable the COs to attend to abandoned calls:

Factors	Proposed / estimated for next phase		
	Shift - 1	Shift - 2	Shift – 3
Estimated enquiry calls	1,500 – 2,000		
Seats	4	4	2

e. Desks for other Services:

Based on the current assessment of call load it is analysed that future workload is expected to increase, hence a dedicated team shall be continued to respond to the calls from other sources, thus the estimated desks requirement for NexGen UP112 is shown below:

Factors	Proposed / estimated for next phase		
	Shift - 1	Shift - 2	Shift – 3
Savera	-	-	-
SIS	1	1	1
Calls from other/border States	1	1	1
1090/5001/2872	3	3	2
181 -WCD	4	4	2
Cyber Desk-1930	20	20	10
Total	**29**	**29**	**16**

f. Total required seats for contact centre:

Based on assessment for the future requirements as mentioned above, the total estimated desk and seat requirements are as follows:

Medium	Proposed Count of Seats			
	Shift - 1	Shift - 2	Shift – 3	Total
Inbound voice calls	162	217	72	**451**
Inbound non-voice calls	6	6	6	**18**
Inbound enquiry calls	4	4	2	**10**
Outbound calls for feedback	36	36	-	**72**
Desks for other services	**29**	**29**	**16**	**74**
Total Seats	**237**	**292**	**96**	**625**

g. Location wise bifurcation of seats for contact centre:

	Lucknow			OMC Ghaziabad			OMC Prayagraj		
Medium	**Count of Seats**			**Count of Seats**			**Count of Seats**		
	Shift - 1	**Shift - 2**	**Shift - 3**	**Shift - 1**	**Shift - 2**	**Shift - 3**	**Shift - 1**	**Shift - 2**	**Shift - 3**
Inbound voice calls	114	151	50	24	33	11	24	33	11
Inbound non-voice calls	4	4	4	1	1	1	1	1	1
Inbound enquiry calls	4	4	2	0	0	0	0	0	0
Outbound calls for feedback	36	36	0	0	0	0	0	0	0
Desks for other services	21	21	12	4	4	2	4	4	2
Total Seats	**179**	**216**	**68**	**29**	**38**	**14**	**29**	**38**	**14**

h. Manpower requirement for contact centre

MSI should make deployment of trained COs in a phased manner as defined under clause 4.28.3.a. The actual deployment may increase or decrease depending upon the number of calls received at UP112. Based on the current state assessment on call load and severity

of events, the future CO manpower requirements has been analysed and indicative resource requirement of Communication Officers at Lucknow, Prayagraj and Varanasi is presented below:

Table: CO Manpower at Call centre

Medium	Proposed Count of CO manpower
Inbound voice calls	**590**
Inbound non-voice calls	**30**
Inbound enquiry calls	**12**
Outbound calls for feedback	**96**
Desks for other services	**97**
Total Communication Officer	**825**

Table: Location wise bifurcation for CO Manpower

	Count of CO Manpower		
Medium	**Lucknow**	**OMC Ghaziabad**	**OMC Prayagraj**
Inbound voice calls	418	86	86
Inbound non-voice calls	20	5	5
Inbound enquiry calls	12		
Outbound calls for feedback	96		
Desks for other services	97		
Total Communication Officer	**643**	**91**	**91**

Note: Buffer of 33% manpower is assumed for continuity in the Contact centre in case of dropouts / attrition, planned/unplanned leaves, training reserve etc.

- The UP112 Contact centres shall be operational for 24X7 in 3 shifts
- MSI shall ensure zero tolerance policy for the attendance during the festive seasons.
- Operation timings for Lucknow, Prayagraj and Ghaziabad Call Centre:
  - Shift 1: 8:00 AM to 4:00 PM
  - Shift 2: 4:00 PM to 12:00 AM
  - Shift 3: 12:00 AM to 8:00 AM

1.3. Minimum qualification criteria

#	Role Description	Minimum Qualification	Minimum required skills	Minimum Experience
1	Communication officer (CO)	Intermediate .	▶ Soft spoken ▶ Active listening and understands the situation of other person ▶ Patient while conversing with person in distress ▶ Excellent oral and written communication skills ▶ Trained on process flows and call centre operations ▶ IT skills (Note: Should know how to operate Desktop, software etc.)	➢ Freshers should be between 18 to 30 years of age till the date of publish of the RFP and should carry below skills prior to joining: • computer literate. • 25 words per minute typing speed.

#	Role Description	Minimum Qualification	Minimum required skills	Minimum Experience
			▶ Proficiency in Hindi. ▶ Understanding of English and regional languages of UP ▶ Proficiency in knowledge of office suits, computer application. ▶ CO at the time of joining UP112 phase 1 age limit was Max. 30yrs, COs of Phase 1 will be provided commensurate age relaxation up to 6 years during NexGen UP112. ▶ 25 words per minutes Typing on the system ▶ Good geographical knowledge of UP	➢ Preference would be given to resources having at least 6 months of prior working experience in any of the ERSS/Govt/ police call centre/BPO operations ➢ 1-2 years as sign language interpreter for handling non-voice calls of people with special needs (only for COs dedicatedly handling people with special needs)

1.4. Detailed Resources Profile, Roles and Responsibilities

Below mentioned (but not limited to) are the responsibilities of Contact Centre Manpower as per their roles:

Sl.	Role Description	Roles and Responsibilities
1.	Communication officer (CO)	▶ Answer all incoming calls/ Signals ▶ Adhere to SLAs ▶ Adhere to defined Key performance indicators ▶ Deliver quality service to callers ▶ Strictly follow SOPs ▶ Collect primary information from the caller with regards to name, address, contact details, type of emergency, and any other information as defined in SOP or as required by department ▶ Interact and understand the message effectively ▶ Enter all information into the computer-aided dispatch system (CAD) ▶ After collecting primary information, create the event ▶ Responsible for taking feedback from callers on a rating scale of 1, 2, 3, 4 and 5 or any the parameter defined by department ▶ Should make outbound calls to citizens in case of call drop, feedback or to seek any information, or as tasks assigned by UP112 etc. (Outbound caller) ▶ Should respond to SMS, email, IoT, panic buttons, VoIP, messengers, and other inputs channel and effectively communicate with people of special needs

Sl.	Role Description	Roles and Responsibilities
		► Should be attending and managing the voice calls related to any type of enquiry ► Should be managing the other services integrated with UP112 Savera, SIS, Calls from other/border States, 1090/5001/2872, 181 -WCD, Cyber Desk-1930 or any other future integrations etc.

b. Communication Officer Monitoring Staff

To monitor and evaluate the performance of the communication officers, following are the requirement of the manpower based over the industry standard provided below the table:

#	Role Description	Minimum no. of Resources	Number of resources at Lucknow HQ	Number of resources at OMC (Prayagraj, Ghaziabad
1	CO Team Leader*	28	20	8
2	CO Team Manager / Associate Manager *	6	4	2
3	CO Manager	2	2	-
4	Project Head	1	1	-
5	CO QA - Quality Auditor*	21	15	6
6	CO TQL / QAM - Quality team Leader / Associate Manager	3	1	2
7	Quality Manager	1	1	-
8	BPM Business Process Manager	1	1	-
9	RTA Real time Analyst*	18	12	6
10	Agent/CO: MIS executive*	6	4	2
11	MIS RTA Assistant Manager	1	1	-
12	Document Specialist	1	1	-
Total		**89**	**63**	**26**

*For three shifts in a day.

Manpower assessment for Communication officer monitoring and supervision has been done based on following assumptions as per call centre industry standards:

► **General assumptions**

i. CO Team Leader over a ratio of 30:1
ii. CO Team Manager / Associate Manager over a ratio of 150:1
iii. CO Manager over a ratio of 400:1
iv. Project Head 1 Overall
v. CO QA - Quality Auditor over a ratio of 40:1
vi. CO TQL / QAM - Quality team Leader / Associate Manager over a ratio of 280:1
vii. CO Quality Manager 1 Overall

viii. CO BPM - Business Process Manager 1 Overall
ix. CO RTA - Rea time Analyst 6 each location
x. CO: MIS executive over a ratio of 150:1
xi. MIS RTA Assistant Manager 1 Overall
xii. Document Specialist 1 Overall

4.28.4 Minimum qualification criteria for contact centre

#	Role Description	Key Personnel	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
1	Project Head- Contact Centre	Yes	100%	Graduation + MBA	➢ Minimum 15 years' experience working in the BPO industry ➢ Experience of leading large teams (more than 150) in BPO/Telesales environment	PMP/ Prince 2
2	CO Team Leader	Yes	100%	Minimum Graduate Proficiency in knowledge of office suits, computer application etc.	➢ Minimum 4 years of experience working in the BPO industry	Certified Call Centre Manager (CCCM)/ ISO 10002 Quality management – Customer satisfaction – Guidelines for complaints handling in organizations
3	CO Team Manager / Associate Manager	Yes	100%	➢ Graduate ➢ Desirable qualification: MBA (Operations/ Leadership)/ MA	➢ Minimum 7 years' experience working in the BPO industry	Certified Call Centre Manager (CCCM)
4	CO Manager	Yes	100%	➢ MBA (Operations/ Leadership)/ Graduate	➢ Minimum 10 years' experience working in the BPO industry ➢ Experience of leading large teams in BPO/Telesales environment	Certified Call Centre Manager (CCCM)/ ISO 182945 Customer Contact Centres
5	CO QA - Quality Auditor	Yes	100%	Graduate	➢ Minimum 10 years' experience working in the BPO industry	ISO9001 Quality Management/ ISO 10001 Quality

#	Role Description	Key Personnel	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
					➢ Experience Quality audits in large scale BPO/Telesales environment	management – Customer satisfaction – Guidelines for codes of conduct for organizations/
6	CO TQL / QAM - Quality team Leader / Associate Manager	Yes	100%	Graduate	➢ Minimum 10 years' experience working in the BPO industry ➢ Experience of working in Quality management in large scale BPO/Telesales environment	ISO 10002 Quality management – Customer satisfaction – Guidelines for complaints handling in organizations/ISO 10003 Quality management – Customer satisfaction – Guidelines for dispute resolution external to organizations/ISO 10004 Quality management – Customer satisfaction – Guidelines for monitoring and measuring
7	BPM Business Process Manager	Yes	100%	Bachelor's degree in business management, project management, or in a related field.	➢ Minimum 3 years of experience in business process management in BPO industry.	Relevant certification will be a plus point
8	RTA Real time Analyst	Yes	100%	Graduate	➢ Minimum 3 years of experience in a contact center environment.	Relevant certification will be a plus point
9	Agent/CO: MIS executive	Yes	100%	Graduate	➢ Minimum 3 years of experience in a contact center environment.	Relevant certification will be a plus point

#	Role Description	Key Personnel	Deployment	Minimum Qualifications	Minimum Experience	Minimum Certification
10	MIS RTA Assistant Manager	Yes	100%	➢ Graduate ➢ Desirable qualification: MBA	➢ Minimum 5 years of experience in a contact center environment.	Relevant certification will be a plus point
11	Document Specialist	Yes	4	100%	Graduate in any discipline	➢ Minimum 4 years of relevant experience ➢ Relevant experience in and administrative documentation in Government sector. Excellent/Good: Reading, Writing, and Speaking skills in Hindi and English ➢ Experience in formatting documents according to SOP regulatory requirements

4.28.5 Detailed Resources Profile, Roles and Responsibilities

Below mentioned (but not limited to) are the responsibilities of Contact centre Manpower as per their roles:

Sl.	Role Description	Roles and Responsibilities
1.	Project Head (Contact centre)	Supervision of the entire contact centre/call centre Ensuring resource availability and effective allocation and delivering of expected responsibilities on time within budget and scope. Assembling project deliverables such as scope, documents, and schedules Establishing and preparing formal reports on project progress and reports on type of complaints, resolution time and shortcomings for stakeholders Supporting the CO Team Leader/ Managers in defining and implementing documents for control and management of contact centre for UP112, located in Lucknow, Prayagraj and Ghaziabad. Proactive, quick problem-solving skills when issues arise Excellent interpersonal and communication skills

Sl.	Role Description	Roles and Responsibilities
		□ Ability to work in a fast-paced environment while maintaining friendly demeanour □ Ability to work independently with minimal supervision
2.	CO Team Leader	□ SPOC for all CO related queries. □ Responsible for overall deployment and work activity of COs □ Answering caller's questions, guiding the CO(s) through difficult calls or issues, sympathising needy callers, or handling issues that cannot be handled by CO(s). □ Ensure performance of COs is up to the mark □ Monitor attendance and behaviour of COs and motivate them □ Internally resolve issues of COs if any and □ Ensure seamless change in shifts of COs □ Assist Shift In charge of contact centre and co-ordinate with other departments if required.
3.	CO Team Manager / Associate Manager	□ Responsible to train, coach, and lead UP112 call centre representatives as they provide support for customers. □ Leading team meetings, asking questions to better understand the calls CO(s) are receiving, educating and coach CO(s) regarding processes and practices, and explain expectations to them.
4.	CO Manager	□ Responsible to hire CO □ Leading team meetings, asking questions to better understand the calls CO(s) are receiving, educating and coach CO(s) regarding processes and practices, and explain expectations to them.
5.	CO QA - Quality Auditor	□ Each QA shall be responsible for auditing minimum 50 actionable calls including social media and others including 30 blank calls on daily basis □ Responsible for understanding UP112 needs and requirements to develop effective quality control processes. □ Will be responsible to audit summarized holistic quality performance, identify solutions, and implement the necessary actions which lead to improved performance and customer experience. □ Will be responsible for auditing and implementing quality & compliance standards.
6.	CO TQL / QAM - Quality team Leader / Associate Manager	□ Responsible for enforcing quality control processes □ Will be responsible to understand the metrics, build reports which summarizes holistic quality performance, identify solutions, and implement the necessary actions which lead to improved performance and customer experience. □ Will be responsible for monitoring and implementing quality & compliance standards, initiatives, and analysis for UP112 service centres and managing the calibration process across all contact centres. □ Monitoring of QA resources □ Ensuring quality audit of all the communication officers excluding COs deployed for other services. QA to be done on random call basis and should be in such a way that at least 3 calls are audited for each communication officer.

Sl.	Role Description	Roles and Responsibilities
7.	BPM Business Process Manager	□ Evaluating existing business processes. □ Determining and outlining business process improvements. □ Coordinating business process improvement strategies with UP112 department. □ Overseeing all aspects related to the implementation stages of business process improvement initiatives. □ Analysing and monitoring implemented changes to business processes and making adjustments as needed. □ Guiding and supervising personnel who were assigned specific tasks. □ Performing ongoing analyses on business processes related to productivity, quality, costs, and time management. □ Presenting progress reports and integrating feedback. □ Revising and updating procedures and policies.
8.	RTA Real time Analyst	□ Daily real-time monitoring of service levels for all queues at all sites. □ Oversee agent performance from all teams at all sites. □ Drive real-time adherence to expected capacity against actual performance to achieve service levels and efficiency metric goals. □ Support changes within routing profiles. □ Update and send reports related to the performance of each site.
9.	Agent/CO: MIS executive	□ Develop and maintain daily, weekly, and monthly operational analysis as it relates to volume, efficiencies, cycle time, quality, and service □ Create and maintain daily operational scorecards to track and report on KPIs; assist in volume forecast and capacity planning as needed □ Develop MIS documentation to allow for smooth operations and easy system maintenance □ Perform data analysis for generating reports on periodic basis □ Develop MIS system for customer management and internal communication □ Generate both periodic and ad hoc reports as needed □ Understand customer problems and provide appropriate technical solutions □ Analyse business information to identify process improvements for increasing business efficiency and effectiveness. □ Participate in cross-functional meetings to resolve recurring issues. □ Analyse current business processes and make recommendations for improvements
10.	MIS RTA Assistant Manager	□ Report on operational metrics, conduct data and business analysis, and present summary of findings to UP112 department in a clear, concise, convincing, and actionable format □ Provide support and maintenance to existing management information systems (MIS). □ Generate and distribute management reports in accurate and timely manner □ Provide recommendations to update current MIS to improve reporting efficiency and consistency Provide strong reporting and analytical information support to UP112 department

Sl.	Role Description	Roles and Responsibilities
		□ Establish a strong relationship with Team Managers and management through a demonstration of industry knowledge and of the business issues at hand □ Maintain a status on all ongoing activities and proactively communicate with UP112 department
11.	Document Specialist	➢ (S)He shall assist the command centre staff, Trainers etc. in clearly articulating and documenting the artefacts that are created by them

4.28.6 Rewards and recognition

MSI shall design a mechanism and a policy to reward and recognize the top performing resources among the deployed resources on the basis of Key performance indicators. The focus shall be on quality as well as quantity metrics.

Table: Rewards and recognitions for Outsourced staff

Rewards and Recognition Program	Definition	Frequency
Staff of the Week (CO)	Certificate/wall of fame over website/social media - Appreciation of the week	Week
Staff of the Month	Certificate/wall of fame over website/social media - appreciation of the month	Monthly
Best Performer	The top performers name and photo shall be put up on the wall of fame of UP112. Shall be facilitated with complimentary gift if required.	Monthly
Earned day offs	Staff may earn additional day offs with full pay	Biannual
Contests	UP112 may organise games/contests/festival celebration for staff of emergency response centre.	Round the year
Attendance	100% attendance in office as per as per the documented policies and guidelines of UP112.	Biannual
Values Award	Shall be presented to the staff member who has demonstrated: a) Moral behaviour b) Ethics c) Punctuality d) Dress code adherence e) Attended all trainings	Annual
UP112 Personnel of the Year Award	Shall be awarded to person for exemplary performance and exceptional caller service.	Annual

In addition to the above, regular feedback of staff shall be facilitated from SP (operations) level biannually.

4.28.7 MSI Obligations in terms of Human Resource

2.1.1 MSI shall provide trained women Communication Officers (COs), CO monitoring staff, Technical resources as mentioned below in this section of RFP.

2.1.2 MSI should make deployment of trained COs in a phased manner as defined under clause 4.28.3.

2.1.3 MSI must provision adequate count of COs for languages like (Hindi, English) regional dialects (such as, Bhojpuri, Awadhi, Kannauji, Bundelkhandi, Kumauni/Gadhwali, Brajbhasa, Khadi boli), and major foreign language used by Foreign tourist visiting Uttar Pradesh. Also, those understanding the sign language used by differently abled (deaf and dumb) persons.

2.1.4 MSI should be in compliance to the minimum qualification, experience, certifications, and desired skills criteria while proposing names of outsource staff for technical manpower and Contact centre. The minimum qualification criteria, desired skills, certifications, experience and roles and responsibilities are mentioned below in this section of RFP document.

2.1.5 MSI shall be responsible to provide pool of human resources to operationalize UP112 at different locations such as UP112 HQRS Lucknow, OMCs Prayagraj & Ghaziabad and at districts. It is MSI's responsibility to provide adequately trained manpower as per the clause 4.28.

2.1.6 It is MSI's responsibility to provide uniform, shoes and regular trainings to the deployed manpower (communication officers).

2.1.7 MSI shall also be responsible to provide to and fro transportation facilities Cos as required. MSI shall ensure timely availability of COs in office locations as per the shift timings mentioned in Clause 4.28.3. The agency should ensure optimum availability of fleet for this purpose.

2.1.8 MSI shall provide minimum 2 pairs of uniforms and minimum 1 pair of shoes to all COs deployed at UP112 HQRS and OMC centres. The uniforms should also comprise of winter clothes. MSI should also ensure re-allocation of uniforms including winter clothes and shoes after every two year till the end of contract or on need basis.

2.1.9 MSI shall ensure that each deployed CO should comply with the codal formalities of ITECCS like timely availability in office, in uniform with shoes, moral behaviour, way of talking with the callers and internal ITECCS staff, maintaining decorum of ITECCS and adherence to policy and guidelines.

2.1.10 In case of any replacement of resource or resource leaving UP112, it should be the responsibility of MSI to collect all such belongings of UP112 such as IT asset, ID card, any UP112 project document etc. to be handed over to department.

2.1.11 MSI shall be responsible to ensure compliance to all statutory obligations in respect of the human resource engaged or deployed by them under the contract (including payment of minimum wages, ESIC Contribution, PF etc.). MSI shall manage, in case of any upward/downward changes in the minimum wages and its cascading impact on other statutory compliances like PF, ESI, etc. during the contract period. This should comply to all statutory obligations.

2.1.12 MSI shall comply with all applicable State Law, Statutory Rules, Regulations etc. such as Payment of Wages Act, Minimum Wages Act, and Workmen Compensation Act, Employer's Liability Act, Industrial Dispute Act, Employers Provident Act, Employees State Insurance Scheme, Contract Labour (Regulation and Abolition) Act 1970, Payment of Bonus & Gratuity Act and other Acts, Rules and Regulations for labour as may be enacted by the Government during the tenure of the Contract and having force or jurisdiction at Site. MSI shall also give to the local Governing Body, Police, and other relevant Authorities all such notices as may be required by the Law. MSI to adhere State wages as per payment of bonus act 1965.

2.1.13 UP112 reserves the right to change the human resource which shall be communicated to the MSI. MSI with the prior approval of UP112 may make additions to the project team. MSI shall provide UP112 with the CV/resumes along with educational and other certificates of Technical manpower and provide such other information as may reasonably be required.

2.1.14 UP112 reserves the right to interview the proposed Human resources, who shall be deployed as part of the project team including contact centre manpower. If found unsuitable, UP112 may reject the deployment of the personnel. But ultimate responsibility of the project implementation shall lie with the MSI.

2.1.15 MSI should submit profiles of only those resources who will be deployed on the project. Any change of resource should be approved by UP112 and compensated with equivalent or better resource. UP112 may interview the resources suggested by the MSI before their deployment on board. It does not apply in case of change requested by UP112.

2.1.16 MSI shall ensure that none of the Key Personnel (refer clause 4.28.1) proposed manpower, exit from the project during first 5 months.

2.1.17 MSI shall also maintain adequate contracted strength 'on panel' to enable meeting the replacement or substitution and additional resource requirements (if any) within the time period specified in SLAs for such replacements or substitution at all locations.

2.1.18 In case of change/replacement of human resource (post implementation phase), MSI shall ensure a reasonable amount of time to overlap in activities to ensure proper knowledge transfer and handover or takeover of documents and other relevant materials between the outgoing and the new resource. In case of change/replacement of any key personnel Knowledge Transfer Time would not be less than 15 days (All time and cost effect in this respect shall be borne, by MSI within the contract value).

a. MSI shall ensure that the deployed team is competent, professional and possesses the requisite qualifications and experience appropriate to the task they are required to perform under this RFP. MSI shall ensure that the services are performed through the efforts of the deployed team, in accordance with the terms hereof and to the satisfaction of the UP112. Nothing in this Contract relieves the MSI/MSI from its liabilities or obligations under this Contract to provide the Services in accordance with the Purchaser directions and requirements and as stated in this Contract and the Bid to the extent accepted by UP112 and MSI shall be liable for any non-performance, non-compliance, breach or other loss and damage resulting either directly or indirectly by or on account of its Team.

2.1.19 MSI must ensure prior approval of UP112 in case of any replacement or new deployment of key resource or else the candidature of the resource shall not be valid till the time the same is approved by UP112.

2.1.20 UP112 shall always be the Principal Employer for Human resource / outsourced manpower.

2.1.21 In case during execution of works, the progress falls behind schedule or does not meet the Tender requirements/scope of work, MSI shall deploy extra manpower or resources to make up the progress or to meet the RFP requirements. Plan for deployment of extra manpower or resources will be submitted to UP112 for its review and approval. All time and cost effect in this respect shall be borne, by MSI within the contract value.

2.1.22 The deployed manpower including technical manpower and Contact centre manpower would also be under the supervision of Police officers.

2.1.23 MSI shall be responsible for Training, upskilling and capacity building, Human Resource management of the manpower employed for UP112 project.

2.1.24 MSI shall provide UP112 identity card to all the manpower engaged for the project.

2.1.25 MSI shall ensure attendance of all the engaged manpower through biometric attendance, or any other method if approved by department/UP112.

2.1.26 MSI shall ensure that the attendance of District technical support staff designated at respective districts is certified by UP112 District nodal officer and presented to UP112

monthly. Monthly certificate of presence shall be considered for the attendance and payment of respective resource.

2.1.27 MSI shall ensure that mobile phone or any such electronic equipment is not permitted to be used / allowed in the work area (communication hall / Dispatch hall). The same can be put in lockers.

2.1.28 Working Days: Working days shall be 6 days a week.

2.1.29 Leave Policy: Maximum 3 days per quarter in a calendar year of paid leave shall be permitted to all the deployed manpower with the prior approval of ITECCS. Although, availability of any key personnel shall be subject to request by ITECCS.

2.1.30 UP112 shall draft detailed guidelines as per the provisions of Government of UP/UP police for the outsourced staff of UP112. The guidelines shall cover aspects like, role of contact centre staff, office timings, admin processes, breaks and dress codes etc.

2.1.31 MSI shall ensure that all the deployed technical resources are trained every half-yearly covering key aspects of the project, changes, updates, emerging technology, SOP etc. or any other topic as mutually agreed between UP112 and MSI.

2.1.32 Trained manpower is defined as a resource which has completed his training schedule as defined in clause 4.28.3 successfully. Each resource to be certified and department may verify the same before deployment. MSI shall ensure no resource is deployed without completion of training and certification.

2.1.33 MSI shall be responsible to carry out the background checks and provide necessary verification certificates before engaging any candidate for UP112.

2.1.34 ADG UP112 may assign any task related to UP Police to manpower deployed in UP112 HQ. The district police head may assign any task related to UP112 operations at district level.

4.28.8 Details of Human Resource

a. Summary of proposed Manpower

Summary of the key personnel / resources will be provided as per clause 4.28.1.

b. Detailed CV of proposed manpower

Detailed CV of proposed manpower under technical and contact centre domain except communication officer.

1	**Name of Resource:**				
1.	**Proposed position or role**	(only one candidate shall be nominated for each position)			
2.	**Background / Brief Profile**				
3.	**Date of Birth**		Nationality		
4.	**Education**	**Qualification**	**Name of School or College or University**	**Degree Obtained**	**Year of Passing**
5.	**Total Years of experience**				
6.	**Relevant years of experience**	(as required for the Profile)			
7.	**Areas of Expertise**				
8.	**Certifications and Trainings attended**				
9.	**Employment Record**	**Employer**	**Position**	**From**	**To**
		[*Starting with present position and last 3 firms (as relevant), list in reverse order, giving for each employment: dates of employment, name of employing organization, positions held.*]			
10.	Relevant Work Undertaken that Best Illustrates the experience as required for the Role)				
Project 1					
Name of Project/ Assignment					

1	**Name of Resource:**
Year	
Location of assignment/project	
Employer	
Client	
Client reference & contact details	
Main project features	
Position held	
Activities performed	(List all tasks performed under this project)
Project 2	
Name of Project/ Assignment	
Year	
Location of assignment/project	
Employer	
Client	
Client reference & contact details	
Main project features	
Position held	
Activities performed	(List all tasks performed under this project)

Resource Contact Information	
E-mail:	
Phone:	

I, the undersigned, certify that to the best of my knowledge and belief that

- This CV correctly describes my qualifications, certifications, and my experience
- I understand that any willful misstatement described herein may lead to my disqualification or dismissal, if engaged

Name of Resource	Signature	Date

Note: All the relevant documents such as certifications and qualifications to be attached with the CV.

4.29 Training and Capacity Building

4.29.1 Training Objectives

NexGen UP112 Emergency Response and Support Services (ERSS) aims to have an efficient, & capable workforce to provide appropriate support in any emergency to the citizens of Uttar Pradesh. Training and Capacity building of UP112 officials will play an essential role to achieve the objective of the Next-Gen UP112 (ERSS). The quality of training to be provided to each trainee from the identified user group will ensure that they are competent and ready for the assigned roles.

- **a.** NexGen UP112 aims at building a dynamic training program for the officials to understand and gain hands-on experience of various modules of the system.
- **b.** Training shall also be required whenever changes are made to the system so that the officials are in sync with the changes made and are able to perform their tasks efficiently.
- **c.** Further, NexGen UP112 aspires to steadily improve the operational efficiency of UP112 by seamlessly planning and preparing the training requirements and to ensure that it is fully equipped and capable to operate and manage its critical functions during the emergency events.
- **d.** The MSI is required to conduct technology enabled and role specific trainings for overall staff as a part of fresher training. The resources who will complete the fresher training will undergo refresher training only after at least one year.
- **e.** This section covers the detailed requirements regarding the training and capacity building to be conducted by the MSI as part of this project.
- **f.** MSI shall impart adequate and specific training to the identified staff on the functional and technical aspects of UP112.
- **g.** MSI shall plan and provide necessary trainings as per the indicative plan mentioned in clause 4.29. Based on this indicative plan, MSI should submit their detailed training plan for approval to the UP112.
- **h.** MSI shall cover the entire spectrum of Training and Capacity Building including:
    - i. Trainer identification
    - ii. Preparing a detailed training plan comprising of the trainings to be conducted, modules covered, targeted audience, location, dates, and duration of the trainings, etc.
    - iii. content creation
    - iv. training dissemination
    - v. assessment and tracking
- **i.** In case the MSI calls for any external experts to impart any training, expenses of travel and lodging should be borne by the MSI. For trainings other than those mentioned in the indicative plan, the cost would be borne by UP112.
- **j.** MSI shall create a detailed and effective training strategy, training material in Hindi language, training plan and guidelines and should bear the cost of preparation of course

curriculum, printing of training material, training material, presentation material and other consumables etc.

k. Training locations (District Training Units – DTU) shall be made available by UP112. Department to refurbish/customize and make all the necessary arrangements at the DTUs/Training location including course material, writing material, stationery, etc. for each trainee as per the requirement.

l. MSI shall prepare module specific training manuals and submit the same for review and approval. Any revision in the training manual/instruction manual should be done post discussion and approval from UP112.

m. MSI shall update and maintain a digital repository of the training manuals, procedures manual, deployment/Installation guides etc. to reflect the latest changes to the solutions implemented.

n. MSI shall appoint trainers, organize training sessions on a timely basis, prepare soft and hard copy of training material, ensure that the attendance and performance evaluations are recorded.

o. MSI is required to provide regular trainings using video modules, e-learning modules, and training material. All the content should be hosted on the learning portal and made available to the users.

p. It shall be the MSI's responsibility to conduct, manage and close the trainings, keeping in mind the learning capabilities of the trainees.

q. The training programs should be conducted at locations identified in the indicative plan in clause 4.29.6.

r. MSI should ensure that the trainers are adequately trained on all the functional and technical aspects and trainers should be courteous, polite, and co-operative with the staff. Trainers' and Trainees' attendance to be captured using biometric attendance.

s. MSI to evaluate the effectiveness of the training programs as mentioned in Training Effectiveness Evaluation clause 4.29.10.

t. Performance of MSI during these trainings shall be assessed based on the trainee feedback collected for each training course. Bidder shall design the trainee feedback template in consultation with the UP112.

u. MSI shall collate the trainee feedback as defined in clause 4.29.11 and submit a report after the training session to UP112. Individual trainee feedback shall also be submitted as part of this report.

v. Continuous reporting (MIS) and assessment should be an integral function of training. MSI would design templates for weekly, fortnightly, or monthly review status reports or as per the requirement of the UP112. Post approval of the templates, MSI shall adhere to the reporting plan approved by the UP112.

w. If the trainer is unable to deliver required performance, UP112 reserves the right to get the trainer replaced. Bidder shall in such circumstance replace the trainer with a qualified trainer within the stipulated time as communicated by the UP112.

x. Training content shall be periodically updated with every major change in the UP112 system and associated policies. Such updates in the training content should be done post approval of UP112.

y. Any change made to the training module (other than UP112 initiated change because of new business / policy requirements) during the project cycle having cost impacts would be

considered a change request (unless agreed specifically by UP112) and the cost would be borne by the MSI.

z. All the content created for any mode of training shall be made available on online platforms for anywhere anytime on-demand access as defined in eLearning clause 4.29.

aa. Trainings shall be provided on need basis depending on the changes in the systems or in the process or in organization. MSI shall provide trainings to all the new employees/stakeholders under fresher training module as and when required.

bb. The MSI shall be responsible for conducting training for any new locations which will be established by UP112 during the project period. Smaller locations can be clubbed with bigger locations as per the requirement. For clarity, if there are only a few trainees at a small office, their training may be clubbed with trainees at a larger location. This shall however not be mandatory and shall depend on discretion of UP112. Further, no relaxation in the frequency of training shall be allowed unless agreed in writing with UP112 with appropriate justifications.

cc. The MSI shall ensure that the documentation and training services associated with the components shall be provided by the OEMs without any additional cost to the UP112.

4.29.2 Types of Trainees

Senior officers	Officers from UP Police like DIG, IG and ADG etc.
Functional users	Field police personnel and the staff of NexGen UP112 Call Centre like COs, Dispatch Unit, PRV Staff etc.
District level trainers	Trainers identified for each District for 'Train the trainer' programs like SI, Inspector, ARO, Dy. SP, ASP and SP

4.29.3 Trainer Qualifications and Roles & responsibilities

Designation	Qualification	Experience	Minimum Number of Resources
Trainer for ToT	M.Tech or B.Tech /B.E., M.Sc./M.Ed, MBA	Minimum 10 years of experience in training	5
Trainers at district location to deliver the scope as mentioned in Section 4.29.4	MCA or B.Tech /B.E., M.Sc./M.Ed, MBA/MSW	Minimum 05 years of training or teaching experience	120

- Trainer for ToT will be based at central location in Lucknow for content creation, educating district level trainers, coordination for training plans, preparing training schedules, training calendars, completing TNA etc.
- Cost for all the trainers would be borne by the MSI and only trained personnel will be on boarded by MSI. They will be working under Master Trainer as mentioned in Manpower Section.
- MSI to ensure that at least one trainer should be stationed at each district to deliver the training program
- MSI has to ensure that all the district level trainers are certified by department before actual placement in the field.

- MSI has to ensure a combination of district level trainers in such a way that they can be rotated for training delivery purpose within different districts in police range. The cost of travel to impart training, expenses of lodging and boarding should be borne by the MSI.
- Bidder has to arrange additional resources as backup in case of non-availability of respective district level trainers.

4.29.4 Types of Trainings

a. General training: This training shall include the general IT skills that are required for operating the IT components involved in the overall Emergency Response solution e.g., Desktop operations, basic troubleshooting etc

b. Functional training: This would focus on the use of NexGen UP112 applications installed at the headquarter and other OMC sites, so that the users are kept abreast with the system and are able to implement the overall process defined by UP112 for an optimum use of the system.

c. Soft skills training: MSI would be required to provide soft skills training to the communication officers, dispatchers, PRV staff and other identified officials, to be able to communicate in a defined manner. Call etiquettes and call scripts should be provided to the trainees.

d. Process and Policy related trainings: Capability to efficiently perform operations by government officers and their staff is governed by their awareness of changes in process and policy ecosystem. Following indicative trainings shall be provided by MSI under this heading:

i. All the relevant SOPs
ii. Policies pertaining to agreed ways of operations
iii. Understanding of revised business processes
iv. Any other policies/functions that underwent a change and has an or may have an impact on the NexGen UP112

e. Senior officials' training: This training would focus on how to use and access the MIS reporting functionality of the system for day-to-day monitoring. The training should also focus on extracting various MIS reports from the system etc.

4.29.5 Modes of Training

The following modes of trainings shall be undertaken by MSI:

a. Classroom Training: The trainings be conducted by trained and qualified Master Trainers in a classroom environment. To maintain consistency across trainings, standard templates shall be used for each component of a module. The classroom courses for all the core trainings will have the following components:

i. Course presentation (PowerPoint or interactive audio-video presentations)
ii. Instructor demonstrations (application training environment)
iii. Hands-on exercises (Application training environment)
iv. Application simulations
v. Course evaluations

b. E-Learning modules: MSI shall be required to develop e-Learning modules for all the key components and workflows of NexGen UP112. These e-Learning modules should be easily accessible in form of videos, audio-visual learnings along with written documents, which shall be available as online training materials to its key system users and all the key stakeholders

as and when needed. All the training contents / manuals created for different modes of trainings shall reside as e-Learning modules to enable anytime anywhere learning.

c. **Webinar Training:** The MSI shall be required to conduct webinars, where the trainers can impart trainings through audio-visual mode and demonstrate the application. The webinars shall act as a powerful medium to provide interactive and high-quality learning experience to the system users when needed.
d. **Hybrid Training for Senior Officers:** The hybrid training shall enable senior officers to attend training from wherever they are located. Can be delivered primarily through a digital platform but can also be used in face-to-face training sessions, scheduled webinars, online lectures etc.
e. **Train the trainer (TTT):** The MSI shall facilitate a Train the Trainer (TTT) program to help assure quality of training being delivered. The trainers are required to be trained to ensure they have the skills needed to present the training materials to effectively deliver trainings to the end user. The MSI shall identify and assess all the trainers before deployment.

   Also, pilot run for all the trainings is mandatory to identify if there are any gaps in the curriculum. If any gaps are found, the MSI shall address the issue before conducting the training to the end user.

4.29.6 NexGen UP112 Stakeholders indicative training plan and approximate number of trainees:

User Type	Indicative Headcount	Fresher Training days		Total Fresher Training days	Total Refresher Training Days
		By Instructor	By Department (UP112)		
Communication Officer	825	15	0	15	7
Event Supervisory Officer at HQ	239	12	0	12	6
ROIP Monitoring Officer (RMO) at districts	654	6	0	6	3
PRV Field Staff	39638	15	3	18	7
PRV Pilot	23569	8	3	11	4
Police Station Staff	6948	3	0	3	1
Senior Officers	400	1	0	1	0
Office Support Staff – HQ	37	3	0	3	2
Office Support Staff - FSO & CFO Fire Services	542	3	0	3	2
Office Support Staff - Firemen at Fire Station	1100	3	0	3	2
Leadership Development	106	10	0	10	0
Total	74058				

The training shall be carried out in batches, each batch with a maximum of 50 trainees.

Fresher Training – MSI shall conduct trainings for all the new joiners of UP112 as per the indicative plan provided in clause 4.29.6. The training must include a basic induction program, imparting knowledge about the scope of services delivered and followed at UP112.

a. Re-Fresher Training – User attending a classroom based planned training session at least after one year from the date of Fresher Training.

Indicative Training Plan for 1st Year										
S. No.	Dial 112 Unit	Fresher Training				Refresher Training				
		Days	Trainees	Batch	Person-days	Days	Trainees	Batch	Person-days	Training Locations
1	Communication Officer (CO)	15	206	4	62	7	619	12	87	UP112 HQRS/OMCs
2	Event Supervisory Officer at HQ	12	179	4	54	6	60	1	9	UP112 HQRS
3	RMO (ROIP Monitoring Officer) at Districts	6	491	12	74	3	164	4	12	Field
4	Police Station	3	5211	130	391	1	1737	43	43	Field
5	PRV Staff - HC_2W	15	1875	47	703	7	5625	141	984	Field
6	PRV Staff - _2W_PILOT	8	1875	47	375	4	5625	141	563	Field
7	PRV Staff - HC_4W	15	4017	100	1506	7	12052	301	2109	Field
8	PRV Staff - C_4W	15	4017	100	1506	7	12052	301	2109	Field
9	PRV Staff - PILOT_4W	8	4017	100	803	4	12052	301	1205	Field
10	Office Support Staff – HQ	3	28	1	2	2	9	1	2	UP112 HQRS/OMCs
11	Office Support Staff - FSO & CFO Fire Services	3	407	10	30	2	136	3	6	Field
12	Office Support Staff - Firemen at Fire Station	3	825	21	62	2	275	7	14	Field
13	Senior Officers	1	400	1	1	0	0	-	-	Hybrid
Total		**107**	**23548**	**579**	**5570**	**52**	**50404**	**-**	**-**	

Indicative Training Plan for 2nd Year										
S. No.	Dial 112 Unit	Fresher Training				Refresher Training				
		Days	Trainees	Batch	Person-days	Days	Trainees	Batch	Person-days	Training Locations
1	Communication Officer (CO)	15	83	2	25	7	743	15	104	UP112 HQRS/OMCs
2	Event Supervisory Officer at HQ	12	48	1	14	6	191	5	29	UP112 HQRS
3	RMO (ROIP Monitoring Officer) at Districts	6	131	3	20	3	523	13	39	Field
4	Police Station	3	1390	35	104	1	5558	139	139	Field
5	PRV Staff - HC_2W	15	750	19	281	7	6750	169	1181	Field
6	PRV Staff - C_2W_PILOT	8	750	19	150	4	6750	169	675	Field
7	PRV Staff - HC_4W	15	1607	40	603	7	14462	362	2531	Field
8	PRV Staff - C_4W	15	1607	40	603	7	14462	362	2531	Field
9	PRV Staff - PILOT_4W	8	1607	40	321	4	14462	362	1446	Field
10	Office Support Staff – HQ	3	7	0	1	2	30	1	1	UP112 HQRS/OMCs
11	Office Support Staff - FSO & CFO Fire Services	3	108	3	8	2	434	11	22	Field
12	Office Support Staff - Firemen at Fire Station	3	220	6	17	2	880	22	44	Field
13	Senior Officers (Hybrid Training)	1	400	1	1	0	0	0	0	Hybrid
	Total	107	8707	208	2147	52	65245	1627	8742	

Indicative Training Plan for 3rd Year										
S. No.	Dial 112 Unit	Fresher Training				Refresher Training				
		Days	Trainees	Batch	Person-days	Days	Trainees	Batch	Person-days	Training Locations
1	Communication Officer (CO)	15	594	12	178	7	231	5	32	UP112 HQRS/OMCs
2	Event Supervisory Officer at HQ	12	201	5	60	6	38	1	6	UP112 HQRS
3	RMO (ROIP Monitoring Officer) at Districts	6	549	14	82	3	105	3	8	Field
4	Police Station	3	5836	146	438	1	1112	28	28	Field
5	PRV Staff - HC_2W	15	5400	135	2025	7	2100	53	368	Field
6	PRV Staff - C_2W_PILOT	8	5400	135	1080	4	2100	53	210	Field
7	PRV Staff - HC_4W	15	11570	289	4339	7	4499	112	787	Field
8	PRV Staff - C_4W	15	11570	289	4339	7	4499	112	787	Field
9	PRV Staff - PILOT_4W	8	11570	289	2314	4	4499	112	450	Field
10	Office Support Staff – HQ	3	31	1	2	2	6	1	2	UP112 HQRS/OMCs
11	Office Support Staff - FSO & CFO Fire Services	3	455	11	34	2	87	2	6	Field
12	Office Support Staff - Firemen at Fire Station	3	924	23	69	2	176	4	9	Field
13	Senior Officers (Hybrid Training)	1	400	1	1	0	0	0	0	Hybrid
	Total	107	54500	1351	14962	54	19452	486	2693	

Indicative Training Plan for 4th Year										
S. No.	Dial 112 Unit	Fresher Training				Refresher Training				
		Days	Trainees	Batch	Person-days	Days	Trainees	Batch	Person-days	Training Locations
1	**Communication Officer (CO)**	15	195	4	58	7	630	13	88	UP112 HQRS/OMCs
2	**Event Supervisory Officer at HQ**	12	46	1	14	6	193	5	29	UP112 HQRS
3	**RMO (ROIP Monitoring Officer) at Districts**	6	126	3	19	3	528	13	40	Field
4	**Police Station**	3	1334	33	100	1	5614	140	140	Field
5	**PRV Staff - HC_2W**	15	1770	44	664	7	5730	143	1003	Field
6	**PRV Staff - _2W_PILOT**	8	1770	44	354	4	5730	143	573	Field
7	**PRV Staff - C_4W**	15	3792	95	1422	7	12277	307	2148	Field
8	**PRV Staff - C_4W**	15	3792	95	1422	7	12277	307	2148	Field
9	**PRV Staff - PILOT_4W**	8	3792	95	758	4	12277	307	1228	Field
10	**Office Support Staff – HQ**	3	7	0	1	2	30	1	2	UP112 HQRS/OMCs
11	**Office Support Staff - FSO & CFO Fire Services**	3	104	3	8	2	438	11	6	Field
13	**Office Support Staff - Firemen at Fire Station**	3	211	5	16	2	889	22	44	Field
14	**Senior Officers (Hybrid Training)**	1	400	1	1	0	0	0	0	Hybrid
	Total	107	17339	424	4837	52	56613	1412	7450	

Indicative Training Plan for 5th Year										
S. No.	Dial 112 Unit	Fresher Training				Refresher Training				
		Days	Trainees	Batch	Person-days	Days	Trainees	Batch	Person-days	Training Locations
1	Communication Officer (CO)	15	160	3	48	7	665	13	93	UP112 HQRS/OMCs
2	Event Supervisory Officer at HQ	12	42	1	13	6	197	5	30	UP112 HQRS
3	RMO (ROIP Monitoring Officer) at Districts	6	116	3	17	3	538	13	40	Field
4	Police Station	3	1228	31	92	1	5720	143	143	Field
5	PRV Staff - HC_2W	15	1458	36	547	7	6042	151	1057	Field
6	PRV Staff - C_2W_PILOT	8	1458	36	292	4	6042	151	604	Field
7	PRV Staff - HC_4W	15	3124	78	1171	7	12945	324	2265	Field
8	PRV Staff - C_4W	15	3124	78	1171	7	12945	324	2265	Field
9	PRV Staff - PILOT_4W	8	3124	78	625	4	12945	324	1295	Field
10	Office Support Staff – HQ	3	7	0	0	2	30	1	2	UP112 HQRS/OMCs
11	Office Support Staff - FSO & CFO Fire Services	3	96	2	7	2	446	11	22	Field
12	Office Support Staff - Firemen at Fire Station	3	194	5	15	2	906	23	45	Field
13	Senior Officers (Hybrid Training)	1	400	1	1	0	0	0	0	Hybrid
	Total	107	14531	353	4000	52	59421	1482	7862	

4.29.7 Training Need Analysis

a. MSI is required to recognize and review the training and development needs as per course corrections requirement to fulfil competency gaps, operational challenges and required to customise training modules as and when required during the contract period.

b. MSI has to assess problems, needs, and allocate the resources available to meet operational needs in the field especially for PRV staff training requirements.

c. Following are indicative requirements to conduct training needs assessment:

- **i.** Identification of specific operational issues/concerns that can emphasize the staff to achieve the vision and objectives of UP112.
- **ii.** Identification of specific operational issues/concerns with respect to acceptability and adaptability towards new learning ways like e-Learning mode.
- **iii.** Identification of most appropriate delivery mechanisms for the learnings that can convert to actions.
- **iv.** Development of strategic framework for the implementation of training.
- **v.** Conduct desk research and analyse all available training resources, training conducted previously and their outcome.
- **vi.** Carry out stakeholder consultation for training requirements and gap analysis. Even this exercise; develop comprehensive training needs assessment framework and questionnaire.
- **vii.** MSI can also conduct training needs assessment, data management and analysis, draw out the inference

4.29.8 Duration of Training

The duration of trainings shall be finalised jointly by the MSI and UP112 while complying with the minimum duration requirements given in the document. However, the period should be sufficiently long for effecting meaningful assimilation of training content by an average user.

a. Indicative Plan for Fresher Training:

i. Communication officer's (COs), 15 Days

S. No.	Module	Indicative Content	Duration in minutes
1.	**Introductory session & Soft skills**	• Introductory Session • Introduction to UP112 (ERSS) • Hierarchy • Languages & Dialects of UP • Names of months in Hindi • Numerals in Hindi • Full forms/ Abbreviations • Name of Districts/Commissionerate (Renamed District Names) • Geographical details of UP • Contact Centre/ OMCs • Soft Skill Session • Communication Officer • Definition of CO • Roles and Responsibilities of CO • Key success factors for CO • Emergencies Calls • Different types of Callers • Expectation of a Caller	780 (13 hrs)

S. No.	Module	Indicative Content	Duration in minutes
		• Sympathy and Empathy • Importance of Listening Skills • Improving our Listening Skills • Quality Parameters • Accuracy of information captured during the • Call • Probing for accurate address capturing • Telephone etiquette and communication • skills • Responsiveness • Voice Modulation Techniques • Do's & Don'ts for CO	
2.	**Process Skills**	• Call handling process • Different types of emergencies • Priority of event • Event type / subtype • Different types of calls • Blank calls • Abounded calls • Nuisance Calls • Outbound calls • Information calls • Follow up calls • Calls related to other integrated services	2340 (39 hrs)

S. No.	Module	Indicative Content	Duration in minutes
		• Other mode of communication – Social Media Platforms (Twitter, Facebook, SMS, WhatsApp), etc • SOS • Other Desk in Contact Centres • Language Volunteers • Feedback calls • SLAs related to call handling • Cyber Crime • SIS • Woman Power Line (WPL)1090 • Calls from bordering states • Senior citizens registration • Complaint registration through Citizen Portal • UPCOP mobile APP • Zones / Ranges of UP • Fairs of UP • Famous Tourist Places / Festivals • Police Hierarchy • Organizational structure of police • Police Commissionerate system/Districts • Indian Penal Code • Code of Criminal Procedure • FIR • Government Railway Police • GIS maps / functionality	

S. No.	Module	Indicative Content	Duration in minutes
		• Communication officer script • Activity (script rehearsal)	
3.	**Technical Skills – Basic IT Skills/UI/ other applications**	• Software I-Net Intro • How to login / logout I-Net • How to change password • CO (Communications Officer) Software Application Layout • How to register CTI Extension • Use of Search option • Event Monitor intro • MAP Monitor Intro • How to create Event • Interface & its Workflow • How to check Caller History • Actionable Call Workflow • Event Information Page overview • POI/Free Text/XY search method • LBS Call Workflow • D-Group Details • Merge Option feature & its usage • Other Desk • CO Module Login • Analog & Its Features • Hands on practice • Mock call practice • Visit of various functions	2730 (45 hrs and 30 min)

S. No.	Module	Indicative Content	Duration in minutes
		• Quality HRMS sheet Session • Mock session by Quality / Operations • Operations expectation setting Session by Operation AMs • Assessment • Post-training Final test Examination Q & A, Certification.	
Total			**5850 (97.5 hrs)**

Note: The MSI shall provide training to the number of COs as defined in the Manpower clause 4.29.6 of section 4 *of the RFP. The number of COs trained in any calendar year would be the maximum as defined in the section Indicative Training Plan.*

Over and above the defined number of COs to be trained by the MSI at no additional cost to the department.

ii. Event Supervisory Officers, 12 days

S. No.	Module	Indicative Content	Duration in minutes

1.	**Workflow & Introduction of 112**	• Introduction of 112
		• Integration of 112 with other agencies & Objectives
		• Integrated Technologies. (Integration, Process, and workflow)
		  o UPSRTC app
		  o SOS 112 India app
		  o 112 Citizen app
		  o 108 Integration
		  o Any other integrated services
		• Technical Workflow of 112
		• Event supervision pertaining to district
			195 (3 hrs and 15min)

S. No.	Module	Indicative Content	Duration in minutes
		• Hands on Training under the supervision of Trainer	
2.	**Soft Skills: Communication Skills**	• Introduction • Importance & Objectives • Types of Communication: Verbal & Non-Verbal • Dealing with Victim with hospitality • Types of Communication: Formal & Informal Communication of event supervisor's with PRV, Caller and concerned person	390 (6 hrs and 30min)
3.	**SOP**	• Adding new SOP and Updating existing SOPs (as and when required) including new types and Sub types	195 (3 hrs and 15min)
4.	**Domestic violence victim registration**	• Women's registration in 112	195 (3 hrs and 15min)
5.	**Escort for Safety**	• Objective, Process, Role & Advantages	195 (3 hrs and 15min)
6.	**Female PRV** **Supervisor PRV.**	• Objective, Process, Role & Advantages • Objective, Process, Role & Advantages	585 (9 hrs and 45 min)
7.	**112 Supervisor Application.**	• Installation, Objective, Process, Advantages	195 (3 hrs and 15min)
8.	**Custom POI. Display**	• Objective, Process, Advantages	195 (3 hrs and 15min)
9.	**Enhance Response Tagging**	• Objective, Process, Advantages	195 (3 hrs and 15min)
10.	**ATR. Codes.**	• Different disposition codes for submitting ATR in events in different agencies	585 (9 hrs and 45 min)
11.	**Threat to VVIP.**	• SOPs, (Objective, Process, Advantages.)	585 (9 hrs and 45 min)
12.	**Language Volunteers**	• Objective, Process, Advantages	195 (3 hrs and 15min)

S. No.	Module	Indicative Content	Duration in minutes
13.	**#tags in Event remarks and its requirements**	• Objective, Process, Advantages	195 (3 hrs and 15min)
14.	**Event Supervisor's (ES) Portal.**	• Objective, Process, Advantages • Event Supervisor's portal o How to open ES page o Login logout o How to configure CTI extension o Verify login on CMS o Map o Event Dispatch o Merge events o Pre-empt o Forward to Media Cell o Star marked events o Event Updating • INETCALLTAKER o Login logout o Event Creation o Finding caller location on Map o Transfer to DO • Contact Centre IP. Phone o Detailed information of hard phone and softphone o Login through hard phone, logout. • Sanchar Portal o Introduction of Sanchar portal o How to effectively use the portal • E-Learning o Login logout o How to Read content o How to attempt assessment	195 (3 hrs and 15min)

S. No.	Module	Indicative Content	Duration in minutes

		• Map
		  o Introduction of map
		  o How to read/navigate maps (like - village, police station, district etc.
		  o Locate distance between PRV and Event location
		• Introduction to MDT
		  o Responder Login & Overview of Responder App
		  o Responder Workflow
		  o Navigation and its Usage
		  o ATR & Disposition Code
		• Type and Subtype updating
		  o How to update event type and sub type in MDT
		• Field Event
		  o How to create field event in MDT
		• MDT Troubleshooting
		• Integration of Various Technologies
		• SOS
		  o Process of SOS creation to dispatch
		• Social Media Platforms
		  o Citizen portal
		  o Twitter
		  o Facebook
		  o WhatsApp
		  o E-mail
		• HRMS
		  o Admin portal
		  o Employee portal
		  o Leave request
		  o Duty Roaster
		  o Transfer etc.	

S. No.	Module	Indicative Content	Duration in minutes

		• ROIP
		  o Details of application and device
		• NexGen UP112 BI reports
		  o How to fetch DO login hours
		  o Performance report
		  o Other tools of BI etc.
		• Location-LBS & ELS Service.
		  o Location based Service: Objective, Process, Benefits.
		  o Emergency location Service: Objective, Process, Benefits.
		• VTS (Vehicle Tracking System)
		  o Live tracking of PRV
		  o PRV History tracking
		  o Dashboard
		  o Patrol order sheet
		• Citizen portal
		  o About 112
		  o Track my call
		• 112 UP Citizen application
		  o Application Installation
		  o ID Creation
		  o Features & Functions of Application
		• Event closure System (Thana Module)
		  o Event Closure URL
		  o Event Closure Process
		  o Fetching Pending Events
		  o Fetching Closed Events
		  o Event Analysis Thana Wise
		  o Event Analysis PRV Wise
		• Hands on Training under the supervision of Trainer	

S. No.	Module	Indicative Content	Duration in minutes
15.	**Special Task to Event Supervisor**	• Wrong arrival • PMS • Feedback analysis • Circle Supervisory PRV • Hands on Training under the supervision of Trainer • Troubleshoot basic system issues • Agra Expressway, Purvanchal Expressway • Fire/GRP • Event Transfer Desk	390 (6 hrs and 30min)
	Assessment	• Examination Q & A, Certification	195 (3 hrs and 15min)
Total			**4680 (78 hrs)**

iii. ROIP Monitoring staff, 6 days

S. No.	Module	Indicative Content	Duration in minutes
1.	**Technical Training**	• Basic Computer Knowledge & First level of Troubleshooting • Knowledge of Basic computer components • Basic Microsoft Word, Excel, and PowerPoint • Knowledge about URL • System Keys Knowledge • Networking connectivity • Introduction to CAD System	1560 (26 hrs)

S. No.	Module	Indicative Content	Duration in minutes
		• Overview & Functions • RoIP Supervisory module • Correctness of ATR report, event creation, field events, approval process. • How to chase events. • District PRV monitoring • Hands on Training under the supervision of Trainer	
2.	**PMS**	• Introduction of PMS & User Creation • PRV Patrolling Route Creation • Updating & Reassigning the Route • Patrol Order Sheet Acknowledge on PRV Deviance) • Hands on Training under the supervision of Trainer	360 (6 hrs)
3.	**HRMS and BI Reports**	• Introduction of HRMS • Employee Registration on HRMS • Employee Records & Filtration • Leave Management • On Boarding: Date of Joining of Employee in 112 U.P. • Transfer Processing (Assigning Employee to another District) • Response Time (PRV/ES) • Police station/ district-wise event details • Hot Spot Analysis • GPS monitoring • Vehicle Tracking System (VTS) • MS Excel • Report generation	330 (5 hrs and 30min)

S. No.	Module	Indicative Content	Duration in minutes
		• Hands on Training under the supervision of Trainer	
	Assessment	Examination Q & A, Certification	90 (1hr and 30min)
Total			**2340 (39 hrs)**

iv. PRV Field Staff, 15 Days

S. No.	Module	Indicative Content	Duration in minutes
1.	**MDT & Technical Aspects**	• Introduction to 112 and technologies • SOP (Role of PRV in different events) • Introduction to MDT • Responder Login & Overview of Responder App • Responder Workflow • Navigation and its Usage • ATR & Disposition Code • Field Event • MDT Troubleshooting • Integration of Various Technologies • SOS • Hands on Training under the supervision of Trainer • Basic maintenance (MDT equipment etc.)	1950 (32 hrs and 30min)
2.	**Soft Skills:** **Human Values**	• Introduction • Importance & Objective	390 (6 hrs and 30 min)

S. No.	Module	Indicative Content	Duration in minutes
		• Basic Elements of Human Values • Role, duties & Responsibilities of a PRV	
3.	**Communication skills**	• Introduction • Importance & Objectives • Types of Communication: Verbal & Non-Verbal • Types of Communication: Formal & Informal • Dealing with Victim • Negotiation Skills & its use in Managing the Situation	390 (6 hrs and 30 min)
4.	**Dispute Resolution Skills**	• Introduction & Meaning • Importance • Event Types & Sub-Types • Elements of Dispute • Taking Control of the situation • Amicable Resolution of Dispute • Dispute Resolution Techniques • Alternate Dispute Resolution • Escalations to Senior Officers	195 (3hrs and 15 min)
5.	**First Aid**	• Introduction, Objective & Importance • Specialized training by Govt Doctor • How to handle a burns victim? • How to provide First aid during emergency? • Conditions requiring first aid • Initial Check-up • First Aid for different injuries and illness • Types of Bandages and their respective use	195 (3hrs and 15 min)

S. No.	Module	Indicative Content	Duration in minutes
		• Temporary Stretcher • CPR/ Basic Lifesaving skills • Pandemic/Covid 19 and Protocol • Role of PRV & Problems faced by PRV	
6.	**Adult Psychology**	• Introduction, Objective, Importance & meaning • Specialized training in human psychology • Transactional Analysis • Ego Stages & Respective Approach • Methods to Understand Person's Behaviour • Stages of Life • Stroke	195 (3hrs and 15 min)
7.	**Stress Management & Motivation**	• Pranayama/Simple breathing • Yoga & Meditation, Positive thinking • Stress release tools • Self-motivation	195 (3hrs and 15 min)
8.	**Crime Scene Management**	• Introduction & Importance • Familiarization with Crime Scene Protection Kit • Usage of Crime Scene Protection Kit Contents • Securing a Crime Spot	195 (3hrs and 15 min)
9.	**Disaster Management**	• Introduction and Objective • Types of Disaster • Important Terminology • Assessment of Risk • Disaster Management & Disaster Management Cycle • Important Points to spread awareness	195 (3hrs and 15 min)

S. No.	Module	Indicative Content	Duration in minutes
		• Important Points from Disaster Management Act – 2005 • Role of PRV & Problems faced by PRV	
10.	**Fire & Safety**	• Introduction, Objective & Importance • Event Types & Sub-Types, trends from recent data • Elements of Fire • Coordination with Fire department • Classification of Fire • Principles of Fire Extinguishing • Fire Fighting Equipment Emergency Response in case of Fire Accident Role of PRV & Problems faced by PRV	195 (3hrs and 15 min)
11.	**Issues Related to Women**	• Introduction, Meaning & Gender Sensitization • How to handle a female victim (Aggressive, agitated, and abusive victims)? • Importance • Event Types & Sub-Types, trends from recent data • The Protection of Women from Domestic Violence Act, 2005 • The Immoral Traffic (Prevention) Act, 1956. • Issues persistent to women and reasons for crime against them • Important Legal Provisions Role of PRV & Problems faced by PRV, seeking guidance from NGO, Women Power Line (1090) etc.	195 (3hrs and 15 min)
12.	**Child Related Issues**	• Introduction & Meaning and Sensitization about Child related issues • Importance • Event Types & Sub-Types, trends from recent data	195 (3hrs and 15 min)

S. No.	Module	Indicative Content	Duration in minutes
		• The Bonded Labour System (Abolition) ACT, 1976 • The Immoral Traffic (Prevention) Act, 1956. • The Juvenile Justice (Care and Protection of Children) Act, 2015. • POCSO Act, IT Act & digital/internet vulnerabilities • Types of Violence Issues persistent to child and reasons for crime against them Important Legal Provisions • Role of PRV & Problems faced by PRV • Seeking guidance from NGOs such as Mother and Childcare centre, Childcare education, and welfare society, etc.	
13.	**Issues Related to Elderly People**	• Introduction & Meaning and sensitization about elderly people • Importance • Maintenance and Welfare of Parents and Senior Citizens Act, 2007 • Event Types & Sub-Types, trends from recent data • Issues persistent to elderly people and reasons for crime against them • 'SAVERA APP' • Important Legal Provisions Role of PRV & Problems faced by PRV, seeking guidance from NGOs for Sr. Citizen	195 (3hrs and 15 min)
14.	**Issues Related to differently abled people**	• Introduction & Meaning and sensitization about differently abled people • Importance Event types & Sub-types, trends from recent data types • Symptoms of Intellectually challenged Issues persistent to Mentally Challenged Important Legal Provisions Role of PRV & Problems faced by PRV	195 (3hrs and 15 min)

S. No.	Module	Indicative Content	Duration in minutes
		• Seeking help from NGO and associated agencies	
15.	**Traffic Management**	• Role of PRV • Introduction, Objective & Importance • Event Types & Sub-Types, trends from recent data. • Important Facts & Figures • Reasons for Road Accidents • Role & Responsibilities of Driver • Traffic Signals & Markings and rules • Important Points	195 (3hrs and 15 min)
16.	**Tourism Related Issues**	• Introduction, Objective & Importance • Types of Tourism • Modes of Travel • Issues Persistent to Tourism • Communication skills and hospitality towards foreign travellers • Important Points from Relevant Indian Laws related to Tourists and Tourism • Steps Taken by Ministry of Tourism for Safety and Convenience of Tourists • Role of PRV & Problems faced by PRV	195 (3hrs and 15 min)
17.	**Training of In-fleet components**	• Protocol for sound & LED light bar • How to use and maintain in-fleet components • Use of Wireless set • Service Ticket registration for faulty/damaged equipment	195 (3hrs and 15 min)
18.	**Miscellaneous**	• Rescuing Animal (injured in road accidents) • Supporting transgender during emergency	195 (3hrs and 15 min)

S. No.	Module	Indicative Content	Duration in minutes
		• SC/ST act important provision • Daily revision session • New Acts, Amendments to existing Acts discussed in above topics. • Feedback • Valedictory session	
	Assessment	• Post-training test Examination Q & A, Certification	195 (3hrs and 15 min)
Total			5850 (97 hrs and 30 min)

v. PRV Pilot, 8 Days

S. No.	Module	Indicative Content	Duration in minutes
1.	**MDT & Technical Aspects**	• Introduction to 112 and technologies • SOP (Role of PRV in different events) • Introduction to MDT • Responder Login & Overview of Responder App • Responder Workflow • Navigation and its Usage • ATR & Disposition Code • Field Event • MDT Troubleshooting • Integration of Various Technologies	1170 (19 hrs and 30 min)

S. No.	Module	Indicative Content	Duration in minutes
		• SOS • Hands on Training under the supervision of Trainer	
2.	**In fleet equipment & their uses**	• Use of Wireless set • Using light and sound console • Use of Emergency Warning system • Use of body armour • Hands on Training under the supervision of Trainer • How to use and maintain in-fleet components • Service Ticket registration for faulty/damaged equipment	390 (6 hrs and 30min)
3.	**Important practical topics for PRV staff**	• Human Values • Communication skills • Adult Psychology • Dispute Resolution • Issues related to • Women • Children • Elderly • Differently abled • Fire safety • Disaster Management • Tourism • Traffic Management • Stress management and personal health • HRMS and Biometric attendance • Hands on Training under the supervision of Trainer	600 (10 hrs)

S. No.	Module	Indicative Content	Duration in minutes
4.	**First Aid**	• Need and conditions for First Aid • CPR/ Basic Lifesaving skills • Trauma Management • Applying ABC and CAD • Control severe bleeding • Using splint, • Stabilising head and cervical	780 (13 hrs)
	Assessment	• Miscellaneous • Examination Q & A, Certification	180 (3 hrs)
Total			3120 (52 hrs)

vi. Police Station staff, 3 days

S. No.	Module	Indicative Content	Duration in minutes
1.	**Technical Training**	• Introduction to NexGen UP112, duty, roles, and responsibilities of Police Station staff • CAD Application: • Event Creation • Event Dispatch • MDT operations • Event Closure System • Integrations in CAD	360 (6 hrs)

S. No.	Module	Indicative Content	Duration in minutes
		• Hands on Training under the supervision of Trainer	
2.	**Reporting and Monitoring**	• HRMS • BI Reports • VTS • PMS • Incident Dashboard • Incident Analysis • Hands on Training under the supervision of Trainer	360 (6 hrs)
3.	**Other**	• VVIP threats • Female PRV • Abusive and Nuisance Caller SOP • Savera • Sanchar • Domestic Violence • Hands on Training under the supervision of Trainer	300 (5 hrs)
	Assessment	• Examination Q & A, Certification	150 (2 hrs and 30 min)
		• **Total**	1170 (19hrs and 30min)

vii. Senior Officers, 1 day

S. No.	Indicative Content	Duration in minutes
1.	• Introduction: • Walk through & Functioning of NexGen UP112 • Key stakeholders (internal and external) • Technology Walkthrough • CAD system and its features (PowerPoint presentation) • Performance of field staff, CO, Dos, ROIP, PS • Response time in various district • Citizen feedback • Others • Major Escalations and action taken in resolving issues, discussion on pending issues (if any) • Recommendations from Higher officials • Analytics, MIS Hands on training concerned software & tools (Walkthrough in training to NexGen UP112 Officers) • Supervisory training	240 (4 hrs)

viii. Office Support Staff in HQ, 3 days

S. No.	Module	Indicative Content	Duration in minutes
1.	**Technical Training**	• Introduction to NexGen UP112, duty, roles & responsibilities of Office support staff deployed in respective departments. • Overview of applications used in NexGen UP112 • Introduction to the role specific application • Features and Functionality of role specific applications	360 (6 hrs)

S. No.	Module	Indicative Content	Duration in minutes
		• Asset management application features • Monitoring of Calls and its evaluation • How to access to call logger application • Call logger features and user rights • How to audit the call quality and fact finding • Identifying high areas of concerns from the system • Prioritizing the concern and reporting to higherups • Hands on Training under the supervision of Trainer	
2.	**Reporting and Monitoring**	• Asset management application reports • HRMS • HRMS reports • Leave management • Data analytics and Review of performance • MIS • Data representation • BI Reports • Preparing of reports in specific formats • Review periodic reports and send collated reports to senior management • Dashboard • Analysis of data • Hands on Training under the supervision of Trainer	360 (6 hrs)
3.	**Other**	• Report writing skills • Information related to RTI	300 (5 hrs)
	Assessment	• Examination Q & A, Certification;	150 (2 hrs and 30 min)

S. No.	Module	Indicative Content	Duration in minutes
Total			1170 (19hrs and 30min)

ix. Fire Services officials, 3 days

S. No.	Module	Indicative Content	Duration in minutes
1.	**Workflow & Introduction of 112**	• Introduction of 112 • Integration of 112 with Fire services • Technical Workflow of 112 • Fire Event supervision pertaining to district • Hands on Training under the supervision of Trainer	180 (3 hrs)
2.	**Event Supervisor's (ES) Portal.**	• Objective, Process, Advantages • Event Supervisor's portal • How to open ES page • Login logout • How to configure CTI extension • Verify login on CMS • Map • Merge events • Pre-empt • Event Updation • Sanchar Portal • Introduction of Sanchar portal	240 (4 hrs)

S. No.	Module	Indicative Content	Duration in minutes
		• How to effectively use the portal • E-Learning • Effective use of e-learning • How to view the content • How to attempt assessment • Map • Introduction of map • Working of map (like - village, police station, district etc. • Introduction to MDT • Login & Overview of App • Navigation and its Usage • ATR & Disposition Code • Field Event • How to create field event in MDT • MDT Troubleshooting • Integration of Various Technologies • HRMS • Admin portal • Employee portal • NexGen UP112 BI reports • MIS reporting • Data Analytics and Business Intelligence • Fire Event Analysis • Hands on Training under the supervision of Trainer	

S. No.	Module	Indicative Content	Duration in minutes
3.	**SOP**	• Adding new SOP and Updating existing SOPs (as and when required) including new types and Sub types related to Fire emergency	240 (4 hrs)
4.	**ATR. Codes.**	• Different disposition codes for submitting ATR in events in different agencies	240 (4 hrs)
5.	**Special Task to Fire Event Supervisor**	• Wrong arrival • Feedback analysis • Fire Supervisory PRV • Hands on Training under the supervision of Trainer • Troubleshoot basic system issues • Maintenance of MDTs/Mobile devices	180 (3 hrs)
	Assessment	• Examination Q & A, Certification	90 (1 hr and 30min)
Total			1170 (19 hrs and 30min)

x. Leadership Development Training, 10 days Course Schedule:

Indicative Topics
• The fundamentals of leadership and critical decision making • Principled policing and community-oriented policing efforts, and promotional aspirations • Budget, finance, and Resource allocation • Building an Effective Organization • Research methods for conducting community and organization assessments

- Analytical procedures for evaluating crime trends
- Effective communication to build trust, create transparency and foster an atmosphere of mutual respect and empathy
- Constitutional law and how it shapes law enforcement policy
- Designing of NexGen UP112 functions
- Designing Mandatory requirements
- Best Practices
- Technology Upgrades
- Manpower requirements
- One-on-one mentoring
- Group mentoring and Peer mentoring
- Identifying Needs and/or Skill Gap
- Quality assurance and quality improvements (QA & QI)
- SOP Development
- Cybersecurity Awareness
- GIS Data Collection and Maintenance
- Disaster management and analysis of hazards
- Continuity of Operations Plan

b. Re-fresher Training detailed Syllabus:

The modules described below are tentative the sequence of which can be altered according to the requirement of the class.

i. Communication officer's (COs), 7 Days

S. No.	Module	Indicative Content	Duration in minutes
1.	**Introductory session & Soft skills**	• Introductory Session • Introduction to 112 • Languages & Dialects of UP • Names of months in Hindi • Numerals in Hindi • Full forms/Abbreviations • Name of Districts/Commissionerate (Renamed District Names) • Contact Centre/OMCs • Soft Skill Session • Communication Officer • Definition of CO • Roles and Responsibilities of CO • Key success factors for CO • Emergencies Calls • Different type of Callers • Expectation of a Caller • Sympathy and Empathy • Importance of Listening Skills • Improving our Listening Skills • Quality Parameters • Accuracy of information captured during the Call • Probing for accurate address capturing • Telephone etiquette and communication skills • Responsiveness	390 (6.5 hrs)

S. No.	Module	Indicative Content	Duration in minutes
		• Voice Modulation Techniques • Do's & Don'ts for CO	
2.	**Process Skills**	• Call handling process • Different type of emergencies • Priority of event • Event type / sub type • Different type of calls • Blank calls • Abounded calls • Nuisance Calls • Outbound calls • Information calls • Follow up calls • Calls related to other integrated services • Other mode of communication – Social Media Platforms, etc • SOS • Other Desk in Contact Centres • Language Volunteers • Feedback calls • SLAs related to call handling • Cyber Crime • SIS • Woman Power Line (WPL)1090 • Calls from bordering states • Senior citizens registration	1170 (19.5 hrs)

S. No.	Module	Indicative Content	Duration in minutes
		• Complaint registration through Citizen Portal • UPCOP mobile APP • Zones / Range of UP • Fairs of UP • Famous Tourist Places / Festivals • Police Hierarchy • Organizational structure of police • Police Commissionerate system • Indian Penal Code • Code of Criminal Procedure • FIR • Government Railway Police • GIS maps / functionality • Communication officer script • Activity (script rehearsal)	
3.	**Technical Skills – Basic IT Skills/UI/ other applications**	• Software I-Net Intro • How to login / logout I-Net • How to change password • CO (Communications Officer) Software Application Layout • How to register CTI Extension • Use of Search option • Event Monitor intro • MAP Monitor Intro • How to create Event • Soft phone Interface & its Workflow	1170 (19.5 hrs)

S. No.	Module	Indicative Content	Duration in minutes
		• How to check Caller History • Actionable Call Workflow • Event Information Page overview • POI/Free Text/XY search method • LBS Call Workflow • D-Group Details • Merge Option feature & its usage • Other Desk • CO Module Login • Analog & Its Features • Hands on practice • Mock call practice • Visit of various functions • Quality HRMS sheet Session • Mock session by Quality / Ops • Operations expectation setting Session by Operations AMs	
	Assessment	• Post-training Final test Examination Q & A, Certification.	
Total			2730 (45.5 hrs)

ii. Event Supervisory Officers, 6 days

S. No.	Module	Indicative Content	Duration in minutes
1.	**Workflow & Introduction of 112**	• Introduction of 112 • Integration of 112 with other agencies & Objectives • Integrated Technologies. (Integration, Process, and workflow) • UPSRTC app • SOS 112 India app • 112 Citizen app • 108 Integration • Any other integrated services • Technical Workflow of 112 • Event supervision pertaining to district • Hands on Training under the supervision of Trainer	90 (1hr and 30min)
2.	**Soft Skills: Communication Skills**	• Introduction • Importance & Objectives • Types of Communication: Verbal & Non-Verbal • Dealing with Victim with hospitality • Types of Communication: Formal & Informal Communication of event supervisor's with PRV, Caller and concerned person.	180 (3hr)
3.	**SOP**	• Adding new SOP and Updating existing SOPs (as and when required) including new types and Sub types.	90 (1hr and 30min)
4.	**Domestic violence victim registration**	• Women's registration in 112	90 (1hr and 30min)
5.	**Escort for Safety**	• Objective, Process, Role & Advantages	90 (1hr and 30min)
6.	**Female PRV** **Supervisor PRV.**	• Objective, Process, Role & Advantages. • Objective, Process, Role & Advantages.	240 (6hr)

S. No.	Module	Indicative Content	Duration in minutes
7.	**112 Supervisor Application.**	• Installation, Objective, Process, Advantages.	90 (1hr and 30min)
8.	**Custom POI. Display**	• Objective, Process, Advantages.	90 (1hr and 30min)
9.	**Enhance Response Tagging**	• Objective, Process, Advantages	90 (1hr and 30min)
10.	**ATR. Codes.**	• Different disposition codes for submitting ATR in events in different agencies	240 (6hr)
11.	**Threat to VVIP.**	• SOPs, (Objective, Process, Advantages.)	240 (6hr)
12.	**Language Volunteers**	• Objective, Process, Advantages	90 (1hr and 30min)
13.	**#tags in Event remarks and its requirements**	• Objective, Process, Advantages	90 (1hr and 30min)
14.	**Event Supervisor's (ES) Portal.**	• Objective, Process, Advantages • Event Supervisor's portal • How to open ES page • Login logout • How to configure CTI extension • Verify login on CMS • Map • Event Dispatch • Merge events • Pre-empt • Forward to Media Cell • Star marked events • Event Updating • INETCALLTAKER	90 (1hr and 30min)

S. No.	Module	Indicative Content	Duration in minutes
		• Login logout • Event Creation • Finding caller location on Map • Transfer to DO • Contact Centre IP. Phone • Detailed information of hard phone and softphone • Login through hard phone, logout. • Sanchar Portal • Introduction of Sanchar portal • How to effectively use the portal • E-Learning • Login logout • How to Read content • How to attempt assessment • Map • Introduction of map • Working of map (like - village, police station, district etc. • Locate distance between PRV and Event location • Introduction to MDT • Responder Login & Overview of Responder App • Responder Workflow • Navigation and its Usage • ATR & Disposition Code • Type and Sub type updating • How to update event type and sub type in MDT	

S. No.	Module	Indicative Content	Duration in minutes
		• Field Event • How to create field event in MDT • MDT Troubleshooting • Integration of Various Technologies • SOS • Process of SOS creation to dispatch • Social Media Platforms • Citizen portal • Twitter • Facebook • WhatsApp • E-mail • HRMS • Admin portal • Employee portal • Leave request • Duty Roaster • Transfer etc. • ROIP • Details of application and device • NexGen UP112 BI reports • How to fetch DO login hours • Performance report • Other tools of BI etc. • Location LBS & ELS Service.	

S. No.	Module	Indicative Content	Duration in minutes
		• Location based Service: Objective, Process, Benefits. • Emergency location Service: Objective, Process, Benefits. • VTS (Vehicle Tracking System) • Live tracking of PRV • PRV History tracking • Dashboard • Patrol order sheet • Citizen portal • About 112 • Track my call • 112 UP Citizen application • Application Installation • ID Creation • Features & Functions of Application • Event closure System (Thana Module) • Event Closure URL • Event Closure Process • Fetching Pending Events • Fetching Closed Events • Event Analysis Thana Wise • Event Analysis PRV Wise • Hands on Training under the supervision of Trainer	
15.	**Special Task to Event Supervisor**	• Wrong arrival • PMS • Feedback analysis	360 (6hrs)

S. No.	Module	Indicative Content	Duration in minutes
		• Circle Supervisory PRV • Hands on Training under the supervision of Trainer • Troubleshoot basic system issues	
	Assessment	• Examination Q & A, Certification	180 (3hrs)
Total			2340 (39 hrs)

iii. RoIP Monitoring Staff, 3 days

S. No.	Module	Indicative Content	Duration in minutes
1.	**Technical Training**	• Basic Computer Knowledge & First level of Troubleshooting • Knowledge of Basic computer components • Basic Microsoft Word, Excel, and PowerPoint • Knowledge about URL • System Keys Knowledge • Networking connectivity • Introduction to CAD System • Overview & Functions • RoIP Supervisory module • Correctness of ATR report, event creation, field events, approval process. • How to chase events. • District PRV monitoring	780 (13 hrs)

S. No.	Module	Indicative Content	Duration in minutes
		• Hands on Training under the supervision of Trainer	
2.	**PMS**	• Introduction of PMS & User Creation • PRV Patrolling Route Creation • Updating & Reassigning the Route • Patrol Order Sheet Acknowledge on PRV Deviance) • Hands on Training under the supervision of Trainer	180 (3 hrs)
3.	**HRMS and BI Reports**	• Introduction of HRMS • Employee Registration on HRMS • Employee Records & Filtration • Leave Management • On Boarding: Date of Joining of Employee in 112 U.P. • Transfer Processing (Assigning Employee to another District) • Response Time (PRV/DS) • Police station/ district-wise event details • Hot Spot Analysis • GPS monitoring • Vehicle Tracking System (VTS) • MS Excel • Report generation • Hands on Training under the supervision of Trainer	165 (2 hrs and 45 min)
	Assessment	• Examination Q & A, Certification;	45 min (0.75hr)
Total			1170 (19 hrs and 30 min)

iv. PRV Field Staff, 7 days

S. No.	Module	Indicative Content	Duration in minutes
1.	**MDT & Technical Aspects**	• Introduction to 112 and technologies • SOP (Role of PRV in different events) • Introduction to MDT • Responder Login & Overview of Responder App • Responder Workflow • Navigation and its Usage • ATR & Disposition Code • Field Event • MDT Troubleshooting • Integration of Various Technologies • SOS • Hands on Training under the supervision of Trainer • Basic maintenance (MDT equipment etc.)	1170 (19 hrs and 30 min)
2.	**Soft Skills: Human Values**	• Introduction • Importance & Objective • Basic Elements of Human Values • Role, duties & Responsibilities of a PRV	120 (2 hr)
3.	**Communication skills**	• Introduction • Importance & Objectives • Types of Communication: Verbal & Non-Verbal • Types of Communication: Formal & Informal • Dealing with Victim	120 (2 hr)

S. No.	Module	Indicative Content	Duration in minutes
		• Negotiation Skills & its use in Managing the Situation	
4.	**Dispute Resolution Skills**	• Introduction & Meaning • Importance • Event Types & Sub-Types • Elements of Dispute • Taking Control of the situation • Amicable Resolution of Dispute • Dispute Resolution Techniques • Alternate Dispute Resolution • Escalations to Senior Officers	120 (2 hr)
5.	**First Aid**	• Introduction, Objective & Importance • Specialized training by Govt Doctor • How to handle a burns victim? • How to provide First aid during an emergency situation? • Conditions requiring first aid • Initial Check-up • First Aid for different injuries and illness • Types of Bandages and their respective use • Temporary Stretcher • CPR/ Basic Life-saving skills • Pandemic/Covid 19 and Protocol • Role of PRV & Problems faced by PRV	120 (2 hr)
6.	**Adult Psychology**	• Introduction, Objective, Importance & meaning • Specialized training in human psychology • Transactional Analysis	120 (2 hr)

S. No.	Module	Indicative Content	Duration in minutes
		• Ego Stages & Respective Approach • Methods to Understand Person's Behaviour • Stages of Life • Stroke	
7.	**Stress Management & Motivation**	• Pranayama/Simple breathing • Yoga & Meditation, Positive thinking • Stress release tools • Self-motivation	120 (2 hr)
8.	**Crime Scene Management**	• Introduction & Importance • Familiarization with Crime Scene Protection Kit • Usage of Crime Scene Protection Kit Contents • Securing a Crime Spot	120 (2 hr)
9.	**Disaster Management**	• Introduction and Objective • Types of Disaster • Important Terminology • Assessment of Risk • Disaster Management & Disaster Management Cycle • Important Points to spread awareness • Important Points from Disaster Management Act – 2005 • Role of PRV & Problems faced by PRV	120 (2 hr)
10.	**Fire & Safety**	• Introduction, Objective & Importance • Event Types & Sub-Types, trends from recent data • Elements of Fire • Coordination with Fire department • Classification of Fire	60 (1 hr)

S. No.	Module	Indicative Content	Duration in minutes
		• Principles of Fire Extinguishing • Fire Fighting Equipment Emergency Response in case of Fire Accident Role of PRV & Problems faced by PRV	
11.	**Issues Related to Women**	• Introduction, Meaning & Gender Sensitization • How to handle a female victim (Aggressive, agitated, and abusive victims)? • Importance • Event Types & Sub-Types, trends from recent data • The Protection of Women from Domestic Violence Act, 2005 • The Immoral Traffic (Prevention) Act, 1956 • Issues persistent to women and reasons for crime against them • Important Legal Provisions Role of PRV & Problems faced by PRV, seeking guidance from NGO, Women Power Line (1090) etc.,	60 (1 hr)
12.	**Child Related Issues**	• Introduction & Meaning and Sensitization about Children related issues • Importance • Event Types & Sub-Types, trends from recent data • The Bonded Labour System (Abolition) ACT, 1976 • The Immoral Traffic (Prevention) Act, 1956. • The Juvenile Justice (Care and Protection of Children) Act, 2015. • POCSO Act, IT Act & digital/internet vulnerabilities • Types of Violence Issues persistent to child and reasons for crime against them Important Legal Provisions • Role of PRV & Problems faced by PRV	60 (1 hr)

S. No.	Module	Indicative Content	Duration in minutes
		• Seeking guidance from NGO such as Mother and Childcare centre, Childcare education and welfare society, etc.,	
13.	**Issues Related to Elderly People**	• Introduction & Meaning and sensitization about elderly people • Importance • Maintenance and Welfare of Parents and Senior Citizens Act, 2007 • Event Types & Sub-Types, trends from recent data • Issues persistent to elderly people and reasons for crime against them • 'SAVERA APP' • Important Legal Provisions Role of PRV & Problems faced by PRV, seeking guidance from NGOs for Sr. Citizen	60 (1 hr)
14.	**Issues Related to differently abled people**	• Introduction & Meaning and sensitization about differently abled people • Importance Event types & Sub-types, trends from recent data types • Symptoms of Intellectually challenged Issues persistent to Mentally Challenged Important Legal Provisions Role of PRV & Problems faced by PRV • Seeking help from NGO and associated agencies	60 (1 hr)
15.	**Traffic Management**	• Role of PRV • Introduction, Objective & Importance • Event Types & Sub-Types, trends from recent data. • Important Facts & Figures • Reasons for Road Accidents	60 (1 hr)

S. No.	Module	Indicative Content	Duration in minutes
		• Role & Responsibilities of Driver • Traffic Signals & Markings and rules • Important Points	
16.	**Tourism Related Issues**	• Introduction, Objective & Importance • Types of Tourism • Modes of Travel • Issues Persistent to Tourism • Communication skills and hospitality towards foreign travellers • Important Points from Relevant Indian Laws related to Tourists and Tourism • Steps Taken by Ministry of Tourism for Safety and Convenience of Tourists • Role of PRV & Problems faced by PRV	60 (1 hr)
17.	**Training of In-fleet components**	• Protocol for sound & LED light bar • How to use and maintain in-fleet components • Use of Wireless set • Service Ticket registration for faulty/damaged equipment	60 (1 hr)
	Miscellaneous	• Rescuing Animal (injured in road accidents) • Supporting transgender during emergency • SC/ST act important provision • Daily revision session • New Acts, Amendments to existing Acts discussed in above topics. • Feedback • Valedictory session	60 (1 hr)

S. No.	Module	Indicative Content	Duration in minutes
	Assessment	• Post-training test Examination Q & A, Certification;	60 (1 hr)
Total			2730 (45 hrs and 30 minutes)

v. PRV Pilot, 4 days

S. No.	Module	Indicative Content	Duration in minutes
1.	**MDT & Technical Aspects**	• Introduction to 112 and technologies • SOP (Role of PRV in different events) • Introduction to MDT • Responder Login & Overview of Responder App • Responder Workflow • Navigation and its Usage • ATR & Disposition Code • Field Event • MDT Troubleshooting • Integration of Various Technologies • SOS • Hands on Training under the supervision of Trainer	390 (6 hrs and 30 min)
2.	**In fleet equipment & their uses**	• Use of Wireless set • Using light and sound console • Use of Emergency Warning system • Use of body armour	300 (5 hrs)

S. No.	Module	Indicative Content	Duration in minutes
		• Hands on Training under the supervision of Trainer • How to use and maintain in-fleet components • Service Ticket registration for faulty/damaged equipment	
3.	**Important practical topics for PRV staff**	• Human Values • Communication skills • Adult Psychology • Dispute Resolution • Issues related to • Women • Children • Elderly • Differently abled • Fire safety • Disaster Management • Tourism • Traffic Management • Stress management and personal health • HRMS and Biometric attendance • Hands on Training under the supervision of Trainer	300 (5 hrs)
4.	**First Aid**	• Need and conditions for First Aid • CPR/ Basic Lifesaving skills • Trauma Management • Applying ABC and CAD • Control severe bleeding • Using splint,	300 (5 hrs)

S. No.	Module	Indicative Content	Duration in minutes
		• Stabilising head and cervical	
	Assessment	• Miscellaneous • Examination Q & A, Certification;	300 (5 hrs)
Total			1560 (26 hrs)

vi. Police Station staff, 1 day

S. No.	Module	Indicative Content	Duration in minutes
1.	**Technical Training**	• Introduction to NexGen UP112, duty, roles, and responsibilities of Police Station staff • CAD Application: • Event Creation • Event Dispatch • MDT operations • Event Closure System • Integrations in CAD • Hands on Training under the supervision of Trainer	120 (2 hrs)
2.	**Reporting and Monitoring**	• HRMS • BI Reports • VTS • PMS • Incident Dashboard • Incident Analysis	120 (2 hrs)

S. No.	Module	Indicative Content	Duration in minutes
		• Hands on Training under the supervision of Trainer	
3.	**Other**	• VVIP threats • Female PRV • Abusive and Nuisance Caller SOP • Savera • Sanchar • Domestic Violence • Hands on Training under the supervision of Trainer	120 (2 hrs)
	Assessment	• Examination Q & A, Certification;	30 (30 min)
Total			390 (6:30 hrs)

vii. Office Support Staff in HQ, 1 day

S. No.	Module	Indicative Content	Duration in minutes
1.	**Technical Training**	• Introduction to NexGen UP112, duty, roles and responsibilities of Office support staff deployed in respective departments. • Overview of applications used in NexGen UP112 • Introduction to the role specific application • Features and Functionality of role specific applications • Asset management application features • Monitoring of Calls and its evaluation • How to access to Call logger application • Call logger features and user rights	120 (2 hrs)

		• How to audit the call quality and fact finding • Identifying high areas of concern from the system • Prioritizing the concern and reporting to higherups • Hands on Training under the supervision of Trainer	
2.	**Reporting and Monitoring**	• Asset management application reports • HRMS • HRMS reports • Leave management • Data analytics and Review of performance • MIS • Data representation • BI Reports • Preparing of reports in specific formats • Review periodic reports and send collated reports to senior management • Dashboard • Analysis of data • Hands on Training under the supervision of Trainer	120 (2 hrs)
3.	**Other**	• Report writing skills • Information related to RTI	120 (2 hrs)
	Assessment	Examination Q & A, Certification;	30 (30 min)
Total			390 (6:30 hrs)

viii. Fire Services officials, 2 days

S. No.	Module	Indicative Content	Duration in minutes
1.	**Workflow & Introduction of 112**	• Introduction of 112 • Integration of 112 with Fire services • Technical Workflow of 112 • Fire Event supervision pertaining to district • Hands on Training under the supervision of Trainer	60 (1 hr)
2.	**Event Supervisor's (ES) Portal**	• Objective, Process, Advantages • Event Supervisor's portal • How to open ES page • Login logout • How to configure CTI extension • Verify login on CMS • Map • Merge events • Pre-empt • Event Updation • Sanchar Portal • Introduction of Sanchar portal • How to effectively use the portal • E-Learning • Effective use of e-learning • How to view the content • How to attempt assessment • Map • Introduction of map • Working of map (like - village, police station, district etc.	120 (2 hrs)

S. No.	Module	Indicative Content	Duration in minutes
		• Introduction to MDT • Login & Overview of App • Navigation and its Usage • ATR & Disposition Code • Field Event • How to create field event in MDT • MDT Troubleshooting • Integration of Various Technologies • HRMS • Admin portal • Employee portal • NexGen UP112 BI reports • MIS reporting • Data Analytics and Business Intelligence • Fire Event Analysis • Hands on Training under the supervision of Trainer	
3.	**SOP**	Adding new SOP and Updating existing SOPs (as and when required) including new types and Sub types related to Fire emergency	150 (1 hr and 30min)
4.	**ATR. Codes.**	Different disposition codes for submitting ATR in events in different agencies	240 (2 hrs)
5.	**Special Task to Fire Event Supervisor**	Wrong arrival Feedback analysis Fire Supervisory PRV Hands on Training under the supervision of Trainer Troubleshoot basic system issues Maintenance of MDTs/Mobile devices	120 (2 hrs)

S. No.	Module	Indicative Content	Duration in minutes
	Assessment	Examination Q & A, Certification	90 (1 hr and 30min)
Total			780

4.29.9 e-Learning Module

MSI is required to manage the eLearning module for administration, tracking, reporting and delivery of learning courses or training programs. UP112 may use the module to manage any other training program beyond what MSI is providing. The objective is to upgrade e-learning module and audio-visual learnings.

The module shall be available to be used by UP112 resources to access learning content and to create, deliver, monitor participation, and assess attendees/ trainees' performance.

For the police personnel on the field, the bidder shall design an e-Learning module that can be accessed through the MDT devices installed in their vehicles.

MSI should ensure that the e-Learning modules are not limited to Technical aspects of the solution but should also include the SOPs as defined by UP112.

In order to track the effectiveness of training programmers, MSI should also provide an online catalogue of e-Learning modules and allow for Training and Competency Assessment through online tests.

The module shall ensure that for each of the learner groups identified, the system shall enable the user to define the learning path and allow for mandatory trainings along with schedules to complete these trainings.

Also, the system should allow to track the performance of the trainee before and after training, helping in analysing the impact analysis of the training.

Some of the key requirements of the eLearning module:

a. The MSI shall design and provide content for training, in case the content is being provided by UP112, the MSI shall upload the content on the module.
b. The content shall be tailor-made, easy, and convenient to use and shall be categorized based on the proficiency level of the user. Should ensure active and effective learning by participants.
c. The e-learning levels may be defined (Beginner, Intermediate, Advanced) and identified by the MSI in consultation with UP112.
d. The content shall include text, documents, audio, video, simulations etc.
e. The system shall record the feedback of trainees for all trainings conducted online or offline and shall provide analysis as per requirements of UP112.
f. The system shall mandate users to under-go any trainings without skipping any content as per the requirements and shall also provide soft copy of certificates generated from the system.
g. The MSI shall regularly update the content of the courses as per the defined periodicity in consultation with UP112.
h. MSI shall create a detailed Dashboard with insights of learning records for each trainee including details like date of completion, assessment score, progress of training course etc. and option to download intelligence reports from the admin account in different formats like .xlsx, pdf, csv etc.
i. The module shall generate regular notifications and alerts to the users reminding them of any trainings which are due or the trainings for which deadlines have already been crossed.
j. Auto search functionality for video lectures/training modules.
k. Content should have subtitles wherever possible

l. Intelligent suggestions based on user history and course content Customisation as per skills and course recommendations
m. Recommendations based on the trainings undertaken/signed up for.
n. Small videos/quick learnings
o. Pop up with training summary while hovering over recommended trainings
p. Automatic SMS reminders to supervisors of new content, learners with past due modules, and learners with routinely low assessment scores.

4.29.10 Training Effectiveness Evaluation/Training Assessment

a. MSI shall evaluate the effectiveness of all end-users' trainings via online and/or manual surveys.
b. The MSI shall prepare a question/answer bank for all the trainings and get it approved by UP112. Random questions will be selected and uploaded for online assessment.
c. SI shall make all arrangements for conducting the test online (including data entry in simulated environment).
d. Online examination would be administered in the presence of competent supervisors.
e. Scoring a minimum of 70% marks by each trainee shall conclude the success of a training.
f. MSI shall consolidate the results and submit it to UP112. In case the result is found to be unsatisfactory, MSI shall undertake the trainings as again times as required to meet the expectations of UP112 at no additional cost.

4.29.11 Feedback Mechanism

a. A periodic maturity level analysis of trainees shall be conducted from time to time to assess the impact of the trainings conducted. This assessment should be facilitated through UP112.
b. The trainings shall be assessed based on the trainee feedback collected for each training course. MSI shall design the trainee feedback template in consultation with UP112. The objective of the feedback is to assess the quality of the sessions and the trainees' understanding and takeaways from the session.
c. In case of an unsatisfactory (below average feedback from 50% of the trainees) feedback, MSI will be required to repeat the session at no extra cost to UP112. In case the feedback is still the same, the MSI will be required to change the trainer.
d. Access to training feedback should be given to the UP112 for performance monitoring of MSI.
e. A transparent mechanism shall be devised by MSI and approved by UP112 for certifying the trainees.
f. Upon completion of trainings, MSI would have to ensure that attendees submit their feedbacks. MSI would be required to send across the link of web-based feedback forms to every attendee via text message/email. Filling of feedback form would be made mandatory.

5 ADDITIONAL TERMS AND CONDITIONS OF THE CONTRACT

5.1 Definitions

5.1.1 "Acceptance of System": The system shall be deemed to have been accepted by the ITECCS, subsequent to its installation, rollout, and deployment of trained manpower, when all the activities as defined in Scope of Work have been successfully executed and completed to the satisfaction of ITECCS.

5.1.2 "ATCG" means Additional Terms and Conditions of Contract

5.1.3 "Bidder's Team" means the Bidder who has to provide goods and services to the ITECCS under the scope of this Contract. This definition shall also include any and/or all of the employees of the Bidder, authorized MSIs or partners and representatives or other personnel employed or engaged either directly or indirectly by the Prime Bidder or the Consortium Members for the purposes of this Contract.

5.1.4 "Bidder" means organization or consortium submitting the proposal in response to this RFP

5.1.5 "Buyer" shall mean Government of Uttar Pradesh (GoUP) acting through Integrated Technology Enabled Citizen Centric Services (ITECCS) unit of UP Police and its successors and assignees "Contract" means the Contract entered into by the parties with the entire documentation specified in the RFP.

5.1.6 "Commercial Off-The-Shelf (COTS)" refers to software products that are ready-made and available for sale, lease, or license to the general public.

5.1.7 "Communication officers" means all outsourced staff deployed at UP112 Contact Centre at Lucknow, OMC centres at Prayagraj and Ghaziabad. These staff will be the first point of contact to any caller.

5.1.8 "Consortium" means the entity named in the contract for any part of the work has been sublet with the consent in writing of ITECCS and the heirs, legal representatives, successors, and assignees of such person. The entry of consortium is as per constitution of Consortium described in clause 5.9 and Annexure 18 and 19.

5.1.9 "Contract Value" means the price payable to the Bidder under this Contract for the full and proper performance of its contractual obligations.

5.1.10 "Data Center site" means the DC sites including their respective Data Centre space, Communications Room and Non-Data Centre space wherein the delivery, installation, integration, management, and maintenance services as specified under the scope of work are to be carried out for the purpose of this Contract. The site for DC is already setup in ITECCS Headquarters, Lucknow, and Disaster Recovery Centre (DRC) will be hosted on cloud by the bidder. The DRC site should be outside UP state and in a different seismic zone.

5.1.11 "Document" means any embodiment of any text or image however recorded and includes any data, text, images, sound, voice, codes, databases, or any other electronic documents as per IT Act etc.

5.1.12 "Effective Date" means the date on which this Contract is signed or LoI is issued by ITECCS, whichever is earlier and executed by the parties hereto. If this Contract is executed in parts, then the date on which the last of such Contracts is executed shall be construed to be the Effective Date.

5.1.13 "GCC" means General Conditions of Contract

5.1.14 "Goods" means all of the equipment, sub-systems, hardware, software, products accessories, software and/or other material OR items which the Bidder is required

to supply, install, and maintain under the contract.

5.1.15 "Intellectual Property Rights" means any patent, copyright, trademark, trade name, service marks, brands, proprietary information whether arising before or after the execution of this Contract and the right to ownership and registration of these rights.

5.1.16 "ITECCS" means Integrated Technology Enabled Citizen Center Services. ITECCS is a unit of Uttar Pradesh Police which works under the leadership of ADG UP112.

5.1.17 "LOI" means Letter of Intent to be issued by the ITECCS to the successful bidder for awarding the contract.

5.1.18 "Master System Integrator (MSI)" means the bidder who is selected by ITECCS at the end of this RFP process. The MSI will carry out all the services mentioned in the scope of work of this RFP.

5.1.19 "Notice" means:

a notice; or

a consent, approval or other communication required to be in writing under this Contract.

5.1.20 "OEM" means the Original Equipment Manufacturer of any equipment or system or software or product which are providing such goods to the ITECCS under the scope of this RFP

5.1.21 "Project" shall mean procurement, migration, installation and integration of technology solution, deployment of trained manpower and operations and maintenance of UP112 at ITECCS, Lucknow, Operational Mirroring Centres and all identified field locations.

5.1.22 "Prime bidder" shall mean the lead bidder in case of bid submitted by the Consortium or single bidder in case of bid submitted by the single entity.

5.1.23 "Replacement MSI" means the organization replacing the bidder in case of contract termination for any reasons.

5.1.24 "Services" means the work to be performed by the MSI pursuant to this RFP and to the contract to be signed by the parties in pursuance of any specific assignment awarded by ITECCS.

5.1.25 "Shadow Support" shall mean that TSP will provide all resources (as per his contract) for running UP112 ERSS but will not be actually operating the system rather assisting the resources of NexGen UP112 provided by MSI

5.1.26 "Sub-Contractor" shall mean the entity named in the contract for any part of the work or any person to whom any part of the contract has been sublet with the consent in writing of ITECCS and the heirs, legal representatives, successors, and assignees of such person.

5.1.27 "UP112" means the Emergency Response Support System (ERSS) managed by ITECCS under Uttar Pradesh Police.

5.2 Interpretations

In this Contract unless a contrary intention is evident:

5.2.1 the clause headings are for convenient reference only and do not form part of this Contract.

5.2.2 unless otherwise specified a reference to a clause number is a reference to all of its sub-clauses.

5.2.3 the word "include" or "including" shall be deemed to be followed by "without limitation" or "but not limited to" whether or not they are followed by such phrases.

5.2.4 unless otherwise specified a reference to a clause, sub-clause or section is a

reference to a clause, sub-clause or section of this Contract including any amendments or modifications to the same from time to time.

5.2.5 a word in the singular includes the plural and a word in the plural includes the singular.

5.2.6 a word importing a gender includes any other gender.

5.2.7 a reference to a person includes a partnership and a body corporate.

5.2.8 a reference to legislation includes legislation repealing, replacing or amending that legislation.

5.2.9 where a word or phrase is given a particular meaning, it includes the appropriate grammatical forms of that word or phrase which have corresponding meanings.

5.2.10 in the event of an inconsistency between the terms of this Contract and the RFP and the Bid, the terms hereof shall prevail.

5.3 Condition's precedent

This Contract is subject to the fulfilment of the following conditions precedent by the Selected Bidder:

5.3.1 Furnishing by the Successful Bidder, an unconditional, irrevocable, and continuing Bank Guarantee for Contract Performance, in a form and manner as stipulated in clause 2.15.

5.3.2 Execution of a Deed of Indemnity in terms of Clause 5.15.

5.3.3 Obtaining of all statutory and other approvals required for the performance of the Services under this Contract

5.3.4 Furnishing of such other documents as the Buyer may specify

5.3.5 The Buyer reserves the right to waive any or all the conditions specified above in writing and no such waiver shall affect or impair any right, power, or remedy that the Buyer may otherwise have

5.4 Representations & warranties

5.4.1 In order to induce the ITECCS to enter into the Contract, the MSI hereby represents and warrants as of the date hereof, which representations and warranties shall survive the term and termination hereof, the following:

5.4.2 That the MSI is a company which has the requisite experience in providing Services related to setting up of police emergency response system, the technical know-how and the financial wherewithal, the power and the authority that would be required to successfully commission the project and operate the UP112 and OMC Centers and to enter into the Contract and provide the Services sought by ITECCS, for the purposes of the Contract.

5.4.3 That the bidder is not involved in any major litigation, potential, threatened and existing, that may have an impact of affecting or compromising the delivery of Services of the Contract.

5.4.4 That the representations made by the bidder in its Bid are and shall continue to remain true and fulfil all the requirements as are necessary for executing the obligations and responsibilities as laid down in the Contract and the Bid and unless the ITECCS specifies to the contrary, the bidder shall be bound by all the terms of the Bid Document.

5.4.5 That the bidder has the professional skills, personnel, infrastructure, and resources/authorizations that are necessary for providing all such services as are necessary to fulfil the Schedule of Requirements stipulated in the Bid Document and the Contract.

5.4.6 That the bidder shall ensure that all assets including but not limited to equipment, licenses, etc. developed, procured, deployed, and created during the term of the Contract are duly maintained and suitably updated, replaced with regard to contemporary requirements

5.4.7 That the bidder shall use such assets of the UP112 as ITECCS may permit for the sole purpose of execution of its obligations under the terms of the Bid Document, or the Contract. The bidder shall, however, have no claim to any right, title, lien, or other interest in any such property, and any possession of property for any duration whatsoever shall not create any right in equity or otherwise, merely by fact of such use or possession during or after the term hereof.

5.4.8 That during the term of the Contract, the bidder shall procure insurance policies for all its present and future property and assets that are developed, procured, and created for fulfilment of obligations under the Contract with financially sound and reputable insurers to the satisfaction of ITECCS and shall pay all premium in relation thereto and shall ensure that nothing is done to make such insurance policies void or voidable. The bidder shall also furnish to ITECCS a certificate evidencing such insurance, risks covered, names of beneficiaries, expiration dates, names of insurers and all other features of the insurance policy, both original and renewed and shall keep the same alive during the term of the Contract

5.4.9 That the bidder shall procure all the necessary permissions and adequate approvals and licenses for use of various software and any copyrighted process or product free from all claims, titles, interests, and liens thereon and shall keep ITECCS indemnified in relation thereto.

5.4.10 That all the representations and warranties as have been made by the MSI with respect to its Bid and Contract, are true and correct, and shall continue to remain true and correct through the term of the Contract.

5.4.11 That the execution of the Services herein is and shall be in accordance and in compliance with all applicable laws.

5.4.12 That it has not been initiated nor is it pending nor are there threatened any legal proceedings against any bidder or it's Team which adversely affects or may affect performance under the Contract.

5.4.13 That the MSI has the corporate power to execute, deliver and perform the terms and provisions of the Contract and has taken all necessary corporate action to authorise the execution, delivery, and performance by it of the Contract.

5.4.14 That all Conditions Precedent under the Contract have been satisfied.

5.4.15 That neither the execution and delivery by the bidder of the Contract nor the bidder's compliance with or performance of the terms and provisions of the Contract (i) will contravene any provision of any Applicable Law or any order, writ, injunction or decree of any court or Governmental Authority binding on the bidder, (ii) will conflict or be inconsistent with or result in any breach of any of the terms, covenants, conditions or provisions of, or constitute a default under any agreement, contract or instrument to which the bidder is a party or by which it or any of its property or assets is bound or to which it may be subject or (iii) will violate any provision of the Memorandum and Articles of Association of the bidder.

5.4.16 That the MSI certifies that all registrations, recordings, filings and notarisations of the Contract and all payments of any tax or duty, including without limitation stamp duty, registration charges or similar amounts which are required to be effected or made by the bidder, which is necessary to ensure the legality, validity, enforceability, or admissibility in evidence of the Contract have been made.

5.4.17 That the MSI confirms that there has not and shall not occur any execution, amendment or modification of any agreement or contract without the prior written consent of ITECCS, which may directly or indirectly have a bearing on the Contract

5.4.18 That the MSI owns or has good, legal, or beneficial title, or other interest in, to the property, assets, and revenues of the bidder on which it grants or purports to grant or create any interest pursuant to the Contract, in each case free and clear of any encumbrance and further confirms that such interests created or expressed to be created are valid and enforceable.

5.4.19 That the MSI owns, has license to use or otherwise has the right to use, free of any pending or threatened liens or other security or other interests all Intellectual Property Rights, which are required or desirable for the project and the bidder does not, in carrying on its business and operations, infringe any Intellectual Property Rights of any person. None of the Intellectual Property or Intellectual Property Rights owned or enjoyed by the MSI or which the MSI is licensed to use, which are material in the context of the MSI's business and operations are being infringed nor, so far as the bidder is aware, is there any infringement or threatened infringement of those Intellectual Property or Intellectual Property Rights licensed or provided to the bidder by any person. All Intellectual Property Rights (owned by the bidder or which the bidder is licensed to use) are valid and subsisting. All actions (including registration, payment of all registration and renewal fees) required to maintain the same in full force and effect have been taken thereon and shall keep ITECCS indemnified in relation thereto.

5.5 Scope of work

5.5.1 Scope of the project is defined in Section 4 of this RFP.

5.6 Key performance measurements

5.6.1 The Buyer shall define key performance indicators for this project to measure the performance of the MSI in good faith.

5.6.2 The Buyer reserves the right to monitor the performance of the MSI and the quality of the services delivered by the MSI, not limitation to service levels pursuant to Section 6 of this RFP.

5.7 Standards of performance

5.7.1 The MSI shall perform the Services and carry out its obligations under the Contract with due diligence, efficiency, and economy, in accordance with generally accepted techniques and best practices used in the industry and with standards recognized by international professional bodies and shall observe sound management, engineering and security practices. It shall employ appropriate advanced technology and engineering practices and safe and effective equipment, machinery, material, and methods. The MSI shall always act, in respect of any matter relating to the Contract, as faithful advisors to the Buyer and shall, always, support and safeguard the Buyer legitimate interests.

5.8 Approvals and Required Consents

5.8.1 The MSI to obtain required permissions from various department for Right-of-Way (ROW) clearance. ITECCS shall provide necessary support in terms of issuing letters for ROW clearance. Further, the MSI cannot claim any additional/extra amount or time (for achieving milestone) associated for ROW clearance from the Buyer. Delay in getting ROW permission should not amount to delay in

commissioning of the site.

5.8.2 The MSI to obtain required permissions for installing the RF end point equipment at public or private premise rooftops. In case an RF Tower is installed in the premises, it should not be used for any other commercial activities other than required/approved by ITECCS in writing. In any case, the MSI cannot claim any additional/extra amount associated for supply, installation and maintenance of RF tower.

5.9 Constitution of Consortium

5.9.1 For the purposes of fulfilment of its obligations as laid down under the Contract, where the ITECCS deems fit and unless the contract requires otherwise, Prime Bidder shall be the sole point of interface for the ITECCS and would be absolutely accountable for the performance of its own, the other member of Consortium and/or its Team's functions and obligations.

5.9.2 The Consortium member has agreed that the Prime Bidder is the prime point of contact between the Consortium member and the ITECCS and it shall be primarily responsible for the discharge and administration of all the obligations contained herein and, the ITECCS, unless it deems necessary shall deal only with the Prime Bidder.

5.9.3 Without prejudice to the obligation of the Consortium member to adhere to and comply with the terms of this Contract, the Consortium member has executed and submitted a Power of Attorney in favour of the Prime Bidder authorizing him to act for and on behalf of such member of the Consortium and do all acts as may be necessary for fulfilment of contractual obligations.

5.9.4 The ITECCS reserves the right to review, approve and require amendment of the terms of the Consortium Contract or any contract or agreements entered into by and between the members of such Consortium and no such agreement/contract shall be executed, amended, modified and/or terminated without the prior written consent of the ITECCS. An executed copy of each of such agreements/contracts shall, immediately upon execution be submitted by the Prime Bidder to the ITECCS.

5.9.5 Where, during the term of this Contract, the Prime Bidder terminates any contract/arrangement or agreement relating to the performance of Services, the Prime Bidder shall be responsible and severally liable for any consequences resulting from such termination. The Prime Bidder shall in such case ensure the smooth continuation of Services by providing a suitable replacement to the satisfaction of the ITECCS at no additional charge and at the earliest opportunity.

5.10 Term and extension of the contract

5.10.1 The Contract Period for the services shall include the implementation phase of 5 months followed by Operation and Maintenance phase for 5 years after the UAT of the implementation phase. The Contract may be further extended up to 3 years annually on the basis of satisfactory performance. The bidder shall ensure the support for all the deployed components and services from the respective OEM for 8 years. The MAF will be provided accordingly as per Annexure – 12 of Section 9 of this RFP.

5.10.2 The ITECCS shall reserve the sole right to grant any extension to the term above mentioned subject to the Buyer's obligations at law and shall notify in writing to the MSI, at least three (3) months before the expiration of the Term hereof, whether it will grant the Bidder an extension of the Term.

5.10.3 The ITECCS reserves the right to extend the Term for a period up to three (3) years,

such extensions shall be on annual basis and on the same terms and conditions and at the same rate quoted for the fifth year of the O&M phase of the contract. The bidder to ensure the necessary support services of all products and applications from respective OEMs during this period. No additional payment shall be applicable during this period other than the fifth year AMC cost.

5.11 Insurance

5.11.1 The Goods supplied under this project shall be comprehensively insured by the MSI at their own cost, against any loss or damage, theft for the entire period of the Contract. The MSI shall submit to the ITECCS, documentary evidence issued by the insurance company, indicating that such insurance has been taken.

5.11.2 The MSI shall bear all the statutory levies like customs, insurance, freight, etc. applicable on the goods and the charges like transportation, packaging, delivery etc. that may be applicable till the goods are delivered at the respective sites of installation.

5.11.3 The MSI shall take out and maintain at its own cost, on terms and conditions approved by the ITECCS, insurance against the risks, and for the coverages, at the request of the ITECCS, the MSI shall provide evidence of such insurance taken out and maintained and that the current premiums therefor have been paid.

5.12 Insolvency of bidder

5.12.1 In the event of the MSI being adjudged insolvent or going voluntarily into liquidation or having received order or other order under Insolvency act made against Company or, the passing of any resolution, or making of any order for winding up whether voluntarily or otherwise, or in the event of the MSI failing to comply with any of the conditions herein specified, the Buyer shall have the power to terminate the contract without previous notice.

5.13 Sub-contracts

5.13.1 The MSI shall provide all the services through its own company and no sub-contracting is allowed.

5.14 Payment to MSI

5.14.1 ITECCS shall make payments to the MSI at the times and in the manner set out in the Payment schedule as specified in Section 8 of this RFP. ITECCS will make all efforts to make payments to the Prime Bidder within 30 days of receipt of invoice (s) and all necessary supporting documents.

5.14.2 All payments agreed to be made by ITECCS to the MSI in accordance with the Financial Bid shall be inclusive of all statutory levies, duties, taxes and other charges whenever levied or applicable, if any, and ITECCS shall not be liable to pay any such levies or other charges under or in relation to this Contract and/or the Services.

5.14.3 No invoice for extra work or change order on account of change order will be submitted by the Bidder unless the said extra work or change order has been authorized or approved by the ITECCS in writing in accordance with Change Control Note (Annexure I of this section of the RFP).

5.14.4 In the event of ITECCS noticing at any time that any amount has been disbursed wrongly to the MSI or any other amount is due from the MSI to the ITECCS, the ITECCS may without prejudice to its rights recover such amounts by other means

after notifying the MSI or deduct such amount from any payment falling due to the MSI. The details of such recovery, if any, will be intimated to the MSI. The MSI shall receive the payment of undisputed amount under subsequent invoice for any amount that has been omitted in previous invoice by mistake on the part of the ITECCS or the MSI.

5.14.5 All payments to the MSI shall be subject to the deductions of tax at source under Income Tax Act, and other taxes and deductions as provided for under any law, rule or regulation. All costs, damages or expenses which ITECCS may have paid or incurred, for which under the provisions of the Contract, the Bidder is liable, the same shall be deducted by ITECCS from any dues to the MSI. All payments to the MSI shall be made after making necessary deductions as per terms of the Contract and recoveries towards facilities, if any, provided by the ITECCS to the MSI on chargeable basis.

5.15 Indemnification and Limitation of Liability

5.15.1 MSI (the "Indemnifying Party") undertakes to indemnify, hold harmless the Buyer (the "Indemnified Party") from and against all claims, liabilities, losses, expenses (including reasonable attorneys' fees), fines, penalties, taxes or damages (Collectively “Loss”) on account of bodily injury, death or damage to tangible personal property arising in favour of any person, corporation or other entity (including the Indemnified Party) attributable to the Indemnifying Party's negligence or wilful default in performance or non-performance under this Agreement.

5.15.2 If the Indemnified Party promptly notifies Indemnifying Party in writing of a third-party claim against Indemnified Party that any Service provided by the Indemnifying Party infringes a copyright, trade secret or patents incorporated in India of any third party, Indemnifying Party will defend such claim at its expense and will pay any costs or damages, that may be finally awarded against Indemnified Party.

5.15.3 Indemnifying Party will not indemnify the Indemnified Party, however, if the claim of infringement is caused by:

a. Indemnified Party’s misuse or modification of the Service.
b. Indemnified Party’s failure to use corrections or enhancements made available by the Indemnifying Party.
c. Indemnified Party’s use of the Service in combination with any product or information not owned or developed by Indemnifying Party.

5.15.4 However, if any service, information, direction, specification or materials provided by Indemnified Party or any third party Contracted to it, is or likely to be held to be infringing, Indemnifying Party shall at its expense and option either

a. Procure the right for Indemnified Party to continue using it
b. Replace it with a non-infringing equivalent
c. Modify it to make it non-infringing.

The foregoing remedies constitute Indemnified Party’s sole and exclusive remedies and Indemnifying Party’s entire liability with respect to infringement.

5.15.5 The indemnities set out in Clause 5.15 shall be subject to the following conditions:

a. The Indemnified Party as promptly as practicable informs the Indemnifying Party in writing of the claim or proceedings and provides all relevant evidence, documentary or otherwise.

b. The Indemnified Party shall, at the cost of the Indemnifying Party, give the Indemnifying Party all reasonable assistance in the defence of such claim including reasonable access to all relevant information, documentation, and personnel provided that the Indemnified Party may, at its sole cost and expense, reasonably participate, through its attorneys or otherwise, in such defence.

c. If the Indemnifying Party does not assume full control over the defence of a claim as provided in this Article, the Indemnifying Party may participate in such defence at its sole cost and expense, and the Indemnified Party will have the right to defend the claim in such manner as it may deem appropriate, and the cost and expense of the Indemnified Party will be included in Losses.

d. The Indemnified Party shall not prejudice, pay or accept any proceedings or claim, or compromise any proceedings or claim, without the written consent of the Indemnifying Party.

e. All settlements of claims subject to indemnification under this Clause will:

   i. be entered only with the consent of the Indemnified Party, which consent will not be unreasonably withheld and include an unconditional release to the Indemnified Party from the claimant or plaintiff for all liability in respect of such claim; and

   ii. include any appropriate confidentiality agreement prohibiting disclosure of the terms of such settlement.

f. The Indemnified Party shall account to the Indemnifying Party for all awards, settlements, damages and costs (if any) finally awarded in favour of the Indemnified Party which are to be paid to it in connection with any such claim or proceedings.

g. The Indemnified Party shall take steps that the Indemnifying Party may reasonably require mitigating or reduce its loss because of such a claim or proceedings.

h. If the Indemnifying Party is obligated to indemnify an Indemnified Party pursuant to this Article, the Indemnifying Party will, upon payment of such indemnity in full, be subrogated to all rights and defences of the Indemnified Party with respect to the claims to which such indemnification relates; and

i. If a Party makes a claim under the indemnity set out under Clause 5.15 above in respect of any Loss or Losses, then that Party shall not be entitled to make any further claim in respect of that Loss or Losses (including any claim for damages).

5.15.6 The liability of either Party (whether in Contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this Agreement, including the work, deliverables or Services covered by this Agreement, shall be the payment of direct damages only which shall in no event exceed 10% of the total Contract value payable under the Contract Agreement in between the Successful Bidder and the Buyer. The liability cap given under this Clause shall not be applicable to the indemnification obligations

5.15.7 In no event shall either party be liable for any consequential, incidental, indirect,

special or punitive damage, loss or expenses (including but not limited to business interruption, lost business, lost profits, or lost savings) nor for any third-party claims (other than those set-forth in Clause 5.15) even if it has been advised of their possible existence.

5.15.8 The allocations of liability represent the agreed and bargained for understanding of the parties and compensation for the Services/ deliverables reflects such allocations. Each Party has a duty to mitigate the damages and any amounts payable under an indemnity that would otherwise be recoverable from the other Party pursuant to this Agreement by taking appropriate and commercially reasonable actions to reduce or limit the amount of such damages or amounts.

5.16 MSI's Obligations

5.16.1 The MSI's obligations shall include provision of all the services and deliverables specified by the ITECCS in the Scope of Work and other sections of the RFP, Contract and changes thereof to enable the ITECCS to meet their objectives and operational requirements. It shall be the MSI's responsibility to ensure the proper and successful execution, performance and continued operation of the proposed services in accordance with and in strict adherence to the terms of their Bid, the RFP and Contract.

5.16.2 The MSI shall ensure that its resources are competent, professional and possess the requisite qualifications and experience appropriate to the task he/she is required to perform under this Contract.

5.16.3 The MSI shall be responsible for coordination with other vendors and agencies of the ITECCS in order to resolve issues and oversee smooth execution of this Contract.

5.16.4 The MSI shall maintain the list of project assets during the Contract. ITECCS reserves right to review the same at any point of time.

5.16.5 The MSI shall ensure that the only proposed OEMs shall supply components including associated accessories, software and shall support MSI during installation, integration and maintenance of these components during the Contract period. The warranty/ AMC of the system, products and services would commence from the day of UAT by ITECCS till Contract period.

5.16.6 Bidder to provide cloud infrastructure from any of the MIETY empanelled CSP (Cloud Service Provider).

5.16.7 All the product's licenses (subscription/ perpetual) that MSI procures should be in the name of ITECCS for Contract period.

5.16.8 The MSI shall ensure that none of the components and sub-components is declared end-of-sale or end-of-support by the respective OEM at the time of submission of bid. If the OEM declares any of the products/ solutions end-of-sale subsequently, MSI shall ensure that the same is supported by the respective OEM for Contract period.

5.16.9 MSI's Representative: The MSI's representative shall have all the powers requisite for the performance of services under the Contract. The MSI's Representative shall liaise with for the proper coordination and timely completion of the works and on any other matters pertaining to the works. He/she shall extend full co-operation to ITECCS in the manner required by them for supervision/ inspection/ observation of the procedures, performance, reports and records pertaining to the works. He shall also have complete charge of the Bidder's personnel engaged in the performance of the works and to ensure internal discipline, compliance of rules, regulations and

safety practice. The MSI's Project Manager is expected to act as single point of contact for any matter related to this project till completion of all the milestones. During the Operation and Maintenance phase, Project Manager is expected to attend all the performance review meetings and shall be single point of contact for the ITECCS for any matter related to contract or the services.

5.16.10 Reporting Progress

a. The MSI shall monitor progress of all the activities related to the execution of this Contract and shall submit report to the ITECCS, at no extra cost. These progress reports with reference to all related work and their progress to be submitted at the end of each month or before the expiry of the last day. If there is a delay in achieving milestones, the MSI shall notify the ITECCS in writing with in three (03) days for extended timelines. Post default of achieving milestone, penalty shall be applicable as per Section 6 of this RFP.
b. Periodic meetings shall be conducted on an ongoing basis between the representatives of the ITECCS and the MSI.
c. The ITECCS reserves the right to inspect and monitor/ assess the progress/ performance of the work/ services at any time during the Contract. The ITECCS may demand information related to project and the MSI shall provide documents, data, material or any other information which the ITECCS may require, to enable it to assess the progress/ performance of the Work/ Service.
d. At any time during the course of the Contract, the ITECCS shall also have the right to conduct an audit to monitor the performance by the MSI of its obligations/ functions in accordance with the standards committed to or required by the ITECCS, the said audit can be conducted either itself or through an independent audit firm appointed by the ITECCS as it may deem fit. The MSI undertakes to cooperate for audit and provide to the ITECCS/ any other firm appointed by the ITECCS, all documents and other details as may be required by them for this purpose.

5.16.11 Responsibilities of the MSI in respect of local laws, employment of works etc.

a. The MSI at all times during the continuance of this contract shall, in all his dealings with local labour for the time being employed on or in connection with the work, have due regard to all local festivals and religious and other customs.
b. The MSI shall comply with all applicable State and Central Laws, Statutory Rules, Regulations etc. such as Payment of Wages Act, Minimum Wages Act, and Workmen Compensation Act, Employer's Liability Act, Industrial Dispute Act, Employers Provident Act, Employees State Insurance Scheme, Contract Labour (Regulation and Abolition) Act 1970, Payment of Bonus & Gratuity Act and other Acts, Rules and Regulations for labour as may be enacted by the Government during the tenure of the Contract and having force or jurisdiction at the project Site. The MSI shall also give to the local Governing Body, Police and other relevant Authorities all such notices as may be required by the Law.
c. The MSI shall pay all taxes, fees, license charges, deposits, tolls, royalties, commission or other charges which may be liable on account of his operations in executing the contract.
d. The MSI shall be responsible for provision of Health and Sanitary arrangements (more particularly described in Contract Labour Regulation & Abolition Act),

Safety precautions etc. as may be required for safe and satisfactory execution of contract.

e. The MSI shall arrange, coordinate his work in such a manner as to cause no hindrance to other agencies working in the same premises.

5.17 Project Plan

5.17.1 The successful Bidder shall submit a detailed project plan within (15) working days from Issuance of LoI that is to be approved by ITECCS.

5.17.2 The project plan shall include details of the project showing the sequence, procedure and method in which MSI proposes to carry out the works.

5.17.3 The Plan so submitted by MSI shall conform to the requirements and timelines specified in the Contract.

5.17.4 The ITECCS and MSI shall discuss and agree upon the work procedures to be followed for an effective execution of the works, which MSI intends to deploy and shall be clearly specified.

5.17.5 The detailed project plan shall clearly specify the various project milestones and project deliverable schedules. It shall also include the following:

a. Project governance and management plan,
b. Communication structure,
c. Proposed staffing,
d. Roles and responsibilities,
e. Processes and tool set to be used for quality assurance,
f. Security and confidentiality practices in accordance with industry best practices,
g. Timelines for completion of activity,
h. Delivery schedule in accordance with the Contract,
i. Hardware and Software installation, commissioning and configuration plan at SDC, PHQ and other offices.
j. Migration Plan

5.17.6 Approval by the ITECCS of the Project Plan shall not relieve MSI of any of his duties or responsibilities under the Contract.

5.17.7 If MSI's work plans necessitates a disruption/ shutdown in ITECCS's operation, the plan shall be mutually discussed and developed so as to keep such disruption/ shutdown to the barest unavoidable minimum. The MSI shall be held responsible for any time and cost arising due to failure of MSI to develop/adhere such a work plan.

5.18 Buyer's obligations

5.18.1 The ITECCS or his/her nominated representative shall act as the nodal point for implementation of the contract and for issuing necessary instructions, approvals, commissioning, acceptance certificates, payments etc. to MSI.

5.18.2 The ITECCS shall ensure that timely approval is provided to MSI as and when required, which may include approval of project plans, implementation methodology, design documents, specifications, or any other document necessary in fulfilment of this contract.

5.18.3 The ITECCS representative shall interface with MSI, to provide the required information, clarifications, and to resolve any issues as may arise during the execution of the Contract. ITECCS shall provide adequate cooperation in providing

details, coordinating and obtaining of approvals from various governmental agencies, in cases, where the intervention of the ITECCS is proper and necessary.

5.18.4 The ITECCS Shall ensure the proper coordination between the selected MSI for NexGen UP112 and existing TSP for smooth project transition by assigning an officer as a single point of contact (SPOC).

5.18.5 The ITECCS may provide on MSI's request, particulars/ information/ or documentation that may be required by MSI for proper planning and execution of work and for providing services covered under this contract and for which MSI may have to coordinate with respective vendors.

5.18.6 The ITECCS shall provide to MSI only sitting space and basic infrastructure not including, stationery and other consumables at the NexGen UP112 Office Locations.

5.18.7 The ITECCS reserves the right to procure the hardware including devices on the basis End of Life/End of Service of the items to be replaced and AMC will be applicable whenever the devices are procured and deployed till end of the contract without any additional cost.

5.18.8 The ITECCS hereby agrees to provide access to the project sites within the agreed timelines. ITECCS agrees that the MSI shall not be in any manner liable for any delay arising out of ITECCS failure to provide access of the sites.

5.19 Confidentiality

5.19.1 The MSI shall not, either during the term or after expiration of this Contract, disclose any proprietary or confidential information relating to the Services or Contract and/or ITECCS business/ operations, information, Application/software, hardware, business data, architecture schematics, designs, storage media and other information or documents without the prior written consent of the ITECCS.

5.19.2 The MSI shall execute a Non-Disclosure Agreement (NDA) as given in Proformas; Section 9 of this RFP, in favour of the ITECCS

5.19.3 The ITECCS reserves the right to adopt legal proceedings, civil or criminal, against the MSI in relation to a dispute arising out of breach of obligation by the MSI under this clause.

5.19.4 The MSI shall do everything reasonably possible to preserve the confidentiality of the Confidential Information including execution of a confidentiality agreement with the ITECCS to the satisfaction of the ITECCS.

5.19.5 The MSI shall notify the ITECCS promptly if it is aware of any disclosure of the Confidential Information otherwise than as permitted by the Contract or with the authority of the ITECCS.

5.19.6 The MSI shall be liable to fully recompense the ITECCS for any loss of revenue arising from breach of confidentiality.

5.19.7 For the avoidance of doubt, it is expressly clarified that the aforesaid provisions shall not apply to the following information:

a. information already available in the public domain.
b. information which has been developed independently by the Implementation MSI
c. information which has been received from a third party who had the right to disclose
d. aforesaid information.

5.19.8 Information which has been disclosed to the public pursuant to a court order

5.20 Intellectual Property Rights

5.20.1 Retention of Ownership except for the rights expressly granted to the Licensee under this Agreement, the Licensor will retain all right, title and interest in and to the Licensed Technology, including all worldwide Technology and intellectual property and proprietary rights.

5.20.2 Preservation of Notice Licensee shall not remove, efface or obscure any copyright notices or other proprietary notices or legends from any Licensed Technology or materials provided under this Agreement, and shall reproduce all such notices and legends when incorporating Licensed Technology or materials into any Integrated Products.

5.20.3 The MSI must ensure that while using any software, hardware, processes, document or material in the course of performing the Services, it does not infringe the Intellectual Property Rights of any person or Company. The MSI shall keep the ITECCS indemnified against all costs, expenses and liabilities howsoever, arising out any illegal or unauthorized use (piracy) or in connection with any claim or proceedings relating to any breach or violation of any permission/license terms or infringement of any Intellectual Property Rights by the MSI or the MSI's Team during the course of performance of the Services. The MSI's liability is excluded regarding any claim based on any of the following (a) anything MSI provides which is incorporated into the Solution; (b) the ITECCS modification of the solution; (c) the combination, operation, or use of the solution with other materials, if the third-party claim has been caused by the combination, operation or use of the solution

5.20.4 ITECCS shall own and have a right in perpetuity to use all newly created Intellectual Property Rights which have been developed solely during execution of this Contract, including but not limited to all processes, products, specifications, software, customization in software, reports and other documents which have been newly created and developed by the MSI solely during the performance of Services and for the purposes of inter-alia use or sub-license of such Services under this Contract. The MSI shall also ensure to submit the source code of the developed product to the department as and when required. The MSI undertakes to disclose all such Intellectual Property Rights arising in performance of the Services to the ITECCS, execute all such agreements or documents and obtain all permits and approvals that may be necessary in regard to the Intellectual Property Rights of the ITECCS.

5.20.5 If ITECCS desires, the MSI shall be obliged to ensure that all approvals, registrations, licenses, permits and rights etc. which are inter-alia necessary for use of the goods supplied / installed by the MSI, the same shall be acquired in the name of the ITECCS, prior to termination of this Contract and which may be assigned by the ITECCS to the Prime Bidder for the purpose of execution of any of its obligations under the terms of the Bid, Tender or this Contract. However, subsequent to the term of this Contract, such approvals, registrations, licenses, permits and rights etc. shall endure to the exclusive benefit of the ITECCS.

5.20.6 The MSI shall not copy, reproduce, translate, adapt, vary, modify, disassemble, decompile or reverse engineer or otherwise deal with or cause to reduce the value of the Materials except as expressly authorized by ITECCS in writing

5.21 Compliance with Statutory and Regulatory Provisions

5.21.1 It shall be the sole responsibility of the bidder to MSI with all statutory and regulatory provisions while delivering the services mentioned in this RFP, during the course of the contract. Also, the MSI needs to ensure compliance of the project with

Government of India IT security guidelines including provisions of:

a. The Information Technology Act, 2000 and amendments thereof and
b. Guidelines /Advisories/ Orders / Notifications published by CERT-IN/MeitY/DPIIT /DOT (Government of India) and Government of Uttar Pradesh issued till the date of publishing of tender notice. Periodic changes in these Guidelines /Advisories/ Orders / Notifications during project duration need to be complied with.
c. With Reference to the Department for Promotion of Industry and Internal Trade (DPIIT) Order 2017 on 15th June 2017, which has recently been amended vide DPIIT order No. P-45021/2/2017-PP(BE-II) Dated 4 Jun 2020 and MeitY revised PPP-MII Order dated 04.06.2020 & order issued by Department of Expenditure Public Procurement Division, Ministry of Finance following two points to be considered for this RFP
d. Non-compliance to GB/T 2818 protocol Terms and Conditions for Make in India
    i. The MSI has to submit a certificate from OEM regarding the percentage of the Local Content and the details of Locations at which the local value addition is made.
    ii. In case value of such product is more than 10 crores, the declaration relating to percentage of local content shall be certified by the statutory auditor or cost auditor, if the OEM is a company and by a practicing cost accountant or a charted accountant for OEM's more than companies as per the public procurement (preference to Make in India) order 2017 dated 04-06-2020.
    iii. The MSI has to submit the bills/ E-way bills/ purchase details from OEM of local components along with the technical bid.

5.22 Taxes and duties

5.22.1 The MSI shall bear all personnel taxes levied or imposed on its personnel, or any other member of the MSI's Team, etc. on account of payment received under this Contract. The MSI shall bear all corporate taxes, levied or imposed on the MSI on account of payments received by it from the ITECCS for the work done under this Contract.

5.22.2 The successful bidder shall bear all applicable taxes and duties of the states and the union and international. It shall be the responsibility of the MSI to submit to the concerned Indian authorities the returns and all other connected documents required for this purpose. The MSI shall also provide the Buyer such information, as it may be required regarding the MSI's details of payment made by the Buyer under the Contract for proper assessment of taxes and duties. The amount of tax withheld by the Purchaser shall always be in accordance with Indian Tax Law and the Purchaser shall promptly furnish to the MSI original certificates for tax deduction at source and paid to the Tax Authorities.

5.22.3 Any increase or decrease in the rates of the applicable taxes or any new levy because of changes in law shall be adjusted such that payment to be made by the Buyer is increased / decreased accordingly and corresponding adjustments shall be made. In case of any new or fresh tax or levy imposed after submission. The MSI shall be entitled to reimbursement on submission of proof of payment of such tax or levy.

5.22.4 The MSI agrees that he and his team shall comply with the Indian Income Tax act

in force from time to time and pay Indian Income Tax, as may be imposed / levied on them by the Indian Income Tax Authorities, for the payments received by them for the works under the Contract. Should the MSI fail to submit returns/pay taxes in times as stipulated under applicable Indian/State Tax Laws and consequently any interest or penalty is imposed by the concerned authority, the MSI shall pay the same. The MSI shall indemnify Buyer against all liabilities or claims arising out of this Contract for such taxes including interest and penalty by any such Tax Authority may assess or levy against the Buyer/MSI.

5.22.5 The Buyer shall if so, required by applicable laws in force, at the time of payment, deduct income tax payable by the MSI at the rates in force, from the amount due to the MSI and pay to the concerned tax authority directly.

5.23 Termination

5.23.1 The Buyer may, terminate this Contract in whole or in part by giving the MSI a prior and written notice indicating its intention to terminate the Contract under the following circumstances:

a. Termination for Default:

i. If the MSI fails to deliver any or all of the services within the Project term specified in the Clause 5.10, or within any extension thereof granted by the Buyer pursuant or

ii. If the MSI fails to provide services to the Buyer to the satisfaction level

iii. If the MSI fails to perform any other obligation(s) under the Contract.

iv. If the MSI, in the judgment of the Buyer has engaged in corrupt or fraudulent practices in competing for or in executing the Contract.

b. Where it comes to the Buyer's notice that the MSI is in a position of actual conflict of interest with the interests of the Buyer, in relation to any of terms of the Bidder's Bid, the RFP or this Contract.

5.23.2 Termination for Insolvency: The Buyer may at any time terminate the Contract by giving written notice to the MSI, without compensation to the MSI, if the MSI becomes bankrupt or otherwise insolvent, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the Buyer.

5.23.3 Termination for Convenience: The Buyer, may, by prior written notice sent to the MSI at least 3 months in advance, terminate the Contract, in whole or in part at any time for its convenience. The notice of termination shall specify that termination is for the Buyer's convenience, the extent to which performance of work under the Contract is terminated, and the date upon which such termination becomes effective. In case of termination, Buyer shall pay for accepted services completed up to the date of termination.

5.23.4 Consequence of Termination

a. In the event of termination due to any cause whatsoever, the Buyer shall be entitled to impose any such obligations and conditions and issue clarifications as may be necessary to ensure an efficient transition and effective business continuity of the project. The MSI shall be obliged to comply with such

obligations/conditions and take all necessary steps to minimize loss resulting from that termination or breach. Further, MSI shall allow and provide all such assistance to the Buyer, as may be required, to take over the obligations in relation to the execution or continued execution of the Project.

b. Nothing herein shall restrict the right of the Buyer to invoke the Bank Guarantee and other Guarantees furnished hereunder and pursue such other rights and/or remedies that may be available to the Buyer under law.

5.23.5 The termination hereof shall not affect any accrued right or liability of MSI nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come into or continue in force on or after such termination.

5.24 Disputes and arbitration

5.24.1 If during the subsistence of this Contract or thereafter, any dispute between the Parties hereto arising out of or in connection with the validity, interpretation, implementation, material breach or any alleged material breach of any provision of this Contract or regarding any question, including as to whether the termination of this Contract by one Party hereto has been legitimate, the Parties hereto shall endeavour to settle such dispute amicably and/or by Conciliation to be governed by the Arbitration and Conciliation Act, 1996 or as may be agreed to between the Parties. The attempt to bring about an amicable settlement is considered to have failed as soon as one of the Parties hereto, after reasonable attempts, which attempt shall continue for not less than 21 (Twenty-One) days, gives 30 (thirty) day notice to refer the dispute to arbitration to the other Party in writing.

5.24.2 The Arbitration proceedings shall be governed by the Arbitration and Conciliation Act, 1996.

5.24.3 The Arbitration proceedings shall be held in Lucknow, Uttar Pradesh, India.

5.24.4 The Arbitration proceeding shall be governed by the substantive laws of India.

5.24.5 The proceedings of Arbitration shall be in Hindi/ English language.

5.24.6 Except as otherwise provided elsewhere in the Contract if any dispute, difference, question or disagreement arises between the parties hereto or their respective representatives or assignees, at any time in connection with construction, meaning, operation, effect, interpretation or out of the Contract or breach thereof the same shall be referred to a Tribunal of three (3) Arbitrators, constituted as per the terms of and under the (Indian) Arbitration and Conciliation Act, 1996. Each party to the Contract shall appoint or nominate one Arbitrator each, the two Arbitrators so appointed/ nominated by the Parties herein shall together choose the third Arbitrator, who will be the Presiding Arbitrator of the Tribunal. The consortium of the three Arbitrators shall form the Arbitral Tribunal.

5.24.7 Both the Parties will make attempts to appoint arbitrators with background of Information Technology related activities, Information Technology related acts, understanding of the processes and activities of police organizations and an understanding of the software applications.

5.24.8 In case, a party fails to appoint an arbitrator within 30 days from the receipt of the request to do so by the other party or the two Arbitrators so appointed fail to agree on the appointment of third Arbitrator within 30 days from the date of their appointment upon request of a party, the Justice of the Allahabad High Court, Lucknow Bench or any person or institution designated by him shall appoint the Arbitrator or Presiding Arbitrator upon request of one of the parties.

5.24.9 Any letter, notice or other communications dispatched to the MSI relating to either

arbitration proceeding or otherwise whether through the post or through a representative on the address last notified to the ITECCS by the MSI shall be deemed to have been received by the MSI although returned with the remarks, refused 'undelivered' where about not known or words to that effect or for any other reasons whatsoever

5.24.10 If the Arbitrator so appointed dies, resigns, incapacitated or withdraws for any reason from the proceedings, it shall be lawful for the MSI to appoint another person in his place in the same manner as aforesaid. Such person shall proceed with the reference from the stage where his predecessor had left if both parties consent for the same, otherwise, he shall proceed de novo.

5.24.11 It is a term of the Contract that the party invoking arbitration shall specify all disputes to be referred to arbitration at the time of invocation of arbitration and not thereafter

5.24.12 It is also a term of the Contract that neither party to the Contract shall be entitled for any interest on the amount of the award

5.24.13 The Arbitrator shall give reasoned award and the same shall be final, conclusive and binding on the parties

5.24.14 The fees of the arbitrator, costs and other expenses incidental to the arbitration proceedings shall be borne equally by the parties

5.24.15 Each Party shall bear the cost of preparing and presenting its case, and the cost of arbitration, including fees and expenses of the arbitrators, shall be shared equally by the Parties unless the award otherwise provides

5.25 Exit Management Plan

5.25.1 An Exit Management plan shall be furnished by the MSI in writing to the ITECCS within 90 days from the date of Award of Notification, which shall deal with at least the following aspects of exit management in relation to the contract as a whole and Service Level monitoring.

i. A detailed program of the transfer process that could be used in conjunction with a Replacement Service Provider including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer.

ii. Plans for provision of contingent support to Project and Replacement Service Provider for a reasonable period after transfer.

iii. Exit Management plan in case of normal termination of Contract period

iv. Exit Management plan in case of any eventuality due to which Project is terminated before the contract period.

v. Exit Management plan in case of termination of the Bidder

5.25.2 Exit Management plan will cover the scope as defined in Clauses 4.5.1 (b) and (d) of Section 4 of this RFP.

5.25.3 In the event of termination or expiry of the contract, Pilot site Implementation, or Service Level monitoring, both MSI and ITECCS shall comply with the Exit Management Plan.

5.25.4 During the exit management period, the MSI shall use its best efforts to deliver the services.

5.26 Time is of the essence

5.26.1 Time shall be of the essence in respect of any date or period specified in this Contract or any notice, demand or other communication served under or pursuant to any provision of this Contract and in particular in respect of the completion of the activities by the MSI by the specified completion date.

5.27 Notices

5.27.1 Any notice, request or consent required or permitted to be given or made pursuant to this contract shall be in writing. Any such notice, request or consent shall be deemed to have been given or made when delivered in person to an authorized representative of the party to whom the communication is addressed, or when sent to such party at the address mentioned in the project specific Work Order/Contract Agreement.

5.28 Conflict of interest

5.28.1 The MSI shall not have a conflict of interest that may affect the Selection Process or the service delivery (the "Conflict of Interest"). Any Bidder found to have a Conflict of Interest shall be disqualified. In the event of disqualification, the Buyer shall forfeit and appropriate the EMD and/or PBG, if available, as mutually agreed genuine pre-estimated compensation and damages payable to the Buyer for, inter alia, the time, cost and effort of the Buyer including consideration of such Bidder's Proposal, without prejudice to any other right or remedy that may be available to the Buyer hereunder or otherwise.

5.28.2 The Buyer requires that the MSI provides services which always hold the Buyer's interest's paramount, avoid conflicts with other assignments or its own interests, and act without any consideration for future work. The selected Bidder shall not accept or engage in any assignment that would conflict with its prior or current obligations to other clients, or that may place it in a position of not being able to carry out the assignment in the best interests of the Buyer.

The MSI shall disclose to the Buyer in writing, all actual and potential conflicts of interest that exist, arise or may arise (for the selected Bidder) in the course of performing the Services as soon as practical after it becomes aware of that conflict.

5.29 Trademarks, Publicity

5.29.1 Neither Party may use the trademarks of the other Party without the prior written consent of the other Party except that the MSI may, upon completion, use the Project as a reference for credential purpose. Except as required by law or the rules and regulations of each stock exchange upon which the securities of one of the Parties is listed, neither Party shall publish or permit to be published either alone or in conjunction with any other person any press release, information, article, photograph, illustration or any other material of whatever kind relating to this Agreement, the SLA or the business of the Parties without prior reference to and approval in writing from the other Party, such approval not to be unreasonably withheld or delayed provided however that the MSI may include ITECCS for reference to third parties subject to the prior written consent of the ITECCS not to be unreasonably withheld or delayed. Such approval shall apply to each specific case and relate only to that case

5.30 Governing law

5.30.1 This Contract shall be governed in accordance with the laws of India or GoUP.

5.31 Force majeure

5.31.1 Force Majeure shall not include any events caused due to acts or omissions of MSI resulting in a breach or contravention of any of the terms of the Contract and/or the MSI 's Bid. It shall also not include any default on the part of MSI due to its negligence or failure to implement the stipulated or proposed precautions, as were required to be taken under the Contract.

5.31.2 The failure or occurrence of a delay in performance of any of the obligations of either party shall constitute a Force Majeure event only where such failure or delay could not have reasonably been foreseen i.e. war, or hostility, acts of the public enemy, civil commotion, sabotage, fire, floods, explosions, epidemics, pandemics quarantine restriction, strikes, lockouts or act of God (such as lighting, earthquake, landslide, etc. or other events of natural disaster of rare severity), or where despite the presence of adequate and stipulated safeguards the failure to perform obligations has occurred at any location in scope. In such an event, the affected party shall inform the other party in writing within 21 (twenty-one) days of the occurrence of such event. Any failure or lapse on the part of MSI in performing any obligation as is necessary and proper, to negate the damage due to projected force majeure events or to mitigate the damage that may be caused due to the above-mentioned events or the failure to provide adequate disaster management or recovery or any failure in setting up a contingency mechanism would not constitute force majeure, as set out above. In case of a Force Majeure, all Parties will endeavour to agree on an alternate mode of performance to ensure the continuity of service and implementation of the obligations of a party under the Contract and to minimize any adverse consequences of Force Majeure.

5.31.3 No delay or non-performance by either party to this Contract caused by the occurrence of any event of Force Majeure shall:

a. constitute a default or breach of the Contract.

b. give rise to any claim for damages or additional cost or expense occasioned by the delay or
non-performance, if, and to the extent that, such delay or non-performance is caused by the occurrence of an event of Force Majeure.

c. If the performance of the Contract is substantially prevented, hindered, or delayed for a single period of more than 60 (sixty) days on account of one or more events of Force Majeure during the time period covered by the Contract, the parties will attempt to develop a mutually satisfactory solution, failing which, either party may terminate the Contract by giving a notice to the other.

5.32 Variation in Field Locations

5.32.1 The field locations as defined in Annexure – 27 of Section 9 of this RFP, may increase or shift to other locations during contract period. The MSI will be informed well in advance in case of any new site added or shifted to other location.

5.33 Risk Purchase

5.33.1 If the MSI fails to deliver any component or application or service either in full or in part, within the prescribed delivery period or defined service level as defined in Scope of Work and SLAs, the ITECCS shall be entitled to ask MSI to change the OEM (post approval of buyer) of the respective product or application or service at the risk & cost of the MSI without cancelling the contract, to procure the component

or application or service at the risk and cost of the MSI. The price differential in case of higher cost to MSI, if any, shall have to be borne by the defaulting MSI.

5.33.2 It is the discretion of ITECCS either to levy penalty clause and accept delayed deliveries or proceed with the change of OEM invoking the risk purchase clause.

5.34 Information Security

5.34.1 The MSI shall not carry any written or printed document, layout diagrams, CD, hard disk, storage tapes, other storage devices or any other goods /material proprietary to ITECCS into or out of any location without written permission from the ITECCS.

5.34.2 The MSI shall not destroy any unwanted documents, defective tapes/media present at any location on their own. All such documents, tapes or media shall be handed over to the ITECCS.

5.34.3 All documentation and media at any location shall be properly identified, labelled and numbered by the MSI. The MSI shall keep track of all such items and provide a summary report of these items to the ITECCS whenever asked for.

5.34.4 Access to ITECCS data and systems, Email and Internet facility by the MSI at any location shall be in accordance with the written permission by the ITECCS. The ITECCS will allow the MSI to use facility in a limited manner subject to availability. It is the responsibility of the MSI to prepare and equip himself in order to meet the requirements.

5.34.5 The MSI must acknowledge that ITECCS business data and other ITECCS proprietary information or materials, whether developed by ITECCS or being used by ITECCS pursuant to a license agreement with a third party (the foregoing collectively referred to herein as “proprietary information”) are confidential and proprietary to ITECCS; and the MSI along with its team agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by the MSI to protect its own proprietary information. The MSI recognizes that the goodwill of ITECCS depends, among other things, upon the MSI keeping such proprietary information confidential and that unauthorized disclosure of the same by the MSI or its team could damage the goodwill of ITECCS, and that by reason of the MSI’s duties hereunder. The MSI may come into possession of such proprietary information, even though the MSI does not take any direct part in or furnish the services performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the services required by this agreement. The MSI shall use such information only for the purpose of performing the said services.

5.34.6 The MSI shall, upon termination of this agreement for any reason, or upon demand by ITECCS, whichever is earliest, return any and all information provided to the MSI by ITECCS, including any copies or reproductions, both hardcopy and electronic.

5.34.7 By virtue of the Contract, the MSI team may have access to personal information of the ITECCS and/or a third party. The ITECCS has the sole ownership of and the right to use, all such data in perpetuity including any data or other information pertaining to the citizens that may be in the possession of the MSI team in the course of performing the Services under the Contract

5.35 Change control

5.35.1 Change requests in respect of the Contract agreement, implementation and operation of this project, the SLA or Scope of work will emanate from Project

Manager deployed by the MSI who will be responsible for obtaining approval for the change and who will act as its single point of contact (SPOC) throughout the Change Control Process and will complete PART A of the CCN attached as Annexure 20 of Section 9 of this RFP. CCNs will be presented to the ITECCS or his nominated representative who will acknowledge receipt by signature of the CCN.

5.35.2 The MSI and the ITECCS, during the Project Implementation and Operations and Management Phase while preparing the CCN, shall consider the change in the context of the following parameter, namely whether the change is beyond the scope of Services required and as detailed in the RFP and is suggested and applicable only after the testing, commissioning and certification of the Project Implementation Phase as set out in this Agreement.

5.35.3 It is hereby also clarified that any change of control suggested beyond 20% of the Contract value of this Project will be beyond the scope of the change control process and will be considered as the subject matter for a separate bid process and a separate Contract. It is hereby clarified that the 20% of the Contract value of the Project as stated herein above is calculated based on Contract value submitted by the MSI and accepted by the ITECCS. For arriving at the cost / rate for change up to 20% of the Contract value, the payment terms and relevant rates as specified in Section 7 of this RFP shall apply.

5.35.4 Change requests in respect of the Contract, project implementation, or Service levels will emanate from the Party's representative who will be responsible for obtaining approval for the change and who will act as its representative throughout the Change Control Process and will complete Part A of the CCN (Annexure 13.6). CCNs will be presented to the other Party's representative who will acknowledge receipt by signature of the authorized representative of the ITECCS.

5.35.5 The MSI and the ITECCS while preparing the CCN, shall consider the change in the context of whether the change is beyond the scope of Services including ancillary and concomitant services required

5.35.6 The CCN shall be applicable for the items which are beyond the stated/implied scope of work as per the RFP document.

5.35.7 CCN Quotation: The MSI shall assess the CCN and complete Part B of the CCN. In completing Part B of the CCN the MSI shall provide as a minimum:

a. a description of the change.
b. a list of deliverables required for implementing the change.
c. a timetable for implementation.
d. an estimate of any proposed change.
e. any relevant acceptance criteria.
f. an assessment of the value of the proposed change.
g. Material evidence to prove that the proposed change is not already covered within the scope of the project, Agreement and Service Levels.

5.35.8 Prior to submission of the completed CCN to the ITECCS or its nominated agencies, the MSI will undertake its own internal review of the proposal and obtain all necessary internal approvals. As a part of this internal review process, the MSI shall consider the materiality of the proposed change in the context of the Agreement, the Project Implementation, Service levels affected by the change and the total effect that may arise from implementation of the change.

5.35.9 In the event the MSI is unable to meet the obligations as defined in the CCN then the cost of getting it done by third party will be borne by the MSI. Change requests

and CCNs will be reported monthly to each Party's representative who will prioritize and review progress.

5.36 Tripartite Agreement

5.36.1 As per TRAI guidelines, resale of bandwidth connectivity is not allowed. Hence, the execution of the Network Services will be covered by tripartite agreement among GoUP, MSI and TSP as prescribed in Annexure 24 of Section 9.

6 SERVICE LEVEL AGREEMENT

6.1 Definitions

For purposes of the SLA, the definitions and terms as specified in the document along with the following terms shall have the meanings set forth below:

a. "**Agreed Total number of man-days**" would be as per the working days as defined in clause 4.28.7.
b. "**AMC Charges**" is the total amount to be paid for AMC to MSI for the operation and maintenance of NexGen UP112.
c. "**Availability**" means availability of the services of that component or application to NexGen UP112.
d. "**Average Speed to Answer**" is an average amount of time to respond to the call. This includes the amount of time caller waits in a waiting queue.
e. "**Average Handle Time**" – refers to the time taken to manage a call. AHT shall be calculated as the sum of average talk time, hold time and submitted for auto dispatch.
f. "**Critical Software**" – Critical Application means an application whose functionality is critical for the continued operation or the quality of the services of UP112. List of those components are listed in clause 4.27.7.
g. "**Critical Hardware**" – Critical Component means a component whose functionality is critical for the continued operation or the quality of the services of UP112. List of those components are listed in clause 4.27.8.
h. **"Downtime"** – Time period for which the specified services/ components/ outcomes are not available in the concerned period which would exclude downtime owing to Force Majeure, scheduled maintenance time (approved by ITECCS) and reasons beyond control of the MSI.
i. **"Incident"** – Any event/ abnormalities in the service being rendered, that may lead to disruption in normal operations and services to the end user.
j. **"Intranet users"** – All the internal user authorised by UP112 such as officers of UP112, CO, ES, RMO, field officers, etc.
k. **"Key personnel" or "Key resources"** means all the Technical manpower to be deployed by MSI as per the requirement mentioned in clause 4.28.
l. "**Non-Critical Software**" – Non-Critical Applications are those excluding critical applications. List of those components are listed in clause 4.27.7.
m. "**Non-Critical Hardware**" – Critical Components are those excluding critical components. List of those components are listed in clause 4.27.7.

n. **“Resolution Time”** - means time taken by the Helpdesk to close the Service Request for any incident in resolving (diagnosing, troubleshooting and fixing) or escalating to the second level to respective Vendors, getting the confirmatory details about the same.

o. **“Scheduled Maintenance Time”** – Time period for which the specified services/ Application is not available due to scheduled maintenance activity pre-approved by ITECCS.

p. **“Service Request” -** Request from a user for reporting incident or to seek support, delivery, information, advice or documentation.

q. **“Total Time”** – Total number of hours in the quarter (or the concerned period) being considered for evaluation of SLA performance.

r. **"Uptime"** – Time period for which the specified services/ outcomes are available in the period being considered for evaluation of SLA. Formulae for calculation of Uptime:

$$Uptime\ (\%) = \{1 - \frac{Downtime}{Total\ time - scheduled\ maintenance\ time}\} \times 100\%$$

6.2 Purpose of this agreement

6.2.1 The prime objective of service levels is to ensure quality of services from the MSI, in an efficient manner as defined in RFP. To meet this objective, the MSI will provide the Service Levels in accordance with the performance levels as set out in detail in this Section i.e., Service Level Agreement

6.2.2 The service level targets define the levels of service to be provided by the MSI to ITECCS for the duration of this contract or until the stated SLA targets are amended.

6.3 General Principles of SLA

6.3.1 This Agreement shall govern the provision of the Contracted professional services of the MSI to the ITECCS after the Effective Date.

6.3.2 Penalties in case of not meeting defined service levels are not meant to be punitive or, conversely, a vehicle for additional fees.

6.3.3 The MSI shall comply of service level requirements for availability and quality of services, throughout the period of the Contract or extensions, if any, as defined in section 6 of this RFP. The MSI shall monitor and maintain the stated service levels to ensure adherence to quality service to the ITECCS. The SLA is applicable to only those applications, which are duly accepted by the ITECCS.

6.3.4 24x7 shall mean hours between 12:00 AM -11.59 PM midnight on all days of the week.

6.3.5 The MSI needs to perform periodic maintenance on hosting environment for the purposes of system upgrades, maintenance, and backup procedures. The maintenance can be done only on Scheduled Maintenance Time with at least 3 days prior approval from ITECCS. The scheduled downtime for these non-critical components/applications owing to any kind of maintenance should be carried out during non-peak hours i.e., 12:00 A.M. to 04:00 A.M. (all such times being Indian Standard Time); and not exceed four (4) hours in any month. However, no downtime

will be allowed for the critical components/application. For those services, the MSI needs to devise a mechanism for the uninterrupted services even in case of any maintenance and updates through DR sites.

6.3.6 The purpose of imposing penalty on account of SLA is to ensure the performance of the services as per defined parameters. In view of this, if the performance of the services is not improved, it shall constitute enough grounds for the annulment of the Contract. Hence, if the cumulative penalty excluding Liquidated damages, in a year, is more than 2% of Contract value, the ITECCS reserves the right to initiate termination process.

6.4 Liquidated Damages

6.4.1 Time is the essence of the project and the delivery dates are binding on the MSI. In the event of delay or any gross negligence in implementation of the project for causes solely attributable to the MSI, in achieving the milestones, the ITECCS shall be entitled to recover from the MSI as liquidated damages. Delays that are not attributed to MSI shall not be considered for the penalty.

6.4.2 The liquidated damages subject to a maximum of 10% of the Contract Value.

6.4.3 If the cumulative liquidated damages go beyond 10% of the Contract value, the ITECCS reserves the right to take appropriate action including termination.

6.4.4 This right to claim any liquidated damages shall be without prejudice to other rights and remedies available to ITECCS under the Contract and law.

6.4.5 The applicable Liquidated damages will be recovered by deduction of the same value from first or any invoice of CAPEX as defined in payment term under clause 8.2 of this RFP or from any money belonging to the MSI in its hands (which includes the ITECCS right to claim such amount against the MSI's Performance Bank Guarantee) or which may become due to the MSI. Any such recovery or liquidated damages shall not in any way relieve the MSI from any of its obligations to complete the Work or from any other obligations and liabilities under the Contract.

6.4.6 Liquidated damages shall be calculated as below:

#	Activity	Target	Measurement Interval	Liquidated Damages
1.	Deployment of the resources	Deployment of the resources for implementation stage as defined in clause 4.28.1	Weekly after target date of completion of activity No penalty will be applicable on mid of the week	0.001% of the total contract value per resource for the delay of each week beyond the targeted timeline e.g., say total contract value: INR 500 cr. Applicable LD on delay of 3 weeks for any one resource: INR 1.5 lakh
2.	Replacement of the resources	No resource will be allowed to replace in Implementation stage as defined in clause 4.28.1	Weekly after target date of completion of activity	0.001% of the contract value for the instance of such replacement e.g., say total contract value: INR 500 cr.

#	Activity	Target	Measurement Interval	Liquidated Damages
		The exception may be given only in case of person leaving the organization or medical exigency on the sole discretion of the ITECCS		Applicable LD on two such instances: INR 10 lakh
3.	Submission of Project Plan	To be submitted as per timelines defined in clause 4.4 of Section 4 of this RFP	Weekly after target date of completion of activity	0.01% of the contract value for the delay of each week beyond the targeted timeline e.g., say total contract value: INR 500 cr. Applicable LD on delay of 2 weeks: INR 10 lakh
4.	Completion of Stage -1 Milestone: Transition and O&M of existing UP112 as defined under Clause 4.4 of Section 4 of this RFP	Submission of the compliance report on completion of the milestone as per defined timeline	Weekly after target date of completion of activity	0.01% of the contract value for the delay of each week beyond the targeted timeline e.g., say total contract value: INR 500 cr. Applicable LD on delay of 2 weeks: INR 10 lakh
5.	Completion of Stage – 2 Milestone: Design & Implementation of NexGen UP112 system as defined under Clause 4.4 of Section 4 of this RFP	System acceptance by ITECCS based on criteria defined in clause 4.18 of Section 4 of this RFP	Weekly after target date of completion of milestone	0.01% of the contract value for the delay of each week beyond the targeted timeline e.g., say total contract value: INR 500 cr. Applicable LD on delay of 2 weeks: INR 10 lakhs
6.	Timely submission of all the required documents except project plan	Submission of all the required documents as per schedule as defined in Clause 4.4 of Section 4 of this RFP	Weekly after target date of completion of milestone	0.001% of the contract value for the delay of each document for week beyond the targeted timeline e.g., say total contract value: INR 500 cr.

#	Activity	Target	Measurement Interval	Liquidated Damages
				Applicable LD on delay of 2 such documents for 2 weeks: INR 2 lakhs

Performance Service Levels

6.4.7 Availability of the Software at UP112

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
1	Availability of the following critical Software ▶ IP PBX ▶ Automatic Call Distribution (ACD) ▶ Voice Recording & Quality Monitoring ▶ Multimedia System ▶ Computer Telephony Interface (CTI) ▶ Outbound Dialler ▶ Contact Centre Reporting System ▶ Softphone ▶ Computer Aided Dispatch (CAD): ▶ Communication officer ▶ Auto Dispatch officer ▶ CAD Mobile Software for MDT ▶ Web and Desktop Application for Monitoring-Police officials ▶ Police station Module ▶ Mobile Application for Police officials ▶ Citizen Portal ▶ Enterprise Management System ▶ Directory services ▶ Backup software	Measured as availability of application Measurement tool: EMS report	Monthly	Baseline: >= 99.98% uptime of the Software	NIL
				Lower performance: <99.98% >= 90% uptime	(Baseline%-Achieved service level%)/20 x quarterly AMC charges
				Breach: <90%	(Baseline%-Achieved service level%)/10 x quarterly AMC charges e.g., say quarterly AMC value for the period when service is delivered: INR 2.5 cr. and Service Level: 89.98% Applicable penalty: (99.98%-89.98%)/10= 1% of quarterly AMC charges Applicable penalty on breach of

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
	▶ GIS Map ▶ SMS Gateway ▶ MDM-Mobility Device Management ▶ VTS-Vehicle tracking System- ▶ Location Based Services ▶ Emergency Location Services ▶ VMS for cameras ▶ Anti-APT ▶ Endpoint Detection & Response (EDR) ▶ Patch Management Solution ▶ Threat Intelligence Tools/Solutions (SOAR) ▶ DDoS ▶ Intrusion Prevention System (IPS) ▶ VAPT Tools/Solutions ▶ Endpoint Security				service level of that application for the month: INR 2.5 lakhs @ 1% of INR 2.5 Cr.
2	Availability of the following non-critical Software: ▶ Mobile application for GIS Data collection ▶ E-learning Software and Web learning ▶ Patrol Management system	Measured as availability of application Measurement tool: EMS report	Monthly	Baseline: >= 97% uptime of the Software	NIL
				Lower performance: <97% > = 90% uptime	(Baseline%-Achieved service level%)/40 x quarterly AMC charges
				Breach: <90% uptime	(Baseline%-Achieved service

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
	▶ Human resource management system (HRMS) ▶ Document management system ▶ Business Intelligence (BI), Reporting & Analytics ▶ Inventory Management ▶ Number masking ▶ Push to talk (PTT) Subscription per device for three years ▶ PTT Integration ▶ Chat Bot application and software ▶ Video Conferencing software ▶ Fleet management software				level%)/20 x quarterly AMC charges e.g., say quarterly AMC value for the period when service is delivered: INR 2.5 cr. and Service Level: 87.0% Applicable penalty: (97%-87%)/20= 0.5% of quarterly AMC charges Applicable penalty on breach of service level of that application for any month: INR 1.25 lakh @ 0.5% of INR 2.5 Cr.

6.4.8 Availability of the Hardware at DC

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
1		Measured as availability of	Monthly	Baseline: >= 99.98%	NIL

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
	Availability of the following critical Hardware ▶ SAN Storage ▶ VTL ▶ Database server ▶ Blade chassis ▶ Rack ▶ Blade Server-2 CPU ▶ Blade server-4 CPU ▶ Load Balancer ▶ UPS - 200KVA ▶ Core Switch ▶ Managed Access Switch ▶ SAN Switch ▶ Aggregation Switch ▶ Internet Router ▶ Core router ▶ Global Load Balancer ▶ Server for Vehicle Mounted Camera ▶ Web Application Firewall ▶ NextGen Firewall ▶ Security Incident & Event	components. Measurement tool: EMS report		uptime of the Hardware	
				Lower performance: <99.98% > = 90% uptime	(Baseline% - Achieved service level%)/20 x quarterly AMC charges
				Breach: <90% uptime	(Baseline% - Achieved service level%)/10 x quarterly AMC charges e.g., say quarterly AMC value for the period when service is delivered: INR 2.5 cr. and Service Level: 89.98% Applicable penalty: (99.98%-89.98%)/10= 1% of quarterly AMC charges Applicable penalty on breach of service level of that Hardware for the month: INR 2.5 lakhs @ 1% of INR 2.5 Cr.

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
	Management (SIEM) ▶ Data Leakage Prevention (DLP) ▶ Network Access Control (NAC) ▶ Storage for Vehicle Mounted Camera and Body Worn Camera				
2	Availability of the following non-critical Hardware: ▶ Biometric	Measured as availability of components Measurement tool: EMS report	Monthly	Baseline: >= 97% uptime of the Hardware	NIL
				Lower performance: <97% > = 90% uptime	(Baseline% - Achieved service level%)/40 x quarterly AMC charges
				Breach: <90% uptime	(Baseline% - Achieved service level%)/20 x quarterly AMC charges e.g., say quarterly AMC value for the period when service is delivered: INR 2.5 cr. and Service Level: 87.0% Applicable penalty: (97%-87%)/20= 0.5%

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
					of quarterly AMC charges Applicable penalty on breach of service level of that Hardware for the month: INR 1.25 lakh @ 0.5% of INR 2.5 Cr.
3	CPU Utilization for each server	Average CPU utilization of each server should not be more than 50%. Measurement tool: EMS report	Monthly	Baseline: = < 50% average utilization of the CPUs	NIL
				Lower performance: >50% < = 70% average utilization of the CPUs	(Achieved service level% - Baseline level%)/20 x quarterly AMC charges
				Breach: > 70% average utilization of the CPUs	(Achieved service level% - Baseline%)/10 x quarterly AMC charges e.g., say quarterly AMC value for the period when service is delivered: INR 2.5 cr. and Service Level: 90.0% Applicable penalty: (90% - 50%)/10 = 4% of quarterly AMC charges Applicable penalty on breach of service level for the

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
					month: INR 10 lakhs @ 4% of INR 2.5 Cr.

6.4.9 Availability of the Hardware at UP112

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
1	Availability of the following critical Hardware ▶ IP Phones ▶ Managed Access Switch-24 ports	Measured as availability of components. Measurement tool: EMS report	Monthly	Baseline: >= 99.98% uptime of the Hardware	NIL
				Lower performance: <99.98% > = 90% uptime	(Baseline% - Achieved service level%)/20 x quarterly AMC charges
				Breach: <90% uptime	(Baseline% - Achieved service level%)/10 x quarterly AMC charges e.g., say quarterly AMC value for the period when service is delivered: INR 2.5 cr. and Service Level: 89.98% Applicable penalty: (99.98%-89.98%)/10= 1% of quarterly AMC charges Applicable penalty on breach of service level of that Hardware for the month: INR 2.5 lakhs @ 1% of INR 2.5 Cr.

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
2	Availability of the following non-critical Hardware: ► Biometric ► Digital light processing (DLP) video wall ► Radio Gateway for RoIP Server ► VHF static radio device ► CCTV ► CCTTV Controller	Measured as availability of components. Measurement tool: EMS report	Monthly	Baseline: >= 97% uptime of the Hardware	NIL
				Lower performance: <97% > = 90% uptime	(Baseline% - Achieved service level%)/40 x quarterly AMC charges
				Breach: <90% uptime	(Baseline% - Achieved service level%)/20 x quarterly AMC charges e.g., say quarterly AMC value for the period when service is delivered: INR 2.5 cr. and Service Level: 87.0% Applicable penalty: (97%-87%)/20= 0.5% of quarterly AMC charges Applicable penalty on breach of service level of that Hardware for the month: INR 1.25 lakh @ 0.5% of INR 2.5 Cr.

6.4.10 Availability of the Hardware at OMCs

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
1		Measured as availability of	Monthly	Baseline: >= 99.98% uptime	NIL

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
	Availability of the following critical Hardware ▶ IP Phones ▶ Managed Access Switch 24 ports ▶ Router ▶ UPS 20 kVA	components. Measurement tool: EMS report		of the Hardware	
				Lower performance: <99.98% > = 90% uptime	(Baseline% - Achieved service level%)/20 x quarterly AMC charges
				Breach: <90% uptime	(Baseline% - Achieved service level%)/10 x quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 Cr. and Service Level: 89.98% Applicable penalty: (99.98%-89.98%)/10= 1% of quarterly AMC charges Applicable penalty on breach of service level of that Hardware for the month: INR 2.5 lakhs @ 1% of INR 2.5 Cr.
2	Availability of the following non-critical Hardware: ▶ Biometric	Measured as availability of components. Measurement	Monthly	Baseline: >= 97% uptime of the Hardware	NIL
				Lower performance:	(Baseline% - Achieved

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
	▶ VHF static radio device ▶ Radio Gateway	tool: EMS report		<97% > = 90% uptime	service level%)/40 x quarterly AMC charges
				Breach: <90% uptime	(Baseline% - Achieved service level%)/20 x quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 cr. and Service Level: 87.0% Applicable penalty: (97%-87%)/20 = 0.5% of quarterly AMC charges Applicable penalty on breach of service level of that Hardware for the month: INR 1.25 lakh @ 0.5% of INR 2.5 Cr.

6.4.11 Availability of the services between DC and DR

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
1	Availability of the Replication System between DC & DR	Measured as availability of components. Measurement	Monthly	Baseline: >= 99.5% uptime of the Services	NIL

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
		tool: EMS report		Lower performance: <99.5% > = 90% uptime	(Baseline% - Achieved service level%)/20 x quarterly AMC charges
				Breach: <90% uptime	(Baseline% - Achieved service level%)/10 x quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 cr. and Service Level: 89.5% Applicable penalty: (99.5%-89.5%)/10= 1% of quarterly AMC charges Applicable penalty on breach of service level for the month: INR 2.5 lakhs @ 1% of INR 2.5 Cr.
2	DR Drill	MSI shall adhere to the DR Policy of ITECCS and conduct DR Drills accordingly	Half yearly	Baseline: 100% of the time the drill should happen as per schedule and as per request of ITECCS.	NIL

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
				Breach: Any violation of the DR policy.	2% of quarterly AMC charges e.g. say total AMC value for the entire project: INR 50 cr. Applicable penalty on breach of service level for any two violations in half year period: INR 20 lakhs@ 2% of 5 Cr. (Half yearly value)
3	1. Achievement of RTO and RPO as defined in clause 4.27.2 (e) of section 4 this RFP 2. Auto switch of applications from DC to DRC or vice versa	MSI shall ensure that RTO and RPO to be achieved as per targeted duration in case of any incident Measurement tool: Report from EMS	Monthly	Baseline: 100% compliance as per defined target	NIL
				Breach: any instance of non compliance of the defined target	2% of quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 cr. Applicable penalty on breach of such two cases in any month: INR 10 lakhs @ 2% of INR 2.5 Cr.

6.4.12 Availability of the Hardware at Field Location

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
1	Availability of the following critical Hardware ► UPS 1 KVA ► UPS 2KVA ► IP Phone ► VHF static radio device ► VHF Handheld radio device ► Managed Access Switch 24 Ports ► Router	Measured as per availability of Hardware. Measurement tool: EMS report	Monthly	Baseline: >= 99.00% uptime of the Hardware	NIL
				Lower performance: <99.00% > = 90% uptime	(Baseline% - Achieved service level%)/20 x quarterly AMC charges
				Breach: <90% uptime	(Baseline% - Achieved service level%)/10 x quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 cr. and Service Level: 89.00% Applicable penalty: (99.00%-89.00%)/10= 1% of quarterly AMC charges Applicable penalty on breach of service level of that Hardware for the month: INR 2.5 lakhs @ 1% of INR 2.5 Cr.
2	Availability of the following non-critical Hardware:	Measured as per availability of Hardware.	Monthly	Baseline: >= 97% uptime of the Hardware	NIL

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
	▶ Biometric ▶ VHF static radio device ▶ Radio Gateway	Measurement tool: EMS report		Lower performance: <97.00% > = 90% uptime	(Baseline% - Achieved service level%)/40 x quarterly AMC charges
				Breach: <90% uptime	(Baseline% - Achieved service level%)/20 x quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 cr. and Service Level: 87% Applicable penalty: (97% - 87%)/20 = 0.5% of quarterly AMC charges Applicable penalty on breach of service level of that Hardware for the month: INR 1.25 lakhs @ 0.5% of INR 2.5 Cr.
3	Availability of following Hardware ▶ Mobile Data Terminal Devices (MDT) ▶ Smart Phone-2W	Measured as availability of Hardware. Measurement tool: EMS report & MDM	Monthly	Baseline: >=95% uptime of the Hardware	NIL
				Lower performance: <95% > = 90% uptime	(Baseline% - Achieved service level%)/20 x

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
	▶ GPS Device				quarterly AMC charges
				Breach: <90% uptime	(Baseline% - Achieved service level%)/10 x quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 cr. and Service Level: 85% Applicable penalty: (95%-85%)/10= 1% of quarterly AMC charges Applicable penalty on breach of service level of that Hardware for the month: INR 2.5 lakhs @ 1% of INR 2.5 Cr.
4	UPS Power Supply	Supply of power to all IT equipment at Field location with 100% charge Measurement Tool: Report from EMS	Monthly	Baseline: power backup is 240 minutes in each case of power failure	NIL
				Breach: more than one stance of power failure, the backup <240 minutes	0.01% of quarterly AMC charges of each stance e.g. say quarterly AMC

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
					value for the period when service is delivered: INR 2.5 cr. Applicable penalty breach of service level for any two instances for any month: INR 5000 @ 0.01% of INR 2.5 Cr.

6.4.13 Performance of the key Web Applications

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
1	Average time taken for accessing Home page of the following applications hosted centrally for Intranet users: ► Contact Centre Reporting System ► Web and Desktop Application for	Script based checking in every 10 minutes daily (8 am to 8 pm) Monthly average from the log. Script based checking to be facilitated by the MSI	Monthly	Baseline: >= 98% of the transactions take less than or equal to 5 seconds	NIL
				Lower performance: <98% > = 90% transactions take less than or equal to 5 seconds	(Baseline% - Achieved service level%)/100 x quarterly AMC charges

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
	Monitoring-Police officials ▶ E-learning Software and Web learning ▶ Patrol Management system ▶ Human resource management system (HRMS) ▶ Document management system ▶ Business Intelligence (BI), Reporting & Analytics ▶ Enterprise Management System ▶ Inventory Management ▶ MDM-Mobility Device Management ▶ VTS-Vehicle tracking System-			Breach: <90% of the transactions take less than or equal to 5 seconds	(Baseline% - Achieved service level%)/50 x quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 cr. and Service Level: 88% Applicable penalty: (98% - 88%)/50 = 0.2% of quarterly AMC charges Applicable penalty on breach of service level of that application for the month: INR 50,000 @ 0.2% of INR 2.5 Cr.
2.	Average time taken for accessing Home page of the following applications hosted centrally for Internet users:	Script based checking in every 10 minutes daily (8 am to 8 pm) Monthly	Monthly	Baseline: >= 98% of the transactions take less than or equal to 8 seconds	NIL

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
	► Police station Module ► Citizen Portal	average from the log. Script based checking to be facilitated by the MSI		Lower performance: <98% > = 90% transactions take less than or equal to 8 seconds	(Baseline% - Achieved service level%)/100 x quarterly AMC charges
				Breach: <90% of the transactions take less than or equal to 8 seconds	(Baseline% - Achieved service level%)/50 x quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 cr. and Service Level: 88% Applicable penalty: (98% - 88%)/50 = 0.2% of quarterly AMC charges Applicable penalty on breach of service level of that application for the month: INR 50,000 @ 0.2% of INR 2.5 Cr.
3.	Average time taken for accessing Home page of the following applications which are installed on end user devices such	Script based checking in every 10 minutes daily (8 am to 8 pm) Monthly	Monthly	Baseline: >= 98% of the transactions take less than or equal to 10 seconds	NIL

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
	as Mobile/MDT based applications: ► Mobile Application for Police officials ► E-learning Software and Web learning ► Patrol Management system ► Human resource management system (HRMS) ► MDM- Mobility Device Management ► CAD Mobile responder ► PTT application ► GIS Map on MDT/Mobile Phone	average from the log. Script based checking to be facilitated by the MSI		Lower performance: <98% > = 90% transactions take less than or equal to 10 seconds	(Baseline% - Achieved service level%)/100 x quarterly AMC charges
				Breach: <90% of the transactions take less than or equal to 10 seconds	(Baseline% - Achieved service level%)/50 x quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 cr. and Service Level: 88% Applicable penalty: (98% - 88%)/50 = 0.2% of quarterly AMC charges Applicable penalty on breach of service level of that application for the month: INR 50,000 @ 0.2% of INR 2.5 Cr.

6.4.14 Performance of the Location Detection Services

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty

1	Location detection by the following services: ▶ Location Based Services (LBS) ▶ Emergency Location Services (ELS)	Location of the caller should be detected in the system within 15 sec. at Communication officer desktop Measurement Tool: Reports from EMS or call management system *Note: SLA will be measured separately for LBS and ELS*	Monthly	Baseline: >= 98% of the caller location take less than or equal to 15 seconds	NIL
				Lower performance: <98% > = 90% of the caller location take less than or equal to 15 seconds	(Baseline% - Achieved service level%)/100 x quarterly AMC charges
				Breach: <90% of the caller location take less than or equal to 15 seconds	(Baseline% - Achieved service level%)/50 x quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 cr. and Service Level: 88% Applicable penalty: (98% -88%)/50 = 0.2% of quarterly AMC charges Applicable penalty on breach of service level of that application for the month: INR 50,000 @ 0.2% of INR 2.5 Cr.

Note: The above SLA as mentioned in Clause 4.5.8 will be applicable if department accepts the above services i.e. LBS and ELS.

6.4.15 Integration Activity

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
1	Submission of the integration plan	Integration plan including commercial quote to be submitted by the MSI within 15 days from issuance of the order from ITECCS	Weekly	Baseline: Submission of the integration plan within 15 days from the issuance of the order from ITECCS	NIL
				Breach: Delay of one week	0.5% of respective integration price e.g. say total value for the integration of that activity: INR 20 lakhs. Applicable penalty on delay of two weeks: INR 20,000 @ 0.5% of 20 lakhs
2	Completion of the required integrations as defined in clause 4.27.10 of section 4 of this RFP	API level integration to be accepted by the ITECCS based on successful UAT	Weekly after agreed timelines as defined in integration plan and accepted by the ITECCS	Baseline: Completion of the integration as per agreed timeline with ITECCS	NIL
				Breach: Delay of one week	0.5% of respective integration price e.g. say total value for the integration of that activity: INR 20 lakhs. Applicable penalty on delay of two weeks: INR 20,000 @ 0.5% of 20 lakhs

Note:

1. *The applicable penalty on delay of submission of integration plan may be deducted from the invoice of AMC charges for O&M.*

2. *The integration price will be what MSI has quoted in Financial Bid (BoQ).*

6.4.16 Preventive maintenance of the Hardware

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
1	Preventive maintenance of the components as per schedule which is defined in section 4 of the RFP	MSI should provide proof of maintenance/ services as per schedule	Monthly	Baseline: Timely services of the components	NIL
				Breach: Delay of one week beyond schedule date	0.01% of quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 cr. Applicable penalty on delay of two weeks: INR 5,000 @ 0.01% of INR 2.5 Cr.
2	Regular testing of RF lines	MSI should test activation of RF lines Measurement: EMS	Daily	Baseline: Timely testing of network activation	NIL
				Breach: Delay of one week beyond schedule date	0.01% of quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 Cr. Applicable penalty on delay of two weeks: INR 5,000 @ 0.01% of INR 2.5 Cr.

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
3	Regular testing of CUG Mobile Phone for redundant connectivity	MSI should test activation of CUG Mobile Measurement: EMS	15 days	Baseline: Timely testing of network activation	NIL
				Breach: Delay of one week beyond schedule date	0.01% of quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 Cr. Applicable penalty on delay of two weeks: INR 5,000 @ 0.01% of INR 2.5 Cr.
4	Regular testing of redundant connectivity through RF lines and CUG Mobile Phones	MSI should test incoming calls on RF lines and CUG Mobile Phones with the help of Telecom Service Provider (TSP) Measurement: EMS	Quarterly	Baseline: Timely testing of network activation	NIL
				Breach: Delay of one week beyond schedule date	0.01% of quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 cr. Applicable penalty on delay of two weeks: INR 5000 @ 0.01% of INR 2.5 Cr.

6.4.17 Inventory Management and replacement of Consumables

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
1	Timely replacement of	MSI should replace	Half yearly	Baseline: Timely	NIL

S. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
	consumables as defined in Annexure 29 of section 9 of this RFP	consumables in timely manner as per the schedule		replacement of the consumables	
				Breach: Delay of one week beyond schedule date	0.01% of quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 Cr. Applicable penalty on delay of two weeks: INR 5000 @ 0.01% of INR 2.5 Cr.
2	Inventory Management as defined in FRS document	MSI should ensure the required inventory for the continuity of the smooth operation of UP112. The inventory will be inspected at the periodicity of half year during O&M stage. Measurement tool: Inventory Management System	Half yearly	Baseline: Submission of Inventory Management report.	NIL
				Breach: Delay of one week beyond schedule date	0.01% of quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 Cr. Applicable penalty on delay of two weeks: INR 5,000 @ 0.01% of INR 2.5 Cr.

6.4.18 Documentation and reporting during O&M Stage

Sl. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
1	Documentation and Reports as per scheduled and scope as defined in Clause 4.4 of section 4 of this RFP. This SLA criteria is also applicable to any adhoc report or plan related to customization of the software or related to other assigned task which MSI is asked to deliver/submit.	MSI should submit documents/reports as per the agreed schedule	Monthly	Baseline: No delay or non-submission of the required documents/reports	NIL
				Breach: One week delay in submission of report to ITECCS	0.01% of quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 Cr. Applicable penalty on delay of two such documents/reports of two weeks: INR 10,000 @ 0.01% of INR 2.5 Cr.
2	SLA reports should be available from tool as specified in service levels above	MSI should enable automation of SLA reporting through EMS or other as specified in FRS document	As per measurement interval of respective SLA	Baseline: Availability of SLA report as per required format through specified tool only	NIL
				Breach: Non-availability of the SLA report as per above requirement	10% of quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 Cr. Applicable penalty on non-availability of any two such reports: INR 25 Lakhs @ 10% of INR 2.5 Cr.

6.4.19 Issue resolution

Sl. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
1	Issues related to critical Software/Hardware to be resolved within defined timeline	Issue is to be resolved through Helpdesk and same should be marked in ticketing tool. Ticket will be closed only by the representative of the ITECCS after full satisfaction of the complainant. Measurement Tool: EMS	Monthly	>= 98% of Issues to be analysed and resolved in 2 hours resolution time	NIL
				Lower performance: <98% > = 90% of Issues to be analysed and resolved in 2 hours resolution time	(Baseline% - Achieved service level%)/20 x quarterly AMC charges
				Breach: <90% of Issues to be analysed and resolved in 2 hours resolution time	(Baseline% - Achieved service level%)/10 x quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 Cr. and Service Level: 88% Applicable penalty: (98% - 88%)/10 = 1% of quarterly AMC charges Applicable penalty on breach of service level for the month: INR 2.5 lakhs @ 1% of INR 2.5 Cr.

Sl. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
2	Issues related to non-critical Software/Hardware and consumables to be resolved within defined timeline	Issue is to be resolved through Helpdesk and same should be marked in ticketing tool. Ticket will be closed only by the representative of the ITECCS after full satisfaction of the complainant	Monthly	>= 98% of issues to be analysed and resolved in 4 hours	NIL
				Lower performance: <98% > = 90% of Issues to be analysed and resolved in 2 hours resolution time	(Baseline% - Achieved service level%)/40 x quarterly AMC charges
				Breach: <90% of Issues to be analysed and resolved in 2 hours resolution time	(Baseline% - Achieved service level%)/20 x quarterly AMC charges e.g. say quarterly AMC value for the period when service is delivered: INR 2.5 Cr. and Service Level: 88% Applicable penalty: (98% - 88%)/20 = 0.5% of quarterly AMC charges Applicable penalty on breach of service level for the month: INR 1.25 lakhs @ 0.5% of INR 2.5 Cr.

6.4.20 Network Performance Service Levels

Sl. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
1	Network Bandwidth Utilization for each Network port at DC, DR, UP112, OMC and other connected sites with internet and MPLS	Measured as utilization of Network in each port on 24 x 7 basis with frequency of 10 minutes Measurement tool: EMS report	Monthly	Baseline: >= 95% of the instances should be < = 80 of network utilization	NIL
				Lower performance: < 95% > = 90% of the instances are < = 80 of network utilization	(Baseline% - Achieved service level%)/20 x quarterly AMC charges
				Breach < 90% of the instances are < = 80 of network utilization	(Baseline% - Achieved service level%)/10 x quarterly AMC charges e.g. say total Quarterly Bandwidth charges: INR 50 lakhs Applicable penalty: (95% - 85%)/10 = 1% of quarterly bandwidth charges Applicable penalty on breach of service level for the month: INR 50,000 @ 1% of INR 50 lakhs
2	Network availability for each port at DC, DR, UP112, OMC and other connected sites with internet and	Measured as availability of the Network in each port on 24 x 7 basis Measurement tool: EMS report	Monthly	Baseline: > = 99.5% uptime of the port	NIL
				Lower performance: <99.5% > = 90% uptime	(Baseline% - Achieved service level%)/20 x quarterly AMC charges

Sl. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
	MPLS on Fiber Link			Breach: <90% uptime	(Baseline% - Achieved service level%)/10 x quarterly bandwidth charges e.g. say total Quarterly Bandwidth charges: INR 50 lakhs and service level: 89.5% Applicable penalty: (99.5%-89.5%)/10 = 1% of quarterly bandwidth charges Applicable penalty on breach of service level for the month: INR 50,000 lakhs @ 1% of INR 50 lakhs
3	Network availability for each port at DC, DR, UP112, OMC and other connected sites with internet and MPLS on RF Link	Measured as availability of the Network in each port on 24 x 7 basis Measurement tool: EMS report	Monthly	Baseline: > = 98.5% uptime of the port	NIL
				Lower performance: <98.5% > = 90% uptime	(Baseline% - Achieved service level%)/20 x quarterly AMC charges
				Breach: <90% uptime	(Baseline% - Achieved service level%)/10 x quarterly bandwidth charges e.g. say total Quarterly Bandwidth

Sl. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
					charges: INR 50 lakhs and service level: 88.5% Applicable penalty: (98.5% - 88.5%)/10 = 1% of quarterly bandwidth charges Applicable penalty on breach of service level for the month: INR 50,000 lakhs @ 1% of INR 50 lakhs
3	Available Bandwidth of the Network	MSI should ensure that Network bandwidth should be available in all the links as per plan procured by ITECCS Measured as availability of the Bandwidth of Network once in a month Measurement tool: EMS report	Monthly	Baseline: 100% availability of the required bandwidth	NIL
				Breach: >= Single instance of low bandwidth	0.05% of quarterly Bandwidth charges for each instance e.g. say total Quarterly Bandwidth charges: INR 10 lakhs Applicable penalty on breach of service level for any such two instances for any month: INR 1000 @ 0.05% of 10 Lakhs
4	Smooth telecom services for	Any interruption of services due	Monthly	Baseline: No single default	NIL

Sl. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
	continuous network/ MPLS/ Internet connectivity in SIM installed in MDTs, GPS and Smartphone as provided to PRVs which facilitates calls, data, SMS as per data plan procured by ITECCS	to outstanding payment to Telecom Service Provider or any other reason will be considered as default. Measurement tool: Report from MDM, Delivery Report from SMS Gateway		Breach: >= Single instance of default	0.05% of quarterly Bandwidth charges for each instance e.g. say total Quarterly Bandwidth charges: INR 10 lakhs Applicable penalty on two such instances for any month: INR 1000 @ 0.05% of 10 Lakhs
5	Failover mechanism of SIP with compliance of RTO and RPO as defined in clause 4.27.2 (e) of section 4 this RFP	In case of Failure of SIP channels: Automatic failover to available channels such as RF Channels, CUG Mobile, Analog lines Any complaint of no failover will be considered as instance of default	Monthly	Baseline: No single default	NIL
				Breach: >= Single instance of default	0.05% of quarterly Bandwidth charges for each instance e.g. say total Quarterly Bandwidth charges: INR 10 lakhs Applicable penalty on two such instances for any month: INR 1000 @ 0.05% of 10 Lakhs
6	Latency for Fibre Network in WAN	• Data Center to Remote Site.	Monthly	Baseline: Threshold level <= 5 ms (site to site)	NIL

Sl. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
		• Data Center to OMC Measured as latency between the sites on 24 x 7 basis with frequency of 10 minutes Measurement tool: EMS report		More than or equal to 95% instances of testing should be under the baseline value	
				Breach < 95% of the instances under the baseline value	0.05% of quarterly Bandwidth charges for each instance e.g. say total Quarterly Bandwidth charges: INR 10 lakhs Applicable penalty on two such instances for any month: INR 1000 @ 0.05% of 10 Lakhs
7	Latency for Fibre Network in WAN	• Data Center to Disaster Recovery Center Measured as latency between the sites on 24 x 7 basis with frequency of 10 minutes Measurement tool: EMS report	Monthly	Baseline: Threshold level <= 25 ms (site to site) More than or equal to 95% instances of testing should be under the baseline value	NIL
				Breach < 95% of the instances under the baseline value	0.05% of quarterly Bandwidth charges for each instance e.g. say total Quarterly Bandwidth

Sl. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
					charges: INR 10 lakhs Applicable penalty on two such instances for any month: INR 1000 @ 0.05% of 10 Lakhs
8	Latency for RF in WAN	• Data Center to Remote Site. • Data Center to OMC Measured as latency between the sites on 24 x 7 basis with frequency of 10 minutes Measurement tool: EMS report	Monthly	Baseline: Threshold level =< 10 ms (site to site) More than or equal to 95% of the instances should be under the baseline value	NIL
				Breach < 95% of the instances under the baseline value	0.05% of quarterly Bandwidth charges for each instance e.g. say total Quarterly Bandwidth charges: INR 10 lakhs Applicable penalty on two such instances for any month: INR 1000 @ 0.05% of 10 Lakhs
9	Latency for RF in WAN	• Data Center to Disaster Recovery Center	Monthly	Baseline: Threshold level =< 40 ms (site to site)	NIL

Sl. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
		Measured as latency between the sites on 24 x 7 basis with frequency of 10 minutes Measurement tool: EMS report		More than or equal to 95% of the instances should be under the baseline value	
				Breach < 95% of the instances under the baseline value	0.05% of quarterly Bandwidth charges for each instance e.g. say total Quarterly Bandwidth charges: INR 10 lakhs Applicable penalty on two such instances for any month: INR 1000 @ 0.05% of 10 Lakhs
10	Jitter for Fibre and RF in WAN	• Data Center to Remote Site. • Data Center to OMC • Data Center to Disaster Recovery Center Measured as latency between the sites on 24 x 7 basis with frequency of 10 minutes Measurement tool: EMS report	Monthly	Baseline: Threshold level =< 25 ms (site to site) More than or equal to 95% of the instances should be under the baseline value	NIL
				< 95% of the instances under the baseline value	0.05% of quarterly Bandwidth charges for each instance e.g. say total Quarterly Bandwidth

Sl. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
					charges: INR 10 lakhs Applicable penalty on two such instances for any month: INR 1000 @ 0.05% of 10 Lakhs
11	Packet loss for all the links in WAN	• Data Center to Remote Site. • Data Center to OMC • Data Center to Disaster Recovery Center Measured as latency between the sites on 24 x 7 basis with frequency of 10 minutes Measurement tool: EMS report	Monthly	Baseline: Threshold level: no pack loss More than or equal to 99.5% of the instances should be under the baseline value	NIL
				< 99.5% of the instances under the baseline value	0.05% of quarterly Bandwidth charges for each instance e.g. say total Quarterly Bandwidth charges: INR 10 lakhs Applicable penalty on two such instances for any month: INR 1000 @ 0.05% of 10 Lakhs

6.4.21 Cloud Services related Service Levels

Sl. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
1	Application Availability	High Availability of Could as a service (CAS) solution component measured within the Cloud	Monthly	Baseline: >=99.00% average resource availability	NIL
				Breach: <99.00% uptime	For every 0.25% drop, a penalty of 0.25% of quarterly O&M payment will be deducted. e.g., say total AMC value for the entire project: INR 50 cr. and Service Level 90% Applicable penalty: (99.0%-90%)/10=0.90% of quarterly AMC charges Applicable penalty on breach of service level for any month: INR 2.25 lakhs @ 0.90% of 2.5 Cr. (Quarterly value)

6.4.22 Cyber Security related Service Levels

Sl. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
1	Manpower availability at NOC and SOC	100% availability of the manpower at NOC and SOC should be ensured by MSI. The resource availability would be	Monthly	Baseline: >=99% average resource availability	NIL
				Breach: <99.00% uptime	(Breach level%-Achieved service

Sl. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
		calculated as: No. of shift days for which resources present at the designated location/ Total no. of shift days) x 100			level%)/10 x quarterly AMC charges e.g. say total AMC value for the entire project: INR 50 cr. and Service Level 90% Applicable penalty: (99.0%-90%)/10=0.90% of quarterly AMC charges Applicable penalty on breach of service level for any month: INR 2.25 lakhs @ 0.90% of 2.5 Cr. (Quarterly value)
2	Continuous Improvement and suggestions over a month as per Clause 4.24 of Section 4 of this RFP	Continuous improvements suggested and implemented to demonstrate continually evolving methodology and operations to address new threat vectors along with:– Changes suggested for SIEM rules as per the existing scenarios	Monthly	Baseline: 100% compliance	NIL
				Breach: Defaulter	0.05% of quarterly AMC Charges e.g. say total AMC value for the entire project: INR 50 cr. Applicable penalty on breach of service level for any two such defaults in any month: INR 25000 @ 0.05% of 2.5 Cr.

Sl. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
					(Quarterly value)
3	Report on attempted attacks/unauthorized access to database.	Any attacks / unauthorized access on DB including any unlawful attempt of data extraction via any medium needs to be reported to the ITECCS	Weekly	Baseline: 100% of such attempt to be reported within 15 minutes of occurrence	NIL
				Breach: <100%	0.5% of quarterly AMC Charges on each such case e.g. say total AMC value for the entire project: INR 50 cr. Applicable penalty on two such cases for any month: INR 2.5 lakhs @ 1% of 2.5 Cr. (Quarterly value)
4	Non-Detection of Security incidents that occurs and non-compliance with Incident Management and Response SLAs	Any incident wherein system compromised or any actual or reasonably suspected unauthorized use of or access to provider systems or any case wherein data theft occurs (including internal incidents). The SoC team to	Monthly	Baseline: 100% compliance	NIL
				Breach: Any incident of Default	0.1% of quarterly AMC Charges for each such case e.g. say total AMC value for the entire project: INR 50 cr. Applicable penalty on two such default cases for any

Sl. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
		investigate the breach, use its best efforts to mitigate the breach's impact, collect evidence surrounding the breach, and document its response. Measurement tool: SIEM			month: INR 50,000 @ 0.1% of 2.5 Cr. (Quarterly value)
5	Vulnerability Assessment	Authenticated Mode Assessment should be done for all assets on a monthly basis. The report to be submitted to ITECCS by 5th of next month High severity issues to be closed within 7 days of issue of report. Medium severity issues to be closed within the same month of issue of report. Monitoring tool: Vulnerability assessment report	Monthly	100% coverage of assets as per respective VA report for that month	NIL
				For any non-compliance with the SLA target	0.02% of quarterly AMC Charges e.g. say total AMC value for the entire project: INR 50 cr. Applicable penalty on such two non-compliances for any month: INR 10,000 @ 0.02% of 2.5 Cr. (Quarterly value)
6.	Penetration testing	The Penetration Testing of all the public facing assets and	Monthly	Baseline: 100% coverage of assets.	NIL

Sl. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
		services has to be done by the MSI on a quarterly basis. External PT should be done for all public facing assets and on a quarterly basis. The report to be submitted to ITECCS by 5th of the month following the quarter. High severity issues to be closed within 7 days of issue of report.		Breach: Any non-compliance with the SLA target.	0.02% of quarterly AMC Charges e.g. say total AMC value for the entire project: INR 50 cr. Applicable penalty on such two non-compliances for any month: INR 10,000 @ 0.02% of 2.5 Cr. (Quarterly value)
7	Update management This would include OEM patches/OEM version/upgrades/ customizations of software/ applications, Database and operating systems as and when required during project period. The MSI has to take necessary approval with the fallback strategy before such updates. The MSI to ensure all such updates duly communicated through OEM to ITECCS every six months	The updates to be installed on the systems in case released by the OEM or a flaw is identified due to an internal or external assessment by MSI or ITECCS High severity patches to be tested and installed within 7 days of issue of patch. Medium severity patches to be installed within 30 days of issue of patch. Measurement	Half yearly	Baseline: 100% coverage	NIL
				Breach: Any non-compliance with the SLA target.	0.04% of quarterly AMC Charges e.g. say total AMC value for the entire project: INR 50 cr. Applicable penalty on such two non-compliances for any month: INR 10,000 @

Sl. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
		Tool: System generated Incident log at Helpdesk			0.02% of 2.5 Cr. (Quarterly value)
8	All UP 112 data should be fully protected without any single instance of loss	All the project data should be stored and protect without any loss. Data purging policy will be decided mutually between MSI and ITECCS	Monthly	Baseline: No single instance of permanent data loss	NIL
				Lower performance: Any instance of data loss but recovered within 10 days	0.05% of quarterly AMC Charges for each such case e.g. say total AMC value for the entire project: INR 50 cr. Applicable penalty on two such default cases for any month: INR 25,000 @ 0.05% of 2.5 Cr. (Quarterly value)

Sl. No.	Definition	Measurement	Measurement Interval	Target	Applicable Penalty
				Breach: > = 1 instance of permanent data loss	1% of quarterly AMC Charges for each such case e.g. say total AMC value for the entire project: INR 50 cr. Applicable penalty on two such default cases for any month: INR 5 lakhs @ 0.1% of 2.5 Cr. (Quarterly value)

6.4.23 Technical Manpower for NexGen UP112

Sl. No.	Measurement	Definition	Measurement Interval	Target	Applicable Penalty
1	Replacement of key personnel defined in clause 4.28.1 in section Scope of work of the RFP	In case of permanent replacement of the key personnel as approved by the department, the MSI should replace the personnel only after 15 days from the approval and the deployment of the replacement personnel without any additional cost. At least 15 days Knowledge transfer will be applicable for such approved replacement.	Monthly	Not less than 15 days KT	5% of monthly Manpower Fees of the replaced personnel for each day of non-compliance of KT period e.g. say total Monthly unit rate of that resource: INR 1 lakh Applicable penalty on 5 days KT period would be (considering 2 days non-

Sl. No.	Measurement	Definition	Measurement Interval	Target	Applicable Penalty
					compliance): INR 10000 @ 5% of 1 lakh
2	Availability of the particular personnel at designated location as per requirement defined in clause 4.28.1 in section Scope of work of the RFP	[(Actual number of man-days of the deployed resource for a month) / (Agreed Total number of man-days in a month)] *100	Monthly	>= 98%	NIL
				Lower performance >=90 % to < 98%	5% of monthly Manpower Fees of the respective personnel e.g. say total Monthly unit rate of that resource: INR 1 lakh Applicable penalty on lower performance in this month: INR 5000 @ 5% of 1 lakh
				Breach: < 90 %	10% of monthly Manpower Fees e.g. say total Monthly unit rate of that resource: INR 1 lakh

Sl. No.	Measurement	Definition	Measurement Interval	Target	Applicable Penalty
					Applicable penalty on lower performance in this month: INR 10000 @ 10% of 1 lakh

6.4.24 Contact Centre Manpower for NexGen UP112

Sl. No.	Measurement	Definition	Measurement Interval	Measurement target	Applicable Penalty
1.	Average Speed to Answer (ASA)	ASA to be reviewed on a monthly basis. System generated reports to be considered to review the ASA	Monthly	>=98% of the calls to be attended within 5 seconds	NIL
				Lower performance: <98% > = 90% of the calls to be attended within 5 seconds	(Baseline% - Achieved service level%)/20 x monthly manpower cost for contact centre
				Breach: <90% of the calls to be attended within 5 seconds	(Baseline% - Achieved service level%)/10 x monthly manpower cost for contact centre e.g. say monthly manpower cost for contact centre for the period when service is delivered: INR 2 Cr. and Service Level: 88%

Sl. No.	Measurement	Definition	Measurement Interval	Measurement target	Applicable Penalty
					Applicable penalty: (98% - 88%)/10 = 1% of monthly manpower cost for contact centre Applicable penalty on breach of service level for the month: INR 2 lakhs @ 1% of INR 2 Cr.
2.	Average Handle Time (AHT) Compliance - Inbound Non-Actionable Call (AbC)	AHT to be reviewed on a monthly basis. Measurement tool: Report from CMS	Monthly	>=95% of the calls closed within 25 seconds	NIL
				Lower performance: <95% > = 90% of the calls closed within 25 seconds	(Baseline% - Achieved service level%)/20 x monthly manpower cost for contact centre
				Breach: <90% of the calls closed within 25 seconds	(Baseline% - Achieved service level%)/10 x monthly manpower cost for contact centre e.g. say monthly manpower cost for contact centre for the period when service is delivered: INR 2 Cr. and

Sl. No.	Measurement	Definition	Measurement Interval	Measurement target	Applicable Penalty
					Service Level: 85% Applicable penalty: (95% - 85%)/10 = 1% of monthly manpower cost for contact centre Applicable penalty on breach of service level for the month: INR 2 lakhs @ 1% of INR 2 Cr.
3.	Average Handle Time (AHT) Compliance - Inbound Actionable Call (AbC)	AHT to be reviewed on a monthly basis. Measurement tool: Report from CMS	Monthly	>=95% of the calls closed within 180 seconds	NIL
				Lower performance: <95% > = 90% of the calls closed within 180 seconds	(Baseline% - Achieved service level%)/20 x monthly manpower cost for contact centre
				Breach: <90% of the calls closed within 180 seconds	(Baseline% - Achieved service level%)/10 x monthly manpower cost for contact centre e.g. say monthly manpower cost for contact centre for the period when service is delivered:

Sl. No.	Measurement	Definition	Measurement Interval	Measurement target	Applicable Penalty
					INR 2 Cr. and Service Level: 85% Applicable penalty: (95% - 85%)/10 = 1% of monthly manpower cost for contact centre Applicable penalty on breach of service level for the month: INR 2 lakhs @ 1% of INR 2 Cr.
4.	Call Quality Score	Call Quality score method scores CO calls against predefined parameters to ensure adherence of COs to the defined SOPs. The parameters and mechanism for calculating quality score will be mutually agreed between ITECCS and MSI. These may cover: ▶ Adequate and accurate information captured during the call including	Monthly	>=80% score for all audited calls/ COs	NIL

Sl. No.	Measurement	Definition	Measurement Interval	Measurement target	Applicable Penalty
		location of the event ▶ Telephone etiquette and communication skills with require sympathy and empathy factors ▶ Responsiveness and active listening ▶ Knowledge, competency and skill ▶ Call management Call quality score to be reviewed on a monthly basis. Reports to be taken by SLA monitoring tool or reports generated by ITECCS. Measurement Tool: Report from CMS		<80% score for all audited calls/ COs	(Breach Level%-service level%)/50 x monthly Contact Centre Manpower Fees e.g. say total monthly manpower cost for contact centre: INR 2 cr and Service Level 70.0% Applicable penalty: (80%-75%)/50=0.1% of quarterly AMC charges Applicable penalty on breach of service level for any month: INR 20,000 @ 0.1% of 2 Cr.)
5.	Time bound call back for all disconnected calls	If any call is disconnected while the CO is answering before the completion of event process, a dedicated Outbound desk shall call back within 180 seconds of the disconnection. Measurement Tool: Report from CMS	Monthly	>=90% call back within 180 seconds	NIL

Sl. No.	Measurement	Definition	Measurement Interval	Measurement target	Applicable Penalty
				<90% call back within 180 seconds	(Breach Level%-service level%)/50 x monthly Contact Centre Manpower Fees e.g. say total monthly manpower cost for contact centre: INR 2 cr and Service Level 85.0% Applicable penalty: (90%-85%)/50=0.1% of quarterly AMC charges Applicable penalty on breach of service level for any month: INR 20,000 @ 0.1% of 2 Cr.)
6.	Attendance of Contact Centre' Manpower including Communication Officers	Refers to availability of all Contact Centre manpower as per agreed seats per shift and shift timings Attendance to be reviewed on monthly basis. The COs will mark their attendance through login on CTI. However, biometric attendance will be	Monthly	100% attendance of staff at UP POLICE 100	NIL
				Lower performance: <100% > = 90% attendance of staff at UP POLICE 100	(Baseline% - Achieved service level%)/10 x monthly manpower cost for contact centre
				Breach: <90% attendance of	(Baseline% - Achieved service level%)/5 x

Sl. No.	Measurement	Definition	Measurement Interval	Measurement target	Applicable Penalty
		considered for the other supervisory staff of the Contact Centre. Measurement Tool: Report from CMS		staff at UP POLICE 100	monthly manpower cost for contact centre e.g. say monthly manpower cost for contact centre for the period when service is delivered: INR 2 Cr. and Service Level: 80% Applicable penalty: (100% - 80%)/10 = 8% of monthly manpower cost for contact centre Applicable penalty on breach of service level for the month: INR 16 lakhs @ 8% of INR 2 Cr.
7.	Non-compliance to UP112 regulations	Refers to the non-compliance related to UP112 uniform code, moral behaviour, pick & drop facility etc. as per UP112 policy. Violation of the policy will be monitored on the basis of complaints received. It will be	Monthly	Baseline: =<2 such instances monthly	NIL
				Breach >=3 such instances monthly	0.2% of monthly Contact Centre Manpower Fees for each such stance e.g. say total monthly manpower

Sl. No.	Measurement	Definition	Measurement Interval	Measurement target	Applicable Penalty
		reviewed on a monthly basis.			cost for contact centre: INR 2 cr. Applicable penalty on two such instances for any month: INR 80,000 @ 0.2% of 2 Cr
8.	Compliance for caller feedback	Refers to the percentage calls for which a dispatch has happened, and feedback was taken by the Feedback desk to be managed by outbound CO. The Feedback desk is required to take 100% feedback of all the actionable calls within next day.	Monthly	95% feedback of actionable calls within next day	NIL
				Lower performance: <95% > = 90% feedback of actionable calls within next day	(Baseline% - Achieved service level%)/20 x monthly manpower cost for contact centre
				Breach: <90% feedback of actionable calls within next day	(Baseline% - Achieved service level%)/10 x monthly manpower cost for contact centre e.g. say monthly manpower cost for contact centre for the period when service is delivered: INR 2 Cr. and Service Level: 85% Applicable penalty: (95% - 85%)/10 = 1% of monthly

Sl. No.	Measurement	Definition	Measurement Interval	Measurement target	Applicable Penalty
					manpower cost for contact centre Applicable penalty on breach of service level for the month: INR 2 lakhs @ 1% of INR 2 Cr.
9.	Response to non-voice mode of communications: ▶ SMS ▶ IoT, ▶ Panic button ▶ Mobile application ▶ Mobile chat ▶ VoIP ▶ Email ▶ Web chat ▶ SLA for Social media	▶ Response to the citizens from COs as per agreed SOP ▶ Case to be created in the emergency response system ▶ Create event and submit to auto dispatcher Should be monitored on monthly basis and system generated reports should be taken	Monthly	95% average acknowledgement and initiate action within 60 seconds	NIL
				Lower performance: <95% > = 90% average acknowledgement and initiate action within 60 seconds	(Baseline% - Achieved service level%)/20 x monthly manpower cost for contact centre
				Breach: <90% average acknowledgement and initiate action within 60 seconds	(Baseline% - Achieved service level%)/10 x monthly manpower cost for contact centre e.g. say monthly manpower cost for contact centre for the period when service is delivered: INR 2 Cr. and Service Level: 85% Applicable penalty: (95%

Sl. No.	Measurement	Definition	Measurement Interval	Measurement target	Applicable Penalty
					- 85%)/10 = 1% of monthly manpower cost for contact centre Applicable penalty on breach of service level for the month: INR 2 lakhs @ 1% of INR 2 Cr.

6.4.25 Training and Capacity Building

Sl. No.	Measurement	Definition	Measurement Interval	Measurement target	Applicable Penalty
1.	Training as per agreed schedule	Training should be conducted as per agreed schedule with ITECCS	Monthly	Baseline: Delivery of training on schedule	NIL
				Breach: Delay in delivery of training	2.5% of the applicable payment on the respective resource for the delay of each day apart from the deduction on salary based on number of days of absence. e.g. if person is absent for 2 days, the total penalty will be as follows:

Sl. No.	Measurement	Definition	Measurement Interval	Measurement target	Applicable Penalty
					2.5 % of the salary x 2 days delay

6.4.26 The MSI needs to ensure service levels on an average for measurement interval. E.g. applicable penalties for any particular performance criteria in successive 3 months are x, y and z where measurement interval is month while it is to be deducted from quarterly payment. The total penalty will be deducted from the quarterly payment would be x+y+z.

6.4.27 Penalty for not meeting a target level for a component for any 2 consecutive measurement intervals shall result in twice the value of the penalty which is applicable as per the measurement interval defined in the above table. For example, if the applicable penalty for breach of service level in any particular performance criteria for monthly measurement interval is INR10,000 and this performance criteria has been reported breach in last month as well, then the applicability would be INR 20,000. If breach of the service level continues in third successive month, the value of the deduction would be 3 times of the applicable penalty. This would continue in the same manner for each consecutive measurement intervals.

6.4.28 Also, the continuous breach of the service level for any particular performance criteria may lead to "Risk purchase" by ITECCS as per the clause 5.33.

6.4.29 The total penalty applicable for any quarter shall not exceed 30% of the total applicable fees for the respective quarter.

6.4.30 Three consecutive quarterly deductions of 30 % of the total applicable fee on account of any reasons will be deemed to be an event of default and termination as per the clause 5.23.1 of this RFP and the consequences as provided in clause 5.23.5 shall follow.

6.5 Reporting procedures

6.5.1 The SLA parameters shall be monitored on a quarterly basis as per the individual SLA parameter requirements while reporting shall be monthly or instance/incident/event bases. However, if the performance of the system/services is degraded significantly at any given point in time during the contract and if the immediate measures are not implemented and issues are not rectified to the complete satisfaction of ITECCS or an agency designated by them, then ITECCS will have the right to take appropriate disciplinary actions including termination of the contract.

6.5.2 ITECCS reserves the right to determine the monitoring & calculation frequency of SLAs.

6.5.3 Relevant SLA parameter shall be applicable in same quantum for any breach on cloud as in case of DC

6.5.4 The MSI will ensure the automation of SLA reports from the tool as defined in the above service levels. No manual report unless specified in above service levels, will be accepted for the calculation of penalty.

6.5.5 Overall Availability and Performance Measurements will be on a monthly basis for

the purpose of Service Level reporting. An “Availability and Performance Report” will be provided by the MSI on monthly basis in the ITECCS suggested format and a review shall be conducted based on this report. A monthly Availability and Performance Report shall be provided to the ITECCS at the end of every month containing the summary of all incidents reported and associated MSI performance measurement for that period. The monthly Availability and Performance Report will be deemed to be accepted by the ITECCS upon review and signoff by both MSI and ITECCS or ITECCS designated Agency.

6.5.6 EMS system as specified in this RFP shall play a critical role in monitoring the SLA compliance and hence will have to be customized accordingly. The 3rd party testing and audit of the system shall put sufficient emphasis on ensuring the capability of EMS system to capture SLA compliance correctly and as specified in this RFP. The MSI must deploy EMS tool and develop additional scripts (if required) for capturing the required data for SLA report generation in automated way. This tool should generate the SLA Monitoring report in the end of every month which is to be shared with ITECCS on a monthly basis. The tool should also be capable of generating SLA reports for any required measurement interval.

6.5.7 ITECCS or its nominated agency shall have full access to the EMS solution (and any other tools / solutions deployed for SLA measurement and monitoring) to extract data (raw, intermediate as well as reports) as required during the project. ITECCS or its nominated agency will also audit the tool and the scripts on a regular basis.

6.5.8 The measurement methodology / criteria / logic will be reviewed by ITECCS.

6.5.9 Wherever, the measurement is through a client setup at DC / DRC, remote access to the client should be available at ITECCS Headquater. In addition, remote access should be provided at ITECCS Headquarter for all EMS data and logs.

6.5.10 In case of default on any of the service level metric, the ITECCS shall submit performance improvement plan along with the root cause analysis for ITECCS’s approval.

6.6 Issue management procedures

6.6.1 This process provides an appropriate management structure for the orderly consideration and resolution of business and operational issues in the event that quick consensus is not reached between ITECCS and MSI.

6.6.2 Implementing such a process at the beginning of the outsourcing engagement significantly improves the probability of successful issue resolution. It is expected that this pre-defined process will only be used on an exception basis if issues are not resolved at lower management levels.

6.7 Relaxation in SLA

6.7.1 Any relaxation in SLA parameter during contingency/ operational situation/ force majeure is to be made with the prior approval of DGP.

6.7.2 The authority to decide the financial aspect emerging out of such relaxation will be as under on monthly invoices:

a. ADG 112: less than or equal to INR 1.25 Cr.
b. DGP, Uttar Pradesh Police: 1.25 Cr. to INR 5 Cr.
c. GoUP: more than INR 5 Cr.

6.8 Service level change control

6.8.1 It is acknowledged that this Service levels may change as ITECCS business needs evolve over the course of the contract period. As such, this document also defines

the following management procedures:

a. A process for negotiating changes to the Service Levels.
b. An issue management process for documenting and resolving particularly difficult issues.
c. ITECCS and MSI management escalation process to be used in the event that an issue is not being resolved in a timely manner by the lowest possible level of management.
d. Any changes to the levels of service provided during the term of this Agreement will be requested, documented and negotiated in good faith by both parties. Either party can request a change.

6.8.2 Service Level Change Process: The parties may amend Service Level by mutual agreement in accordance. Changes can be proposed by either party Unresolved issues will also be addressed. The MSI's representative will maintain and distribute current copies of the Service Level document as directed by ITECCS. Additional copies of the current Service Levels will be available at all times to authorized parties.

6.8.3 Version Control: All negotiated changes will require changing the version control number. As appropriate, minor changes may be accumulated for periodic release or for release when a critical threshold of change has occurred.

7 FINANCIAL FORMAT

Note:

- All amounts shall be made in Indian Rupees Only
- Bidder should provide all prices, and quantities as per the prescribed format under this Annexure. Bidder should not leave any field blank. In case the field is not applicable, Bidder must indicate “0” (Zero) in all such fields.
- It is mandatory to provide a breakup of all Taxes, Duties and Levies wherever applicable and or payable.
- The buyer reserves the right to ask the Agency to submit proof of payment against any of the taxes, duties, or levies indicated.
- The buyer shall take into account all Taxes, Duties, and Levies for the purpose of Evaluation.
- Bidder to quote maximum 70% cost under CAPEX (for overall and each line item), this excludes manpower and network components.
- No OPEX as AMC charges or recurring charges can be left blank for any component
- All the rates shall be applicable throughout the life cycle of the project and the selected bidder has to provide the same on the same rates in case of any supply/ demand by the department.
- CAPEX-1 to be considered as new procurement/replacement/upgrade under first 2 years of project w.e.f. signing of contract.
- CAPEX-2 to be considered as new procurement/replacement/upgrade after 2 years of project i.e., 3rd year onwards.
- No separate payment will be considered for the deployed manpower during the Implementation and migration phase.
- Year wise manpower cost for O&M Phase shall be provided by the MSI
- All minimum (Min.) number of units are given in the financial table, bidder may like to increase as per solution requirements
- Bidder to ensure 10% variation in scope, hence quote the financials considering such variations.
- All payments to be paid to the selected bidder shall be inclusive of all statutory levies, duties, taxes, and other charges whenever levied/applicable.
- Buyer reserves the right to reject any proposals, whole or in part, to waive any or all informalities and disregard non-conforming, non-responsive or conditional proposals.
- Bidder to consider EOS and EOL sheet for evaluating the cost of bid as per Section 4.27.8 of Scope of Work of RFP

- The bidders must submit the itemized summary of BoQ and other item with all relevant details including description, quantities and rates to the department as prescribed in the RFP.

- Bidder to provide cost of any missing item in BOQ under “Others”, breakup of the other Items needs to be provided by MSI before issuance of LOI.
- Bidder can quote only one OEM against any product, quoting multiple OEM may lead to rejection of bid.

Note- All breakdown or accidental or physical damage will be covered under warranty by MSI

Service or repair due to normal and heavy usage wear and tear and any incidental damages

- *Non-remedial work, including but not limited to reprogramming and product configuration*
- *Repair of problems caused by physical damage, operator error including but not limited to:*
  - *Excessive dirt or contamination affecting performance*
  - *Spillage of liquids and other foreign substances on products*
  - *Scratched, contaminated and or damaged optical components*
  - *Loose or missing parts, broken, cracked, disfigured, scratched displays, windows, housings or triggers*
  - *Broken or cracked plastic parts (internal or external)*
  - *Damaged external cables*

S No	Item	Table	Total Value (INR)
1	Hardware components at DC	Table A	
2	Hardware components at DRC on Cloud	Table B	
3	Hardware components at DC on Cloud	Table C	
4	Hardware components at Command Centre, Lucknow	Table D	
5	Hardware components at Field	Table E	
6	Hardware components at OMCs	Table F	
7	Integration Requirements	Table G	
8	Software Components	Table H	
9	Network Bandwidth	Table I	
10	Data Network	Table J	
11	Contact Centre Staff	Table K	
12	Technical Manpower for O&M Phase	Table L	
13	Miscellaneous Items	Table M	
14	Financial format: Training	Table N	
Total			

The total project value in numbers is

INR_____

The total project value in words is

INR_____

7.1 Table A: Financial format - Hardware components at DC

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) *Write as applicable*
1	Biometric		1											
2	SAN Storage (223 TB)		1											
3	Disk to Disk Storage (160 TB)		1											
4	Database server- 2 CPU (288 core 3.3 TB memory)		7											
5	Blade chassis		6											
6	Rack		8											
7	Blade Server-2 CPU		2											
8	Blade server-4 CPU (1450 core 7 Tb memory)		15											
9	Link Load Balancer		2											
10	Server Load Balancer		2											
11	UPS Battery bank (272 Nos.) for 200KVA UP- 3Nos.		272											

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) *Write as applicable*
	(2 hours backup required)													
12	Core Switch		2											
13	Managed Access Switch		8											
14	SAN Switch		2											
15	Aggregation Switch		2											
16	Internet Router		2											
17	Core router		2											
18	Global Load Balancer		2											
19	Server for Vehicle Mounted Camera-rack mounted with rack		9											
20	Web Application Firewall		2											
21	NextGen Firewall		4											
22	Security Incident & Event Management (SIEM)		1											

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) *Write as applicable*
23	Data Leakage Prevention (DLP)		2											
24	Network Access Control (NAC)		2											
25	Storage for Vehicle Mounted Camera and Body Worn Camera (TB)		2640											
26	Others													
												Total (A) (in INR)		

7.2 Table B: Financial format – DRC on Cloud

#	Description	Unit Rate	Min. No. of Units	Capex-1	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable

1	VMs Cost (approx. 869 cores and 4.7 TB of Memory)												
2	Storage Cost (146 TB)												
3	Disk to Disk Storage (160 TB)												
4	Security Cost												
5	Others												
												Total (B) (in INR)	

Note: Bidder may like to customize above financial format of DRC, in order to host 50% size of DC under high availability mode

7.3 Table C: Financial format - DC on Cloud

#	Description	Unit Rate	Min. No. of Units	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
1	VMs Cost (approx. 1738 cores and 4.7 TB of Memory)												
2	Storage Cost (223 TB)												

3	Disk to Disk Storage (160 TB)												
4	Security Cost												
5	Others												
												Total (C) (in INR)	

Note: Bidder have to customize above financial format of DC on Cloud as per Section 7.1 Table A

7.4 Table D: Financial format - Hardware components at Command Centre, Lucknow

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
1	Biometric		17											
2	Desktops including Hindi Keypad on Keyboard with two monitors with OS and Antivirus		286											
3	Desktops including Hindi Keypad on Keyboard with triple monitors with OS and Antivirus		3											

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
4	Desktops including Hindi Keypad on Keyboard with single monitor with OS and Antivirus		38											
5	Desktop Thin client including Hindi Keypad on Keyboard		183											
6	IP Phones with Headset		671											
7	Laptop		17											
8	Tablets-Android with Stylus, Screen guard and Rugged Cover		24											
9	Printer, scanner and copier (multi-function)		10											
10	Heavy Duty printer		9											
11	Laser jet printer		10											
12	Paper shredder		5											
13	3 Conference room with equipment of capacity 15 people		-											

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
I	Audio System		3											
Ii	Control System		3											
14	2 Conference rooms with equipment of capacity 10 people		-											
I	Audio System		2											
Ii	Control System		2											
14	2 Conference rooms with equipment of capacity 8 people		-											
I	Audio System		2											
Ii	Control System		2											
15	3 Conference room with equipment of capacity 20 people		-											
I	Audio System		3											
Ii	Control System		3											
16	1 Meeting room with equipment of capacity 30 people		-											
I	Audio System		1											
Ii	Control System		1											

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
17	2 Board rooms with equipment of capacity 30 people		-											
I	Audio System		2											
Ii	Control System		2											
18	2 training rooms with equipment of capacity 25 people		-											
i	Screen		2											
ii	Projector		1											
iii	Audio system		2											
iv	Lael Microphone		2											
19	2 training rooms with equipment of capacity 50 people		-											
i	Screen		2											
ii	Projector		1											
iii	Audio system		2											
iv	Lael Microphone		2											
20	1 Training rooms with equipment of capacity 50 people		-											

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
	(35 Dos live training room)													
i	Screen		1											
ii	Projector		1											
iii	Audio system		1											
iv	Lapel Microphone		1											
v	Streaming Solution Device		1											
vi	Desktops with triple monitors with OS and Antivirus		35											
vii	IP phone with headset		35											
viii	Tabletop microphone		1											
ix	VHF static radio device		29											
x	Access Switch		2											
xi	MDT		1											
21	1 training rooms with equipment of capacity 100 people		-											

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
i	Screen		1											
ii	Projector		1											
iii	Audio System		1											
iv	Lapel Microphone		1											
22	1 Training rooms with equipment of capacity 100 people (75 Cos live training room)		-											
i	Screen		1											
ii	Projector		1											
iii	Audio System		1											
iv	Lapel Microphone		1											
v	Access Switch		2											
vi	Tabletop microphone		75											
vii	Streaming Solution Device		1											
viii	Desktops with double monitors with OS and Antivirus		75											

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
ix	IP phone with headset		75											
23	Video Conference equipment for 15 locations		15											
24	Digital light processing (DLP) video wall		3											
25	Radio Gateway		1											
26	Digital Radio Channel License for RoIP Server		1											
27	VHF static radio device		29											
28	lattice Mast and antenna for VHF static set		1											
29	Network Rack		2											
30	Managed Access Switch-24 ports		36											
31	Interactive Screen for EOC		2											
32	Y Jack		12											

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
33	Others													
												Total (D) (in INR)		

Note: 1. Bidder to quote maximum 70% cost under CAPEX

2. Bidder to seek hardware availability and propose new and upgradations as per section 4 clause 4.27.8

7.5 Table E: Financial format - Hardware components at Field

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
1	Desktops including Hindi Keypad on Keyboard with single monitor with OS,		129											

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
	office suite and Antivirus													
2	Desktops including Hindi Keypad on Keyboard with two monitors with OS, office suite and Antivirus		193											
3	Mobile Data Terminal Devices (MDT) minimum 7 inches screen with cradle		4278											
4	Smart Phone-2W & 4W with Screen Guard and Rugged Cover		6278											
5	LED TV 43" for DCR		78											
6	UPS 1 kVA (4 hours backup required)		118											
7	UPS 2KVA (4 hours backup required)		11											
8	Network Rack		130											

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
9	IP Phone with Headset		151											
10	VHF 4W antenna		4278											
11	Lattice Mast and antenna for VHF static set		78											
12	VHF static radio device		4356											
13	Battery of VHF Hand-Held Radio Device and Charger of Battery pack		2000											
14	VHF Handheld radio device		2000											
15	Managed Access Switch 24 Ports		129											
16	Intranet Router 20Mbps		129											
17	RFID Reader and Controller		78											
18	RFID Tags		50000											
19	ROIP Solution													

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
i	Radio Over IP Gateway		78											
ii	ROIP Advance digital software		1											
iii	Digital Radio Channel License for RoIP Server		78											
iv	Digital Subscriber License for RoIP Server		78											
V	Dispatcher Software License		108											
20	Earthing		78											
21	ID Card Printer		4											
22	Body worn camera		6278											
23	Vehicle mounted camera PTZ with accessories and installation		688											
24	MNVR with 1TB Storage		688											
25	PTZ Control unit with Keyboard		688											

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
26	7" LCD Monitor		688											
27	GPS device		6278											
28	Shifting charges of DCR equipment in case of shifting more than 200 meter / within same premises in same city		1											
29	Shifting charges of DCR equipment in case of shifting the field location to be shifted / to another city		1											
30	Others		1											
													Total (E) (in INR)	

Note: Bidder to quote maximum 70% cost under CAPEX

7.6 Table F: Financial format - Hardware components at OMCs

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
1	Desktops including Hindi Keypad on Keyboard with two monitors with OS, office suite and Antivirus		86											
2	Desktops including Hindi Keypad on Keyboard with triple monitors with OS, office suite and Antivirus		2											
3	Desktops including Hindi Keypad on Keyboard with single monitors with OS office suite and Antivirus		6											
3	Laptop		2											
4	IP Phones with Headset		106											
5	Printer, scanner and copier(multi-function)		4											

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
6	Laser jet printer		4											
7	Heavy Duty printer		2											
9	VHF static radio device		8											
10	Lattice Mast and antenna for VHF static set		2											
12	Radio Gateway		2											
13	Digital Radio Channel License for RoIP Server		2											
14	2 Meeting rooms with equipment of capacity 20 people		-											
i	Audio System		2											
ii	Control System		2											
15	Printer, Scanner and copier (multi-function)		2											
16	Network Rack		2											
17	Managed Access Switch 24 ports		8											

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
18	Intranet Router - 500Mbps		4											
19	UPS 20 kVA (2 hours backup required)		4											
20	Biometric		6											
21	Auto-phase sequence corrector in OMCs		2											
22	voltage control stabilization at OMCs		2											
23	Y Jack		8											
24	Others													
												Total (F) (in INR)		

Note: 1. Bidder to quote maximum 70% cost under CAPEX

2. Bidder to seek hardware availability and propose new and upgradations as per section 4 clause 4.27.8

7.7 Table G: Financial format - Integration Requirements

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
1	Integration of Smart cities		1											
2	Integration of Safe cities		10											
3	WCSO-1090 for Map and LBS sharing		1											
4	CRIS Integration		1											
5	Metro Safety Integration													
5.1	Lucknow Metro		1											
5.2	Agra Metro		1											
5.3	Gorakhpur Metro		1											
5.4	Kanpur Metro		1											
6	Disaster helpline Integration		1											
7	NHAI Helpline Integration		1											
8	UPEIDA Helpline Integration		1											
9	YEIDA Helpline Integration		1											
10	Fire Integration													

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
10.1	Smartphone for Fire brigade Vehicles with Screen Guard and rugged cover		1100											
10.2	GPS devices for Fire brigade Vehicle		1100											
10.3	Fire brigade Vehicle Mobile Responder application for CAD access		1100											
10.4	IP Phones with Headset at District Fire Control rooms		75											
10.5	Desktop with 2 Monitors at District Fire Control rooms with Hindi Keypad on Keyboard with triple monitors with OS, office suite and Antivirus		75											

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
10.6	24 Port Switch at District Fire Control rooms		75											
10.7	Router 20Mbps at District Fire Control rooms		75											
10.8	UPS 1KVA with 30min backup at District Fire Control rooms		75											
10.9	2 Mbps Connectivity primary		75											
10.11	2 Mbps Connectivity secondary		75											
11	SDRF Integration		1											
12	GRP Integration													
12.1	MDT 7" for GRP Station		65											
12.2	IP Phones with Headset (3 New and 6 old)		3											
12.3	Desktop with two Monitors with Hindi Keypad on Keyboard		9											

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
	with triple monitors with OS, office suite and Antivirus													
12.4	24 Port Switch at SRP stations		6											
12.5	24 Port Switch at IG, DIG and HQ		3											
12.6	Router 20Mbps		9											
12.7	UPS 1KVA with 30min backup		9											
12.8	2Mbps Connectivity		9											
12.9	Camera for Video Conferencing		9											
13	CM Helpline Integration		1											
14	**VC at SP /SSPs/ commiserates office**													
14.1	Desktop with single Monitors with Hindi Keypad on Keyboard with triple monitors with OS, office suite and Antivirus		78											
14.2	24 Port Switch		78											

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
14.3	Router 20Mbps		78											
14.4	UPS 1KVA with 30 min backup		78											
14.5	2Mbps Connectivity		78											
14.6	IP Phones with Headset		78											
14.7	Camera for Video Conferencing		78											
15	UP COP Integration		1											
16	Others													
												Total (G) (in INR)		

Note: For similar future integrations, the same level of integration defined in section 4.27.10 of the RFP shall apply. The above-mentioned rates will also apply to future API-level integrations.

7.8 Table H: Financial format - Software Components

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
1	IP PBX license													
2	Automatic Call Distribution (ACD) license													
3	Voice Recording & Quality Monitoring license													
4	Multimedia System license													
5	Computer Telephony Interface (CTI)													
6	Outbound Dialler													
7	Contact Centre Reporting System													
8	Softphone Licence													
9	Computer Aided Dispatch (CAD) license													
9.1	Communication officer licence													
9.2	Dispatch license													

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
10	CAD Mobile Software for MDT licence													
11	Web and Desktop Application for Monitoring-Police officials													
12	Police station Module													
13	Mobile Application for Police officials													
14	Mobile application for GIS Data collection													
15	Citizen Portal													
16	E-learning Software and Web learning													
17	Patrol Management system													
18	Human resource management system (HRMS)													

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
19	Document management system													
20	Business Intelligence (BI), Reporting & Analytics													
21	Enterprise Management System													
22	Directory services													
23	Emergency Monitoring System													
24	GIS Map (Map, Map Data, POI) for complete UP state													
25	GIS software license													
26	SMS Gateway													
27	Inventory Management													
28	MDM-Mobility Device Management													
29	VTS-Vehicle tracking System-													

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
30	Number masking													
31	Emergency/Advance Location Services													
32	Location Based Service (LBS)													
33	Chat Bot application													
34	Server OS licence Upgrade													
35	Database license upgrade													
36	Video Conferencing software upgrade													
37	Fleet (PRV) management software													
38	VMS Licence for cameras													
39	Anti-APT													
40	Zero trust network													
41	Patch Management Solution													

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
42	Threat Intelligence Tools/Solutions (SOAR)													
43	Anti DDoS													
44	Intrusion Prevention System (IPS)													
45	Threat Intelligence & dark Web Monitoring + Threat hunting framework with L3 CERT monitoring													
46	Endpoint Security													
47	Identity and Access management													
48	Application Security													
49	SSL Interceptor and VPN Gateway													
50	Hardware Security Module (HSM), Anti Ransomware and Encryption Solution													

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total	Remarks (Upgrade/New/Upgrade and New) Write as applicable
51	User Behaviour Analysis System													
52	SDWAN Controller Software													
53	Software defined Network (SDN)													
54	Others													
												Total (H) (in INR)		

Note: Bidder to quote the quantity and lot as per application user data as per section 9 annexure 25

7.9 Table I: Financial format - Network Bandwidth

#	Description	Unit Rate	Min. Bandwidth in Mbps	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total
1	**Data Centre Location-Lucknow**												
1.1	MPLS bandwidth Primary at DC		800										
1.2	MPLS bandwidth Secondary at DC		600										

#	Description	Unit Rate	Min. Bandwidth in Mbps	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total
1.3	NLD Links DC-DR Primary		500										
1.4	NLD Links DC-DR Secondary		100										
1.5	Internet bandwidth Primary		300										
1.6	Internet bandwidth Secondary		300										
2	**Disaster Recover Location- DC Provider Location**												
2.1	MPLS bandwidth Primary (including APN Bandwidth)		600										
2.2	MPLS bandwidth Secondary (including APN Bandwidth)		250										
2.3	Internet bandwidth Primary		150										
2.4	Internet bandwidth Secondary		150										
3	**Operation Mirroring Centre (OMC) Location**												
3.1	MPLS bandwidth Primary- Prayagraj		30										
3.2	MPLS bandwidth Secondary- Prayagraj		30										

#	Description	Unit Rate	Min. Bandwidth in Mbps	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total
3.3	MPLS bandwidth Primary- Ghaziabad		30										
3.4	MPLS bandwidth Secondary- Ghaziabad		30										
3.5	NLD Links to DC Primary- Prayagraj		12										
3.6	NLD Links to DC Secondary- Prayagraj		12										
3.7	NLD Links to DC Primary—Ghaziabad		12										
3.8	NLD Links to DC Secondary-- Ghaziabad		12										
3.9	NLD Links to DR Primary—Prayagraj		12										
3.10	NLD Links to DR Secondary-- Prayagraj		12										
3.11	NLD Links to DR Primary—Ghaziabad		12										
3.12	NLD Links to DR Secondary- Ghaziabad		12										
4	**District Control Room**												
4.1	MPLS bandwidth Primary		4										

#	Description	Unit Rate	Min. Bandwidth in Mbps	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total
4.2	MPLS bandwidth Secondary		4										
5	Others												
												Total (J) (in INR)	

- **Note:** Bidder to quote 100 % cost under OPEX

7.10 Table J: Financial format - Data Network

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year (A2)	OPEX for 3rd Year (A3)	OPEX for 4th Year (A4)	OPEX for 5th Year (A5)	Tax %	Tax Amt.	Total
1	SIP Lines at DC (Airtel)		25										
2	SIP Lines at DC (Jio)		18										
3	SIP Lines at DC (BSNL)		1										
4	SIP Lines at DC (Voda-Idea)		8										
5	SIP Lines at OMC-Prayagraj (Airtel)		2										
6	SIP Lines at OMC-Prayagraj (BSNL)		1										
7	SIP Lines at OMC-Prayagraj (Jio)		2										
8	SIP Lines at OMC-Prayagraj (Voda-idea)		1										

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year (A2)	OPEX for 3rd Year (A3)	OPEX for 4th Year (A4)	OPEX for 5th Year (A5)	Tax %	Tax Amt.	Total
9	SIP Lines at OMC-Ghaziabad (Airtel)		2										
10	SIP Lines at OMC-Ghaziabad (BSNL)		1										
11	SIP Lines at OMC-Ghaziabad (Jio)		2										
12	SIP Lines at OMC-Ghaziabad (Voda-Idea)		2										
13	MDT 2W &4W SIM charges		6278										
14	4W Mobile Phones SIM charges		4278										
15	GPS 4W & 2W SIM charges		6278										
16	MDT Fire SIM charges		1100										
17	GPS Fire SIM charges		1100										
18	GRP MDT SIM charges		65										
19	Vehicle Mounted camera SIM Charges		688										
20	Body Worn Camera SIM Charges		6278										
21	Outgoing SMS (10 SMS per 25,000		1 lot										

#	Description	Unit Rate	Min. No. of Units	Capex-1	Capex-2	OPEX for 1st Year	OPEX for 2nd Year (A2)	OPEX for 3rd Year (A3)	OPEX for 4th Year (A4)	OPEX for 5th Year (A5)	Tax %	Tax Amt.	Total
	events daily) around 9,12,50,000 per year												
22	Public IP Address		5										
23	RF line PRI failover over SIP-3 at centre and 2 at OMC		5										
24	PNT Line charges for failover		53										
25	Failover SIM Charges		110										
26	WPC / spectrum licensees charges per year		1										
27	Others												
												Total (J) (in INR)	

- **Note:** One SIP line means 30 channels each
- **Note:** Bidder to quote 100 % cost under OPEX

7.11 Table K: Financial format - Contact Centre Staff

#	Description	No of Seats	Cost per Seat	Cost for 1st Year	Cost for 2nd Year	Cost for 3rd Year	Cost for 4th Year	Cost for 5th Year	Tax %	Tax Amt.	Total
1	Communication Officers (CO)	625									

#	Description	No of Seats	Cost per Seat	Cost for 1st Year	Cost for 2nd Year	Cost for 3rd Year	Cost for 4th Year	Cost for 5th Year	Tax %	Tax Amt.	Total
										Sub-total (K1) (in INR)	

#	Description	Unit Rate	Numbers	Cost for 1st Year	Cost for 2nd Year	Cost for 3rd Year	Cost for 4th Year	Cost for 5th Year	Tax %	Tax Amt.	Total
1	CO - Team Leader		41								
2	CO - Team Manager		6								
3	CO - Manager		2								
4	Project Head		1								
5	CO QA - Quality Auditor		21								
6	CO TQL / QAM - Quality team Leader		3								
7	Quality Manager		1								
8	BPM - Business Process Manager		1								
9	RTA - Rea time Analyst		18								
10	CO: MIS executive		6								
11	MIS - RTA Assistant Manager		1								
12	Documentation Specialist		1								
13	Others										
										Sub-total (K2) (in INR)	
										Total Cost (J) (in INR) = K1 + K2	

7.12 Table L: Financial format - Technical Manpower for O&M Phase

#	Description	Unit Rate	Min. No. of Units	Year 1 Cost	Year 2 Cost	Year 3 Cost	Year 4 Cost	Year 5 Cost	Tax %	Tax Amt.	Total
1	Project Manager		1								
2	Solution Architect (DC, DR)		1								
3	Solution Architect (Applications)		1								
4	Solution Architect (Network)		1								
5	Solution Architect (Information Security)		1								
6	Database Architect or Modeler		1								
7	Database Administrator*		4								
8	System Administrator*		4								
9	Network Administrator*		4								
10	CAD Expert (from OEM)		1								
11	GIS Expert (from OEM)		1								
12	Telephony & ACD expert (from OEM)		1								
13	Cloud Architect		1								
14	Application Developer		2								
15	Master Trainer		1								

#	Description	Unit Rate	Min. No. of Units	Year 1 Cost	Year 2 Cost	Year 3 Cost	Year 4 Cost	Year 5 Cost	Tax %	Tax Amt.	Total
16	GIS Data Support Staff		1								
17	SOC Expert*		4								
18	VAPT Expert*		4								
19	IT Security Manager*		8								
20	IT Helpdesk Staff (2999) *		12								
21	DC support Staff*		4								
22	DR Support Staff		1								
23	IT Support staff at Lucknow*		30								
24	IT Support Staff at OMC Ghaziabad*		6								
25	IT Support staff at OMC Prayagraj*		6								
26	Application support staff - Website, HRMS and other app.		4								
27	District technical Support Team		78								
28	Others										
										Total (L) (in INR)	

7.13 Table M: Financial format – Miscellaneous Items

#	Description	Unit Rate	Min. No. of Units	CAPEX (if any)	OPEX for 1st Year	OPEX for 2nd Year	OPEX for 3rd Year	OPEX for 4th Year	OPEX for 5th Year	Tax %	Tax Amt.	Total
1	Dish TV Connection for Television		23									
2	Printing charges at NexGen UP 112 (50,000 pages approx. per month)		1 lot									
3	Miscellaneous like cabling, Patch panel etc.		1 lot									
4	Security Assessment Charges		1 lot									
5	CCTV cameras		100									
6	Application hosting charges on play store and apple store		1 lot									
6	Website ssl certification charges		1 lot									
7	Others											
											Total (M) (in INR)	

7.14 Table N: Financial format: Training

#	Description	Unit Rate	Min. No. of Units	Year 1 Cost	Year 2 Cost	Year 3 Cost	Year 4 Cost	Year 5 Cost	Tax %	Tax Amt.	Total
1	Trainer for Training of trainer (ToT)- Cost Includes lodging,		5								

#	Description	Unit Rate	Min. No. of Units	Year 1 Cost	Year 2 Cost	Year 3 Cost	Year 4 Cost	Year 5 Cost	Tax %	Tax Amt.	Total
	boarding, TA, DA etc.										
2	Trainers at district location-Cost Includes lodging, boarding, TA, DA etc.		125								
										Total (N) (in INR)	

8 Payment Terms

8.1 Payment Milestone

The payment milestones have been defined separately for eight different components required in this project. Explanations for each of these are given below. The MSI is required to obtain prior approval of the ITECCS before placement of orders to the OEMs/service providers. Payment terms are associated with goods and services rendered with quantities pre-approved by the ITECCS (the quantities mentioned in RFP are indicative numbers; actual numbers could vary in some cases). The warranty/AMC of goods and services rendered after at a date later than initial date would require additional warranty for differential period.

8.2 Capex for implementation of NexGen112

All the procurement of hardware and software for upgradation, installation, migration, integration for the implementation of the project and for next 2 years from the date of system acceptance will be paid under this category. The payment will be made as under:

S. No.	Milestone	Payment
1.	Supply & Installation at respective sites	40% of CAPEX1
2.	Migration, upgrades, UAT and System Acceptance	40% of CAPEX1
3.	System Acceptance + 6 months	10% of CAPEX1
4.	System Acceptance + 12 months	10% of CAPEX1

Note: Please refer Section 7 "Financial Format" for the components under CAPEX 1

8.3 Capex during O&M of NexGen112

All the procurement of hardware and software for upgradation and installation for the components of the project during last 3 years of O&M stage will be paid under this category. The payment will be made as under:

S. No.	Milestone	Payment
1.	Supply & Installation	40% of CAPEX2
2.	Migration, upgrades, successful UAT	40% of CAPEX2
3.	Successful UAT + 6 months	10% of CAPEX2
4.	Successful UAT + 12 months	10% of CAPEX2

Note: Please refer Section 7 "Financial Format" for the components under CAPEX 2

8.4 Technical Manpower at UP112 HQ at Lucknow, OMC sites and other Field Locations

All the Technical manpower deployed by the MSI as per the requirements during operation and maintenance of NexGen UP112 would be paid in this category. The MSI will be paid as below:

Sl. No.	Head	Payment
1.	Charges of Technical manpower deployed by MSI	The Monthly cost of the deployed Manpower based on attendance of the individual personnel in designated office as per clause 4.28.7 of Section 4: Scope of Work.

Note: Please refer Section 7 "Financial Format" for the details of Technical Manpower

8.5 Contact Centre Manpower at UP112 HQRS, Lucknow and OMC sites

All the manpower to manage Contact Centre at NexGen UP112 including OMCs would be paid in this category. The MSI will be paid as below:

Sl. No.	Head	Payment
1.	Charges of Communication staff deployed by MSI	The Monthly cost of the deployed Communication Staff based on attendance

Note: Please refer Section 7 "Financial Format" for the details of Technical Manpower

Monthly invoices along with supporting documents to be submitted by the MSI in ITECCS accounts department for clearance

8.6 Network

Bandwidth cost of connecting all sites including DC, DRC, UP112 HQ., OMCs, other field locations and Telecom Services at PRVs would be paid under this category. Payment for network bandwidth for links connecting two active components could be claimed after establishment of links and activation of linked components. Payment for SIP channels would also be paid in similar manner. The SIM charges for the devices in PRVs would also be paid similarly after activation of the services as per plan purchased by ITECCS. The charges for the same will be paid as below:

S. No.	Milestone	Payment

1.	Network services of Network bandwidth between sites (DC, DRC, UP112 HQ., OMCs, and other field locations). This is based on actual commissioned and functional links.	Quarterly payment of the actual bandwidth charges
2.	Recurring SIM charges for the devices in PRVs.	Quarterly payment of the rental charges as per plan opted and as per actual bill from TSP

Note: Please refer Section 7 "Financial Format" for the details of Network components and services under this category

8.7 Capacity Building and Training

For the continuous delivery of the training by the MSI will be paid under this category. The MSI will be paid as below:

S. No.	Milestone	Payment
1.	Satisfactory delivery of the training to batch in the quarter.	The Monthly cost of the deployed Trainers based on attendance duly verified by the respective district or UP HQRS

Note: Please refer Section 4.29 of the detailed Scope of work for Capacity Building and Training and Section 7 "Financial Format" for services covered in this category

8.8 AMC charges

AMC/ maintenance of the UP112 system will be paid in this category: The MSI will be paid as below:

S. No.	Milestone	Payment
1.	AMC/warranty, regular upgrades, security and operation of the all the system of UP112 including Hardwar, Software, IT/Non-IT components, etc.	Quarterly payment of the AMC charges

Note: Please refer Section 7 "Financial Format" for the AMC charges under this category

8.9 Integration with other system

Any integration with other system will be paid in this category: The MSI will be paid as below:

S. No.	Milestone	Payment
1.	Supply & Installation	40% of Integration Cost

S. No.	Milestone	Payment
2.	Migration, updates, UAT and System Acceptance	40% of Integration Cost
3.	Commissioning of the integration + 6 months	10% of Integration Cost
4.	Commissioning of the integration + 12 months	10% of Integration Cost

Note: Please refer clause 4.27.10 "Integration with Other Agencies" of Scope of Work and refer Section 7 "Financial Format" for the Integration charges under this category

8.10 Other Payment terms and conditions

8.10.1 Payment will be made after penalty calculation as described in section 6 and approved by ITECCS. ITECCS reserves the right to validate the credentials of the invoice and supporting documents.

8.10.2 In the event of the Bidder's failure to supply the solution/ equipment on timelines specified in this RFP or to submit any document necessary for project requirement, the ITECCS may at its discretion withhold payment till the fulfilment of the requirements.

8.10.3 Any shifting or addition of the Field Location will be paid as below

a. Capex cost of the components installed in additional location will be paid on the same price as quoted by MSI in commercial bid.

b. In case of shifting the field location within 200 mtr/ within same premises or building, no additional shifting charges will be paid to MSI.

c. In case of shifting the field location more than 200 mtr / within same premises in same city, additional shifting charges will be paid to MSI as per price quoted by MSI in commercial bid.

d. In case of shifting the field location to be shifted to another city, additional shifting charges will be paid to MSI as per price quoted by MSI in commercial bid.

8.10.4 In case of any extension of the contract as provisioned in clause 5.10 of this RFP, the MSI will be paid as below:

a. For the replacement of any component or services declared EoL or EoS, will be paid to MSI upfront at the price of commercial bid of MSI or price discovered by ITECCS through market survey whichever is economical and to the best interest of ITECCS.

b. The AMC charge and Bandwidth charges will be paid quarterly on the same

price of 5th year as quoted by MSI in commercial bid.

c. The payment for manpower will be paid monthly on the same price as quoted by MSI in commercial bid for the last year of project i.e. 5th year.

d. The payment for training will be paid quarterly on the same price as quoted by MSI in commercial bid for the last year of project i.e. 5th year.

8.10.5 The MSI will have to complete the implementation as per mentioned timelines, failing to do so the ITECCS may apply liquidated damages as per clause 6.4.

9 Annexures

Sl No	Annexure No	Annexure description
1	Annexure 1	Earnest Money Deposit Form
2	Annexure 2	Declaration of Non-Blacklisting
3	Annexure 3	Technical Bid Checklist
4	Annexure 4	Technical Bid Letter
5	Annexure 5	Company Profile
6	Annexure 6	Prior Experience
7	Annexure 7	Credential Format
8	Annexure 8	Project Plan
9	Annexure 9	Manpower Plan
10	Annexure 10	Summary of Resources
11	Annexure 11	Statement of Deviations from Schedule of Requirements
12	Annexure 12	Manufacturer's Authorization Form
13	Annexure 13	Anti-Collusion Certificate
14	Annexure 14	Financial Bid Letter
15	Annexure 15	Performance Bank Guarantee
16	Annexure 16	Non-Disclosure Agreement
17	Annexure 17	Consortium Agreement
18	Annexure 18	Format for Power of Attorney to Authorize Signatory
19	Annexure 19	Format for Power of Attorney for Prime Member of Consortium
20	Annexure 20	Change Control Note
21	Annexure 21	Form of Agreement
22	Annexure 22	Integrity Pact (IP)
23	Annexure 23	Format for affidavit for OEM claiming benefit under Make in India Policy
24	Annexure 24	Format for Tripartite Agreement
25	Annexure 25	Application wise user estimations - Concurrent User Category
26	Annexure 26	Application wise user estimations - Application Category
27	Annexure 27	List of Locations
28	Annexure 28	List of POIs and layers
29	Annexure 29	List of Consumables
30	Annexure 30	Preventive Maintenance Schedule
31	Annexure 31	Functional Requirement Specifications
32	Annexure 32	Technical Requirement Specifications

9.1 Annexure 1: Earnest Money Deposit Form

To,

ADG, UP112
UP112 HQRS
112 Bhawan
Shaheed path, Lucknow
Uttar Pradesh

Whereas M/s <<Name of Bidder>>, a company incorporated under the <<Act>>, its registered office at …….. or (hereinafter called 'the Bidder') has submitted its Proposal dated ---------- for "**Request for Proposal for Selection of Master System Integrator (MSI) for Technology implementation, Operationalization and Maintenance of Statewide NexGen UP112 Project"**

KNOW ALL MEN by these presents that WE <<Name of Bank>> of ---------- ---------- having our registered office at ---------- ---------- ---------- (hereinafter called "the Bank") are bound unto the **ITECCS UP POLICE** (hereinafter called "the Client") in the sum of Rs. 20 crores (Rupees Twenty Crores) for which payment well and truly to be made to the said Client, the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this ---------- day of ----------2016

THE CONDITIONS of this obligation are:

1. If the Bidder withdraws its bid during the period of bid validity specified by the Bidder in the Bid
2. If the Bidder, having been notified of the acceptance of its Proposal by the Client during the period of validity of Proposal, bidder:
   - withdraws his participation from the Proposal during the period of validity of Proposal document.
   - fails to extend the validity if required and as requested or
   - fails to produce Performance Bank Guarantee in case of award of tender within 15 days of award of LOI or awarding contract whichever is earlier

We undertake to pay to the Client up to the above amount upon receipt of its first written demand, without the Client having to substantiate its demand, provided that in its demand the Client will note that the amount claimed by it is due to it owing to the occurrence of one or any or a combination of the above conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to the period of bid validity and its validity should be extensible to 90 days beyond the bid validity date. Any demand in respect thereof should reach the Bank not later than the above date.

(Authorized Signatory of the Bank)

9.2 Annexure 2: Declaration of Non-Blacklisting

Declaration for Prime Bidder:

Please provide the declaration on letter head

{Place}
{Date}

To,

Ref: RFP Ref No: _____

Subject: Self Declaration of not been blacklisted in response to the Request for Proposal for Selection of Master System Integrator (MSI) for Technology implementation, Operationalization and Maintenance of Statewide NexGen UP112 Project

Dear Sir,

We confirm that our company or firm, _____, is currently not blacklisted in any manner whatsoever by any of the State or UT and / or Central Government in India on any ground including but not limited to indulgence in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice.

(Signature of the Prime Bidder)

Printed Name

Designation

Seal

Date:
Place:
Business Address:

Declaration for Consortium Member:

{Place}
{Date}

To,

Ref: RFP Ref No: _____

Subject: Self Declaration of not been blacklisted in response to the Request for Proposal for Selection of Master System Integrator (MSI) for Technology implementation, Operationalization and Maintenance of Statewide NexGen UP112 Project

Dear Sir,

We confirm that our company or firm, _____, is currently not blacklisted in any manner whatsoever by any of the State or UT and / or Central Government in India on any ground including but not limited to indulgence in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice.

(Signature of the Consortium Member)

Printed Name

Designation
Seal
Date:
Place:
Business Address:

9.3 Annexure 3: Technical Bid Checklist

S. No.	Checklist Items	Compliance (Yes or No)	Page No. and Section No. in proposal
1.	Technical Bid Letter		
2.	Credential summary		
3.	Detailed credentials		
4.	Detailed proposed solution		
5.	Proposed CVs		
6.	Statement of Deviation		
7.	Breakdown of cost components without mentioning cost		

9.4 Annexure 4: Technical Bid Letter

Date: **<< dd - mm - yyyy >>**

ADG, UP112
UP112 HQRS
112 Bhawan
Shaheed path, Lucknow
Uttar Pradesh

Sir,

Sub: Request for Proposal for Selection of Master System Integrator (MSI) for Technology implementation, Operationalization and Maintenance of Statewide NexGen UP112 Project

Ref: RFP No. **<<>>** dated **<< dd - mm - yyyy >>**

I (in case of single bidder) or We, <<name of the undersigned Bidder and consortium members>>, having read and examined in detail all the bidding documents in respect of "**Request for Proposal for Selection of Master System Integrator (MSI) for Technology implementation, Operationalization and Maintenance of Statewide NexGen UP112 Project"** do hereby propose to provide our services as specified in the bidding proposal submitted by us.

We declare that all the services shall be performed strictly in accordance with the RFP documents except for the variations, assumptions and deviations, all of which have been detailed out exhaustively in the format provided for statement of deviation, irrespective of whatever has been stated to the contrary anywhere else in our Proposal.

We confirm that the information contained in this response or any part thereof, including its exhibits, and other documents and instruments delivered or to be delivered to "ITECCS UP Police" is true, accurate, verifiable and complete. This response includes all information necessary to ensure that the statements therein do not in whole or in part mislead the department in its evaluation process. We also confirm that we shall not attract conflict of interest in principle.

We hereby declare that in case the contract is awarded to us, we shall submit the contract Performance bank guarantee in the form prescribed at Clause <<xxx>> of Section <<>> of the RFP.

We hereby declare that our bid is made in good faith, without collusion or fraud and the information contained in the bid is true and correct to the best of our knowledge and belief.

We understand that our bid is binding on us and that you are not bound to accept a Bid you receive. This proposal is valid for 120 days after opening of technical bid. We shall extend the validity of the bid if required by "ITECCS UP Police".

Thanking you,
Yours sincerely,

(Signature of the Prime Bidder)

Printed Name
Designation

Seal

Date:
Place:
Business Address:

9.5 Annexure 5: Company Profile

A. Brief company profile (required for both bidder and consortium member)

Sl. No.	Particulars	Description or Details
A.	Name of Bidder	
B.	Legal status of Bidder (company, Pvt. Ltd., LLP etc.)	
C.	Main business of the Bidder	
D.	Registered office	
E.	Incorporation date and number	
F.	Service Tax number	
G.	VAT number	
H.	PAN details	
I.	Primary Contact Person (Name, Designation, address, mobile number, fax, email)	
J.	Secondary Contact Person (Name, Designation, address, mobile number, fax, email)	
K.	EMD details	
L.	Demand Draft details (DD No., date, Bank)	

B. Certificate of Incorporation (required for both bidder and consortium member)

Provide the Certificate of Incorporation of the company.

C. Financial Turnover

The financial turnover of the company is provided as follows:

	2019 – 20	2020 – 21	2021 – 22
Annual Turnover			
Net worth			

Copy of audited financial statements or declaration from the appointed statutory auditor to be provided as proof of the financial turnover

D. Certifications (required for bidder or consortium member)

Provide copy of valid certification for SEI CMM or CMMi maturity Level 5, ISO 27001 or ISO 9001

9.6 Annexure 6: Prior Experience

Credential Summary

#	Project Name	Client Name	Client Type	Project Value (in INR)	Project Components	Documentary evidence provided (Yes or No)	Project Status (Completed or Ongoing or Withheld)
1							
2							
3							
4							
5							
6							
7							

- Client type – Indicate whether the client is Government or PSU or Private
- Project Components – Indicate the major project components setting up of case record management application, contact centre establishment, Application development, Maintenance, Hardware procurement and deployment, DC setup and maintenance, Facility management services, provisioning manpower, IT support and maintenance
- Documentary evidence provided – Indicate the documentary evidence provided with the detailed project credential like work order or purchase order or completion certificate or letter of appointment
- Project Status – Completed (date of project completion) or Ongoing (project start date)

9.7 Annexure 7: Credential Format

Prime Bidder or Consortium member is requested to furnish the credentials in the following format for both Pre-qualification and Technical criterion. All credentials should be followed by relevant documentary proof.

Name of the Work and Location	
Client's Name and Complete Address	
Narrative description of project	
Contract Value for the bidder (in INR) (mandatory)	
Date of Start (mandatory)	
Date of Completion	
Activities undertaken by prime bidder or consortium member	

9.8 Annexure 8: Project Plan

A **Detailed Project Plan** covering break-up of each phase into the key activities, along with the start and end dates must be provided as per format given below.

Activity-wise Timelines							
Sl. No.	**Item of Activity**	**Month wise Program**					
		1	2	3	4	5	…
	Project Plan						
1	Activity 1						
1.1	Sub-Activity 1						
1.2	Sub-Activity 2						
2							
2.1							
2.2							
3							
3.1							
4							

Note: The above activity chart is just for the purpose of illustration. Bidders are requested to provide detailed activity and phase wise timelines for executing the project with details of deliverables and milestones as per their proposal.

9.9 Annexure 9: Manpower Plan

Manpower distribution									
S. No.	**Manpower**	**Month wise time to be spent by each personnel (in days)**						**Total**	**Onsite or offsite**
		Month 1	Month 2	Month 3	Month 4	Month 5	…		
1	Project Director								Onsite
									Onsite
2	Project Manager								Onsite
									Onsite
3	Solution Architect (DC, DR)								Onsite
									Onsite
4	Solution Architect (Applications)								Onsite
									Onsite
5	Solution Architect (Network)								Onsite
									Onsite
6	Solution Architect (Information Security)								Onsite
									Onsite
7	Database Architect or Modeler								Onsite
									Onsite
8	Database Administrator								Onsite
									Onsite
9	System Administrator								Onsite
									Onsite
10	Network Administrator								Onsite
									Onsite
11	Business Analyst								Onsite
									Onsite
12	CAD Expert (from OEM of the proposed product)								Onsite
									Onsite
13									Onsite

Manpower distribution									
S. No.	**Manpower**	**Month wise time to be spent by each personnel (in days)**						**Total**	**Onsite or offsite**
		Month 1	Month 2	Month 3	Month 4	Month 5	…		
	GIS Expert (from OEM of the proposed product)								Onsite
14	Telephony & ACD expert (from OEM of the proposed product)								Onsite
									Onsite
15	Radio over IP specialist (from OEM of the proposed product)								Onsite
									Onsite
16	Cloud Architect								Onsite
									Onsite
17	Monitoring center configuration and customization expert								Onsite
									Onsite
18	Application Developers								Onsite
									Onsite
19	QA Manager								Onsite
									Onsite
20	Test Analysts								Onsite
									Onsite
21	Master Trainer								Onsite
									Onsite
22	Documentation Specialist								Onsite
									Onsite
23	GIS Data Support Staff								Onsite
									Onsite

Manpower distribution									
S. No.	**Manpower**	**Month wise time to be spent by each personnel (in days)**						**Total**	**Onsite or offsite**
		Month 1	Month 2	Month 3	Month 4	Month 5	…		
24	Geo Fencing Staff								Onsite
									Onsite
25	Process and Compliance Manager								Onsite
									Onsite
26	SOC Analyst								Onsite
									Onsite
27	VAPT Analyst								Onsite
									Onsite
28	Build and Release Manager								Onsite
									Onsite
29	IT Security Manager								Onsite
									Onsite
30	IT Helpdesk Staff								Onsite
									Onsite
31	DC support Staff								Onsite
									Onsite
32	DR Support Staff								Onsite
									Onsite
33	FMS staff at UP 112								Onsite
									Onsite
34	FMS Staff at OMC Agra								Onsite
									Onsite
35	FMS staff at OMC Varanasi								Onsite
									Onsite
36	Others								
							Total		

Note: The above chart is just for the purpose of illustration. Bidders are requested to provide detailed manpower distribution with clearly stating offsite and onsite deployment, part time or full-time deployment and other details as per their proposal.

9.10 Annexure 10: Summary of Resources

Sl. No.	Name of the Resource	Proposed Role	Higher Qualification	Basic Qualification (E.g. B.Sc. or B.E. or Diploma)	Certifications (ex. PMI or ITIL)	Number of projects in (Dial 100/112 or emergency response)	Total Experience (in years)
1.							
2.							
3.							

Detailed CV:

1	Name:				
1.	**Proposed position or role**	(only one candidate shall be nominated for each position)			
2.	**Date of Birth**		**Nationality**		
3.	**Education**	**Qualification**	**Name of School or College or University**	**Degree Obtained**	**Date Attended**
4.	**Years of experience**				
5.	**Areas of Expertise and no. of years of experience in this area**	(as required for the Profile) ▶			
6.	**Certifications and Trainings attended**	▶			

1	Name:	
7.	**Employment Record**	<table><tr><th>Employer</th><th>Position</th><th>From</th><th>To</th></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td></tr></table> [Starting with present position and last 2 firms, list in reverse order, giving for each employment: dates of employment, name of employing organization, positions held.]
8.	**Detailed Tasks Assigned**	(List all tasks to be performed under this project) ▶
9.	**Relevant Work Undertaken that Best Illustrates the experience as required for the Role**)	

Project 1	
Name of assignment	
Year	
Location	
Employer	
Main project features	
Position held	
Activities performed	

Project 2	
Name of assignment	
Year	
Location	
Employer	
Main project features	
Position held	
Activities performed	

9.11 Annexure 11: Statement of Deviations from Schedule of Requirements

Date: dd - mm - yyyy
To
ADG, UP112
UP112 HQRS
112 Bhawan
Shaheed path, Lucknow
Uttar Pradesh
Sir,
We are providing the deviations from the requirements of RFP document **No <<>> dated <<dd - mm - yyyy>>.** These deviations, assumptions and variations are exhaustive. Except these deviations, assumptions and variations, all other Terms and Conditions of the RFP are acceptable to us.

1.1.1 Deviations in Scope of Work

1.1.2

S. No.	Reference of RFP Volume Number, Clause No. and Page. No	Deviation in the Proposal	Brief Reasons

1.1.3 Deviation in Terms and Conditions

1.1.4

S. No.	Reference of RFP Volume Number, Clause No. and Page. No	Deviation in the Proposal	Brief Reasons

Yours sincerely,

(Signature of the Authorized Representative)

Printed Name
Designation

Seal

Place:
Business Address:

9.12 Annexure 12: Manufacturer's Authorization Form

Note: This letter of authority should be on the letterhead of the manufacturing concern and should be signed by a person competent and having the power of attorney to bind the manufacturer**.**

To, Date:

ADG, UP112
UP112 HQRS
112 Bhawan
Shaheed path, Lucknow
Uttar Pradesh

Subject: Manufacturer's Authorization Form

Reference: RFP No: _____ Dated: _____ for **Selection of Master System Integrator (MSI) for Technology implementation, Operationalization and Maintenance of Statewide NexGen UP112 Project**

.

We_____ (Name of the OEM) who are established and reputable manufacturers of _____ (List of Goods) having factories or product development centre at the locations _____ or as per list attached, do hereby authorize. _____ (Name and address of the Bidder) to bid, negotiate and conclude the contract with you against RFP No. _____Dated _____for the above goods manufactured or developed by us.

We hereby extend, our warranty for the hardware goods supplied by the bidder and / or the maintenance or support services for software products against this invitation for bid by _____ (Name of the Bidder)

During the period of 8 years from the date of system acceptance in case the bidder fails to provide the necessary service, we will be obliged to provide the same, at no extra cost.

All the proposed equipment (except and otherwise) should not be declared End-of-Support by the OEMs for next 8 years and should not be end of production for next two years from the date of bid submission.

Thanking you,
Yours faithfully,

(Signature)
For and on behalf of: _____ (Name of the OEM)
Authorised Signatory
Name:
Designation:
Place:
Date:

9.13 Annexure 13: Anti-Collusion Certificate

Certificate should be provided by Bidder on letter head

Anti-Collusion Certificate (In case of Single Bidder)

We hereby certify and confirm that in the preparation and submission of our Proposal for **Request for Proposal for Selection of Master System Integrator (MSI) for Technology implementation, Operationalization and Maintenance of State wide NexGen UP112 Project** in Uttar Pradesh against the RFP issued by ITECCS UP Police, We have not acted in concert or in collusion with any other Bidder or other person(s) and also not done any act, deed or thing, which is or could be regarded as anti-competitive. We further confirm that we have not offered nor will offer any illegal gratification in cash or kind to any person or organization in connection with the instant proposal.

(Signature of the Bidder)

Printed Name
Designation

Seal

Date:
Place:
Business Address:

Certificate should be provided by Prime Bidder and on letter head

Anti-Collusion Certificate (In case of Consortium)

We hereby certify and confirm that in the preparation and submission of our Proposal for **Request for Proposal for Selection of Master System Integrator (MSI) for Technology implementation, Operationalization and Maintenance of State wide NexGen UP112 Project** in Uttar Pradesh against the RFP issued by ITECCS UP Police, We have not acted in concert or in collusion with any other Bidder or other person(s) and also not done any act, deed or thing, which is or could be regarded as anti-competitive. We further confirm that we have not offered nor will offer any illegal gratification in cash or kind to any person or organization in connection with the instant proposal.

We also certify that any member of our consortium is not an applicant/ member of any other bid for this RFP.

(Signature of the Prime Bidder)

Printed Name
Designation

Seal

Date:

Place:
Business Address:

s

9.14 Annexure 14: Financial Bid Letter

To

ADG, UP112
UP112 HQRS
112 Bhawan
Shaheed path, Lucknow
Uttar Pradesh

Sir,

Sub**: Request for Proposal for Selection of Master System Integrator (MSI) for Technology implementation, Operationalization and Maintenance of Statewide NexGen UP112 Project**

Ref: RFP No. **<<>> dated << >>**

We, <<name of the undersigned Bidder and consortium members>>, having read and examined in detail all the bidding documents in respect of set up of **Request for Proposal for Selection of Master System Integrator (MSI) for Technology implementation, Operationalization and Maintenance of Statewide NexGen UP112 Project** do hereby propose to provide our services as specified in the bidding proposal submitted by us.

All the prices mentioned in our bid are in accordance with the terms as specified in the bidding documents. This bid is valid for a period of 120 calendar days from the date of issuance of RFP to the bidder.

We have studied the relevant clause(s) in Indian Tax Laws and hereby declare that if any taxes, surcharge, Professional and any other corporate Tax in altercated under the laws, we shall pay the same.

We have indicated in the relevant schedules enclosed, the unit rates on account of payment as well as for price adjustment in case of any increase or decrease from the scope of work under the contract.

We declare that our bid prices are for the entire scope of work as specified in the Scope of Work and bid documents. These prices are attached with our bid as part of the bid.

We hereby declare that in case the contract is awarded to us, we shall submit the contract Performance Bank Guarantee in the form prescribed in clause 2.15 within 15 days of issue of LOI.

We hereby declare that our bid is made in good faith, without collusion or fraud and the information contained in the bid is true and correct to the best of our knowledge and belief.

We understand that our bid is binding on us during the validity period or the extensions thereof and that you are not bound to accept a Bid you receive.
We confirm that no deviations are attached here with this commercial offer.

Thanking you,
Yours sincerely,

(Signature of the Prime Bidder)
Printed Name
Designation
Seal

Date:
Place:
Business Address:

9.15 Annexure 15: Performance Bank Guarantee

Ref: _____ Date _____

Bank Guarantee No. _____

To
XXX
XXX

IN consideration of the **Governor of Uttar Pradesh**, _____ < indicate name and address of UP112 > (hereinafter called "the GoUP") having agreed; to exempt _____ (hereinafter called "Agency") from the demand, under the terms and conditions of an Agreement, dated _____ made between _____ and _____ for _____ (hereinafter called "the said Contract"), of security deposit for the due fulfilment by the said Agency of the terms and conditions contained in the said Agreement, on production of a bank Guarantee for Rs._____ (Rupees _____ only) we, _____ < indicate name of the Bank > (hereinafter referred to as "the Bank") at the request of _____ or Agency or , do hereby undertake to pay to the ITECCS-UP Police an amount not exceeding Rs. _____ against any loss or damage caused to or suffered or would be caused to or suffered by the Government by reason of any breach by the said Agency of any of the terms or conditions contained in the said contract

2. We _____ < indicate name of the Bank > do hereby undertake to pay the amounts due and payable under this guarantee without any demur, merely on a demand from the ITECCS-UP Police stating that the amount claimed is due by way of loss or damage caused to or would be caused to or suffered by the ITECCS-UP Police by reason of breach by the said Agency of any of the terms or conditions contained in the said Contract or by reason of the Agency failure to perform the said Contract. Any such demand made on the bank shall be conclusive as regards the amount due and payable by the Bank under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding Rs. _____

3. We undertake to pay to the ITECCS-UP Police any money so demanded notwithstanding any dispute or disputes raised by the contractor(s) supplier(s) in any suit or proceeding pending before any court or Tribunal relating thereto our liability under this present being absolute and unequivocal. The payment so made by us under this bond shall be a valid discharge of our liability for payment there under and the contractor(s) supplier(s) shall have no claim against us for making such payment.

4. We, _____ <indicate name of the Bank> further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said Contract and that it shall continue to be enforceable till all the dues of the Contract under or by virtue of the said Contract have been fully paid and its claims satisfied or discharged or filed _____ Office or Department _____ certifies that the terms and conditions of the said contract, have been fully and properly carried out by the said Agency and accordingly discharges this guarantee. Unless a demand or claim under this guarantee is made on us in writing on or before the _____ we shall be discharged from all liability under this guarantee thereafter.

5. We, _____ <indicate name of the Bank> further agree with the ITECCS-UP Police that the ITECCS-UP Police shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said Contract or to extend time of performance by the said Agency from time to time or to postpone for any time or from time to time any of the powers exercisable by the ITECCS-UP Police against the said ITECCS-UP Police and to for bear or enforce any of the terms and conditions relating to the said contract and we shall not be relieved from our liability by reason of any such variation or extension being granted to the said agency or for any forbearance, act or commission on the part of the ITECCS-UP Police or any indulgence by the ITECCS-UP Police to the said Agency or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have effect of so relieving us.

6. This guarantee will not be discharged due to the change in the constitution of the Bank or the agency.

7. We, _____ <indicate name of the Bank> lastly undertake not to revoke this guarantee during its currency except with the previous consent of the ITECCS-UP Police in writing.

Date _____

Place _____ Signature _____

Witness _____ Printed name _____

(Bank's common seal)

9.16 Annexure 16: Non-Disclosure Agreement

WHEREAS, we the undersigned Bidder, _____, having our principal place of business or registered office at _____, are desirous of bidding for RFP No. <<>> dated <<DD-MM-YYYY>> "**Selection of Master System Integrator (MSI) for Technology implementation, Operationalization and Maintenance of State wide NexGen UP112 Project**" (hereinafter called the said 'RFP') to the "ITECCS-UP Police", hereinafter referred to as 'GoUP'

and,

WHEREAS, the Bidder is aware and confirms that the GoUP business or operations, information, application or software, hardware, business data, architecture schematics, designs, storage media and other information or documents made available by the GoUP in the RFP documents during the bidding process and thereafter, or otherwise (confidential information for short) is privileged and strictly confidential and or or proprietary to the GoUP,

NOW THEREFORE, in consideration of disclosure of confidential information, and in order to ensure the GoUP grant to the Bidder of specific access to GoUP confidential information, property, information systems, network, databases and other data, the Bidder agrees to all of the following conditions.

It is hereby agreed as under:

1. The confidential information to be disclosed by the GoUP under this Agreement ("Confidential Information") shall include without limitation, any and all information in written, representational, electronic, verbal or other form relating directly or indirectly to processes, methodologies, algorithms, risk matrices, thresholds, parameters, reports, deliverables, work products, specifications, architecture, project information, security or zoning strategies and policies, related computer programs, systems, trend analysis, risk plans, strategies and information communicated or obtained through meetings, documents, correspondence or inspection of tangible items, facilities or inspection at any site to which access is permitted by the GoUP.

2. Confidential Information does not include information which:
   a. the Bidder knew or had in its possession, prior to disclosure, without limitation on its confidentiality;
   b. information in the public domain as a matter of law;
   c. is obtained by the Bidder from a third party without any obligation of confidentiality;
   d. the Bidder is required to disclose by order of a competent court or regulatory authority;
   e. is released from confidentiality with the written consent of the GoUP.

The Bidder shall have the burden of proving hereinabove are applicable to the information in the possession of the Bidder.

3. The Bidder agrees to hold in trust any Confidential Information received by the Bidder, as part of the Tendering process or otherwise, and the Bidder shall maintain strict confidentiality in respect of such Confidential Information, and in no event a degree of confidentiality less than the Bidder uses to protect its own confidential and proprietary information. The Bidder also agrees:

a. to maintain and use the Confidential Information only for the purposes of bidding for this RFP and thereafter only as expressly permitted herein;
b. to only make copies as specifically authorized by the prior written consent of the GoUP and with the same confidential or proprietary notices as may be printed or displayed on the original;
c. to restrict access and disclosure of Confidential Information to their employees, consortium members and representatives strictly on a "need to know" basis, to maintain confidentiality of the Confidential Information disclosed to them in accordance with this clause; and
d. to treat Confidential Information as confidential unless and until GoUP expressly notifies the Bidder of release of its obligations in relation to the said Confidential Information.

4. Notwithstanding the foregoing, the Bidder acknowledges that the nature of activities to be performed as part of the Tendering process or thereafter may require the Bidder's personnel to be present on premises of the GoUP or may require the Bidder's personnel to have access to software, hardware, computer networks, databases, documents and storage media of the GoUP while on or off premises of the GoUP. It is understood that it would be impractical for the GoUP to monitor all information made available to the Bidder's personnel under such circumstances and to provide notice to the Bidder of the confidentiality of all such information.

   Therefore, the Bidder shall disclose or allow access to the Confidential Information only to those personnel of the Bidder who need to know it for the proper performance of their duties in relation to this project, and then only to the extent reasonably necessary. The Bidder will take appropriate steps to ensure that all personnel to whom access to the Confidential Information is given are aware of the Bidder's confidentiality obligation. Further, the Bidder shall procure that all personnel of the Bidder are bound by confidentiality obligation in relation to all proprietary and Confidential Information received by them which is no less onerous than the confidentiality obligation under this agreement.

5. The Bidder shall establish and maintain appropriate security measures to provide for the safe custody of the Confidential Information and to prevent unauthorised access to it.

6. The Bidder agrees that upon termination or expiry of this Agreement or at any time during its currency, at the request of the GoUP, the Bidder shall promptly deliver to the GoUP the Confidential Information and copies thereof in its possession or under its direct or indirect control, and shall destroy all memoranda, notes and other writings prepared by the Bidder or its Affiliates or directors, officers, employees or advisors based on the Confidential Information and promptly certify such destruction.

7. Confidential Information shall at all times remain the sole and exclusive property of the GoUP. Upon completion of the Tendering process and or or termination of the contract or at any time during its currency, at the request of the GoUP, the Bidder shall promptly deliver to the GoUP the Confidential Information and copies thereof in its possession or under its direct or indirect control, and shall destroy all memoranda, notes and other writings prepared by the Bidder or its Affiliates or directors, officers, employees or advisors based on the Confidential Information within a period of sixty days from the date of receipt of notice, or destroyed, if incapable of return. The destruction shall be witnessed and so recorded, in writing, by an authorized representative of the GoUP. Without prejudice to the above the Bidder shall promptly certify to the GoUP, due and complete destruction and return. Nothing contained herein shall in any manner impair rights of the GoUP in respect of the Confidential Information.

8. In the event that the Bidder hereto becomes legally compelled to disclose any Confidential Information, the Bidder shall give sufficient notice and render best effort assistance to the GoUP to enable the GoUP to prevent or minimize to the extent possible, such disclosure. Bidder shall not disclose to a third party any Confidential Information or the contents of this RFP without the prior written consent of the GoUP. The obligations of this Clause shall be satisfied by handling Confidential Information with the same degree of care, which the Bidder applies to its own similar Confidential Information but in no event less than reasonable care.

For and on behalf of:

(BIDDER)

Authorised Signatory
Name:
Designation:

Office Seal:
Place:
Date :

9.17 Annexure 17: Consortium Agreement

DRAFT AGREEMENT EXECUTED BY MEMBERS OF THE CONSORTIUM
[On Non-judicial stamp paper of INR 100 duly attested by notary public]

This agreement entered into this day of [Date] [Month] 2022 at [Place] among _____ _____ (hereinafter referred to as "_____") and having office at [Address], India, as Party of the First Part and _____ _____ (hereinafter referred as "_____") and having office at [Address], as Party of the Second Part and _____ _____ (hereinafter referred as "____") and having office at [Address], as Party of the Third Part.

The parties are individually referred to as Party and collectively as Parties.

WHEREAS ITECCS - UP Police has issued a Request for Proposal (RFP) dated [Date] from the Applicants interested in **Selection of Master System Integrator (MSI) for Technology implementation, Operationalization and Maintenance of Statewide NexGen UP112 Project:**

AND WHEREAS the Parties have had discussions for formation of a Consortium for bidding for the said Project and have reached an understanding on the following points with respect to the Parties' rights and obligations towards each other and their working relationship.

AS MUTUAL UNDERSTANDING OF THE PARTIES, IT IS HEREBY AGREED AND DECLARED AS FOLLOWS:

i. The purpose of this Agreement is to define the principles of collaboration among the Parties to:
   - Submit a response jointly to Bid for the "**Selection of Master System Integrator (MSI) for Technology implementation, Operationalization and Maintenance of Statewide NexGen UP112 Project"** as a Consortium.
   - Sign Contract in case of award.
   - Provide and perform the supplies and services which would be ordered by the GoUP pursuant to the Contract.

ii. This Agreement shall not be construed as establishing or giving effect to any legal entity such as, but not limited to, a company, a partnership, etc. It shall relate solely towards the GoUP for **Selection of Master System Integrator (MSI) for Technology implementation, Operationalization and Maintenance of State-wide NexGen UP112 Project"** for and related execution works to be performed pursuant to the Contract and shall not extend to any other activities.

iii. The Parties shall be jointly and severally responsible and bound towards the GoUP for the performance of the works in accordance with the terms and conditions of the BID document, and Contract.

iv. ---------- (Name of Party) shall act as Lead Partner of the Consortium. As such, it shall act as the coordinator of the Party's combined activities and shall carry out the following functions:
   - To ensure the technical, commercial and administrative co-ordination of the work package
   - To lead the contract negotiations of the work package with the GoUP.

- The Lead partner is authorized to receive instructions and incur liabilities for and on behalf of all Parties.
- In case of an award, act as channel of communication between the GoUP and the Parties to execute the Contract

v. That the Parties shall carry out all responsibilities as Developer in terms of the Project Agreement.

vi. That the broad roles and the responsibilities of each Party at each stage of the Bidding shall be as below including % stake in the contract value:

Party A: _____
Party B: _____
Party C: _____

vii. That the Parties affirm that they shall implement the Project in good faith and shall take all necessary steps to see the Project through expeditiously.

viii. The selected bidder shall ensure that all the members of consortium approved under this Contract complies with:
   a. Clause 5.19 (Confidentiality)
   b. Clause 5.34 (Information Security)
   c. Clause 5.28 (Conflict of Interest)

ix. That this agreement shall be governed in accordance with the laws of India and courts in Uttar Pradesh shall have exclusive jurisdiction to adjudicate disputes arising from the terms herein.

In witness whereof the Parties affirm that the information provided is accurate and true and have caused this agreement duly executed on the date and year above mentioned.

(Party of the first part) (Party of the second part) (Party of the third part)

Witness:

i. _____ ____
ii. _____ ____

9.18 Annexure 18: Format for Power of Attorney to Authorize Signatory

POWER OF ATTORNEY

[To be executed on non-judicial stamp paper of the appropriate value in accordance with relevant Stamp Act. The stamp paper to be in the name of the company who is issuing the power of attorney.]

We, M/s._____ (name of the firm or company with address of the registered office) hereby constitute, appoint and authorise Mr. or Ms._____ (Name and residential address) who is presently employed with us and holding the position of _____, as our Attorney to do in our name and our behalf all or any of the acts, deeds or things necessary or incidental to our RFP for the Project _____ (name of the Project), including signing and submission of the RFP response, participating in the meetings, responding to queries, submission of information or documents and generally to represent us in all the dealings with Client or any other Government Agency or any person, in connection with the works until culmination of the process of bidding till the Project Agreement is entered into with _____ (Client) and thereafter till the expiry of the Project Agreement.

We hereby agree to ratify all acts, deeds and things lawfully done by our said Attorney pursuant to this power of attorney and that all acts, deeds and things done by our aforesaid Attorney shall and shall always be deemed to have been done by us.

(Add in the case of a Consortium or Joint Venture)
Our firm is a Member or Lead Member of the Consortium of _____, _____ and _____.

Dated this the _____ day of _____ 2022

(Signature and Name of authorized signatory)
_____

(Signature and Name in block letters of all the remaining partners of the firm Signatory for the Company)

Seal of firm Company

Witness 1: Witness 2:

Notes:

- To be executed by all the members individually.
- The Mode of execution of the power of attorney should be in accordance with the procedure, if any laid down by the applicable law and the charter documents of the executant(s) and when it is so required the same should be under common seal affixed in accordance with the required procedure.

9.19 Annexure 19: Format for Power of Attorney for Prime Member of Consortium

[To be executed on non-judicial stamp paper of the appropriate value in accordance with relevant Stamp Act. The stamp paper to be in the name of the company who is issuing the power of attorney]

Whereas _____ has invited RFP response for _____ (Name of the Project)
Whereas the Members of the Consortium comprising of M/s._____, M/s._____, M/s._____ and M/ s._____ (the respective names and addresses of the registered offices to be given) are interested in bidding for the Project and implementing the same in accordance with the terms and conditions contained in the RFP Documents.

Whereas it is necessary for the members of the Consortium to designate one of them as the lead member with all necessary power and authority to do, for and on behalf of the Consortium, all acts, deeds and things as may be necessary in connection with the Consortium's RFP response for the Project.

NOW THIS POWER OF ATTORNEY WITNESSETH THAT
We, M/ s._____ and M/s _____ and M/s_____ hereby designate M/s. _____ being one of the members of the Consortium, as the lead member of the Consortium, to do on behalf of the Consortium, all or any of the acts, deeds or things necessary or incidental to the Consortium's RFP response for the Project, including submission of the RFP response, participating in meetings, responding to queries, submission of information or documents and generally to represent the Consortium in all its dealings with Client or any other Government Agency or any person, in connection with the Project until culmination of the process of bidding till the Project Agreement is entered into with Client and thereafter till the expiry of the Project Agreement.

We hereby agree to ratify all acts, deeds and things lawfully done by our said Attorney pursuant to this power of attorney and that all acts, deeds and things done by our aforesaid Attorney shall and shall always be deemed to have been done by us or Consortium.

Dated this the _____ day of _____ 2022

_____
(signature)

_____
(Name in Block Letter of Executant) [seal of Company]

Witness 1 Witness 2

Notes:
- To be executed by all the members individually, in case of a Consortium.

The Mode of execution of the power of attorney should be in accordance with the procedure, if any laid down by the applicable law and the charter documents of the executant(s) and when it is so required the same should be under common seal affixed in accordance with the required procedure.

9.20 Annexure 20: Change Control Note

Change Control Note	**CCN Number:**
Part A: Initiation	
Title:	
Originator:	
Sponsor:	
Date of Initiation:	
Details of Proposed Change	
(To include reason for change and appropriate details/specifications. Identify any attachments as A1, A2, and A3 etc.)	
Authorized by GoUP	Date:
Name:	
Signature:	
Received by the Bidder	Date:
Name:	
Signature:	
Change Control Note	**CCN Number:**
Part B : Evaluation	
(Identify any attachments as B1, B2, and B3 etc.) Changes to Services, payment terms, payment profile, documentation, training, service levels and component working arrangements and any other contractual issue.	
Brief Description of Solution:	
Impact:	

Deliverables:	
Timetable:	
Charges for Implementation: (including a schedule of payments)	
Other Relevant Information: (including value-added and acceptance criteria)	
Authorized by the Bidder	**Date:**
Name:	
Signature:	
Change Control Note	**CCN Number :**
Part C : Authority to Proceed	
Implementation of this CCN as submitted in Part A, in accordance with Part B is: (tick as appropriate)	
Approved **Rejected** **Requires Further Information** (as	

follows, or as Attachment 1 etc.)	
For GoUP and its nominated agencies	**For the Bidder**
Signature	Signature
Name	Name
Title	Title
Date	Date

9.21 Annexure 21: Form of Agreement

This Agreement is made on the …….day of……2022,

BETWEEN

The Governor of Uttar Pradesh through Sri……,……..

(Deputy/Special) Secretary, Home Department, Government of Uttar Pradesh (hereinafter referred as "GoUP" which expression shall unless repugnant to the Context thereafter include his Successor in office) of the **ONE PART;**

AND

…….a Company/……..…..registered under the Companies Act, 1956 and having its registered office at …….. through Sri……..,……(hereinafter referred as "Successful Bidder" which expression shall unless repugnant to the Context thereafter include his successor in office and assigns) of the **OTHER PART**.

NOW, THEREFORE, IT IS HEREBY AGREED between the parties as follows:

a. The GoUP has accepted the tender of the Prime Bidder for the provision and execution of the said works for the sum of ……..upon the terms laid out in this RFP.
b. The Bidder hereby agrees to provide Services to GoUP, conforming to the specified Service Levels and conditions mentioned
c. The following documents attached hereto shall be deemed to form an integral part of this Agreement:

Complete Request for Proposal (RFP) Document	*All sections of the RFP*
Break-up of cost components	*Prime Bidder's Commercial Proposal*
The GoUP Letter of Intent dated <<>>	*To be issued later by the GoUP*
The Prime Bidder's Letter of acceptance dated <<>>	*To be issued later by the GoUP*
Bid submitted by the Prime Bidder as per file No. <<>>	

d. The mutual rights and obligations of the "GoUP" and the Prime Bidder shall be as set forth in the Agreement, in particular:
    - the Prime Bidder shall carry out and complete the Services in accordance with the provisions of this Agreement; and
    - the "GoUP" shall make payments to the Prime Bidder in accordance with the provisions of this Agreement.

NOW THESE PRESENTS WITNESS and the parties hereto hereby agree and declare as follows, that is to say, in consideration of the payments to be made to the Prime Bidder by the GoUP as hereinafter mentioned, the Prime Bidder shall deliver the services for the said works and shall do and perform all other works and things in the Contract mentioned or described or which are implied there from or there in respectively or may be reasonably necessary for the completion of the said works within and at the

times and in the manner and subject to the terms, conditions and stipulations mentioned in the said Contract.

AND in consideration of services and milestones, the GoUP will pay to the Prime Bidder the said sum of ……or such other sums as may become payable to the Prime Bidder under the provisions of this Contract, such payments to be made at such time and in such manner as is provided by the Contract.

IN WITNESS WHEREOF the parties hereto have signed this deed hereunder on the dates respectively mentioned against the signature of each.

Signed	Signed
Name : _____	Name : _____
Designation : _____	Designation : _____
Date :	Date :
Place :	Place :
in the presence of :	**in the presence of :**
Signed	Signed
Name : _____	Name : _____
Designation : _____	Designation : _____
Date :	Date :
Place :	Place :

9.22 Annexure 22: Integrity Pact (IP)

(To be given on letter head of the Supplier/Original Equipment Manufacturer (OEM), as the case may be, duly signed by the authority having legal power of attorney to bind the firm/company).

1. This Integrity pact (hereinafter called the IP) is a fidelity agreement between the Supplier (which include all their employees, agents, consultants and also their OEM, if any) who are registered/seeks registration or awarded/seeks Contract(s)/Rate Contract(s) (RCs) on one hand and State Purchase organization (SPO) or any other procuring entity (PE) (hereinafter called the SPO/PE which include all its employees/officials/officers working as Public Authority) on the other.

2. Under this IP, it has been agreed, accepted and undertaken to use, practice and observe all the best, clean, ethical, honest and legal means and behaviour maintaining complete transparency and fairness in all activities concerning Registration, Bidding, Contracting/Rate Contracting and performance thereto. Neither the Supplier nor the Public Authority which include indenters, Purchase and inspection officials of SPO/PE shall have conflict of interest of any kind whatsoever nor demand or pay or accept any illicit gratification/bribe or hospitality or consideration/favour of any kind whatsoever and shall not use any corrupt practices including fraud, misrepresentation, misleading or forged/false documents, concealing/suppressing facts, undue pressures or influences from anyone (written or verbal/telephonic), bribery, rigging, cartelization, collusion, which are not limited to, but also include the following:

   (a) Collusive bidding: Collusive bidding can take form of an agreement among tenderers to divide the market, set prices, or limit production. It can involve 'wage fixing, kickbacks, or misrepresenting the independence of the relationship between the colluding parties'. In legal terms all acts affected by collusion are considered void.

   (b) Bid rotation: In bid-rotation scheme conspiring tenderers continue to bid, but they agree to take turns being the winning (i.e. lowest qualifying) Bidder. The way in which bid-rotation agreements are implemented can vary.

   (c) Cover Bidding: Cover (also called complementary, courtesy, token or symbolic) bidding occurs when individuals or firms/companies agree to submit bids that involve at least one of the following:

      i A competitor agrees to submit a bid that is higher than the bid of the designated winner,

      ii A competitor submits a bid that is known to be too high to be accepted, or

      iii A competitor submits a bid that contains special terms that are known to be unacceptable to the Buyer.

(d) Bid suppression: Bid-suppression schemes involve agreements among competitors in which one or more firms/companies agree to refrain from bidding or to withdraw a previously submitted bid so that the designated winner's bid will be accepted.

(e) Market allocation: Competitors carve up the market and agree not to compete for certain, customers or in certain geographic areas. Competing firms/companies may, for example, allocate specific customers or types of customers to different firms/companies, so that competitors will not bid (or will submit only a cover bid) on Contracts offered by a certain class of potential customers which are allocated to a specific firm/company etc.

3. The party hereby agrees that he will not indulge in any such activity and will inform SPO/PE if any such activity is on. The party further agrees that he will not give bribe, speed money and gifts to any public official of SPO/PE and will not commit any offence in contravention of relevant IPC/PC Act or any Indian law in force.

4. The party hereby agrees that while canvassing order, they will not provide any inducement of the indenter, whether directly or indirectly including cash and non-cash both pre, during and post procurement action and inform the SPO/PE if any such event is unfolding for which SPO/PE on assessment of the issue will refer the matter to the concerned administrative authority.

5. In case of failure or default in terms of this IP the Public Authority will be subjected to actions prescribed under the Government Servant Conduct Rules/Discipline and Appeal Rules etc. including penal actions and prosecution, while the Supplier will bear any or a combination of following penalties:

   (a) Cancellation of Contract/Rate Contracts (RCs)

   (b) Cancellation of Registration

   (c) Forfeiture of all securities and performance Bank Guarantees

   (d) Refusal to grant Registration and Contracts/RCs for further period of 3 (three) years

   (e) Suspension and/or banning the business dealings for period up to 3 (three) years (g) any other administrative or penal actions as deemed fit.

   (f) Action under IPC/PC Act and other relevant laws of the country.

6. It has been further agreed that the actions as aforesaid except that at 5(g) above will not require any criminal conviction from any court of law or arbitration but will be based on 'No-contest' basis, upon satisfaction of the SPO/PE, who will be the competent authority to finally decide the matter on strength of such materials/evidence of default/breach of the terms under this IP.

7. It has been also agreed prescribing that within 30 (thirty) days of such orders passed by SPO/PE, the aggrieved party shall have the right to appeal to the Principal Secretary/Secretary, Micro, Small and Medium Enterprises, Government of Uttar Pradesh, Lucknow and till the time a decision is taken on such appeal, the decision of SPO/PE would be in-force unless otherwise specifically ordered by the Principal Secretary/Secretary.

8. Agreed, accepted and signed on behalf of Supplier on this day and year mentioned below and handed over to the concerned office of SPO/PE forming integral part of all the affairs and transactions with and in relation to SPO/PE.

(Signature of the Prime Bidder)

Printed Name

Designation

<<Seal>>

Date:

Place:

Business Address:

9.23 Annexure 23: Format for affidavit for OEM claiming benefit under Make in India Policy

Date:

I, _____S/o, D/0, W/0 , _____ , Resident of _____do hereby solemnly affirm and declare as signing authority on behalf of _____ <name of OEM>, registered office at _____ that we agree to abide by the terms and conditions of **<Name of Nodal Ministry / Department >** of Government of India, issued vide Notification No:_____ dated _____

That the information furnished hereinafter is correct to best of my knowledge and belief and I undertake to produce relevant records before the procuring entity or any other authority so nominated by the **<Name of Nodal Ministry / Department >**, Government of India, for the purpose of assessing the Local Content (LC).

That the LC for all inputs which constitute the said Product/Services/Works has been verified by me and we are responsible for the correctness of the claims made therein.

That in the event of the LC of the Product/Services/Works mentioned herein is found to be incorrect and not meeting the prescribed LC norms, based on the assessment of an authority so nominated by the **<Name of Nodal Ministry / Department >**, Government of India and we will be liable as under clause 9 (I) of Public Procurement (Preference to Make in India) Order 2017.

We agree to maintain all information regarding my claim for LC in the Company's record for a period of 2 years from the date of bidding and shall make this available for verification to any statutory authorities.

- **I.** Name and details of the Local supplier (Registered Office, Manufacturing unit location, nature of legal entity)
- **II.** Date on which this certificate is issued
- **III.** Product/Services/Works for which the certificate is produced
- **IV.** Procuring agency to whom the certificate is furnished
- **V.** Percentage of LC claimed
- **VI.** Name and contact details of the unit of the manufacturer
- **VII.** Factory Price of the product
- **VIII.** Freight, insurance and handling
- **IX.** Total Bill of Material
- **X.** List and total cost value of inputs used for manufacture of the Product/Services/Works
- **XI.** List and total cost of inputs which are locally sourced. Please attach LC certificates from local suppliers. if the input is not in-house.
- **XII.** List and cost of inputs which are imported, directly or indirectly
- **XIII.** Factory/ manufacturer/ Producer Location with complete address

I confirm that our company or firm **< Name of the Company/Firm>**, are aware regarding restrictions on procurement from a country which shares a land border with India; I hereby certify that the Product/Services/Works and its components proposed in this Tender are not manufactured in such a country and is eligible to be considered.

I hereby certify and confirm that the Product/Services/Works and its components proposed in this Tender are being Manufactured at **< Name and address of facility>** in India and is currently underproduction and not being simply assembled.

For and on behalf of_____ (Name of firm/entity)

Authorized signatory (To be duly authorized by the Board of Directors)

<Insert Name, Designation and Contact No. and date>

Identified by me

Before Me

Advocate
<Name with Signature & Seal>
Date:
Place:

Public Notary
<Name with Signature & Seal>
Date:
Place:

Note:

1. Affidavit should be on Non-judicial stamp paper of Rs.100/-
2. Please fill up the details as per the documents you are annexing.
3. Affidavit should be attested by Notary Public.

9.24 Annexure 24: Format for Tripartite Agreement

1. Agreement

This Agreement is entered on ……. day of <month> <year> among <<BUYER>> constituted by and having its registered office at ..... (hereinafter called the "BUYER)", of the one part AND

<<SERVICE PROVIDER>>, a company incorporated under the Companies Act 1956 and having its corporate office at …….. selected for <<PROJECT>> i.e., Party engaged by …….. vide LOI No…… and detailed order no…… (herein referred to as the "Contract") for Supply, installation, integration, testing, commissioning of System Integration Project covering software, hardware, field survey and Networking (Telecom services, Internet Bandwidth) and Related Services incidental thereto as specified in the Services/ Scope of Work at Section 4 of the said Contract (hereinafter referred to as "**MSI or <<**MASTER SERVICE INTEGRATOR>> which expression shall unless excluded by or repugnant to the meaning or context thereof be deemed to include its successors and assigns) of the second Part.

AND

<<Name of Telecom Service Provider (TSP)>> a company incorporated under the Companies Act 1956 and having its corporate office at ……., being a TELECOM SERVICE PROVIDER/TELECOM BANDWIDTH SERVICE PROVIDER for the referred <<Name of Project>> engaged for Providing ……., Telecom services, Internet Bandwidth and connectivity incidental thereto as specified in the Services/ Scope of Work in the agreement between <<SERVICE PROVIDER>> and <<BUYER>> (hereinafter referred to as "TELECOM SERVICE PROVIDER (TSP))" which expression shall unless excluded by or repugnant to the meaning or context thereof be deemed to include its successors and assigns) of the third Part.

<<BUYER>>, "<<SERVICE PROVIDER>>" and "<<Telecom Service Provider (TSP)>>" are individually referred as "Party" and collectively as "Parties".

WHEREAS <<BUYER>>, the party of the first part has contracted <<SERVICE PROVIDER>>, the second party, for Turn Key Implementation of <<Name of Solution>> at <<Name of SERVICE PROVIDER>> (hereinafter referred to as "The Project") vide its Contract No.……

WHEREAS as per the requirements of the project, <<BUYER>> requires these services for successful implementation of the project.

WHEREAS <<SERVICE PROVIDER>>, in order to service its obligation under the above-mentioned RFP to the full satisfaction of the BUYER, had proposed "<<Telecom Service Provider (TSP)>>" as a service provider vide their letter/ offer no dated and now agrees to associate with <<Telecom Service Provider (TSP)>> for execution of the part of the order, to provide support services as detailed in the purchase Order (SERVICE PROVIDER) and/or indicated in ……. <section> of this agreement to be the responsibility of <<Telecom Service Provider (TSP)>>, namely, related to required Bandwidth services for the project.

WHEREAS SERVICE PROVIDER has done the due diligence with respect to the capabilities, technical or otherwise, of <<TELECOM SERVICE PROVIDER (TSP)>> for providing the required type of connectivity and services within time frame, quality, security, and reliability level as envisaged in the RFP / SRS before recommending their name.

WHEREAS the bid price quoted by <<SERVICE PROVIDER>> for Networking (Telecom services, Internet Bandwidth and connectivity) and Related Services ("Service") at locations as specified in CONTRACT (hereinafter referred to as the "Locations") for the purpose of utilization by the <<BUYER>> and their respective subsidiaries and affiliates as specified in the CONTRACT No. ……to <<SERVICE PROVIDER>> placed by <<BUYER>>, is passed through to <<TELECOM SERVICE PROVIDER (TSP)>> in accordance with the bid proposal dated ……..… submitted to <<BUYER>> by <<SERVICE PROVIDER>>, and the Terms & Conditions and SLA of <<BUYER>> with <<TELECOM SERVICE PROVIDER (TSP)>>, for carrying out the Networking and Related Services.

WHEREAS <<TELECOM SERVICE PROVIDER (TSP)>> has Category 'A' TSP license

having its Telecom spread across India.

The Purchase Order placed vide … ……./ to be placed by <<BUYER>> to <<TELECOM SERVICE PROVIDER (TSP)>> shall form an integral part of this agreement. <<SERVICE PROVIDER>>, shall be responsible for

(i) coordinating /entering into a tripartite agreement with the TSP along with the Buyer

(ii) getting the work executed by the TSP as per the Contract for Bandwidth as well as SLA's (iii) the replacement, if any, of the TSP without changing any penalty/LD criteria. However, the new TSP must meet the qualification criteria. Any breach or failure to fulfil the obligations as mentioned in the Tripartite Agreement which has a material impact on the performance of the Contract shall be treated as a breach of the terms of 'The Contract'.

WHEREAS by virtue of this agreement, the parties <<SERVICE PROVIDER>> and <<TELECOM SERVICE PROVIDER (TSP)>> bind themselves to the terms & conditions that are embedded in the contract between the first two parties.

Now these presents witness, and it is hereby agreed by and between the parties hereto as follows:

2. APPLICATION

This Agreement details the general terms and conditions for the provision of the Services to be rendered by <<TELECOM SERVICE PROVIDER (TSP)>> [as per CONTRACT placed vide…./to be placed by <<BUYER>>] and by <<SERVICE PROVIDER>> [as per CONTRACT No……..with <<BUYER>>]. Upon signing the scope, duration and other services to be so rendered under this Agreement the parties agree to accept and be bound by these terms and conditions.

3. PROVISION OF SERVICE

- The provision of the Services is subject to these terms and conditions stated in this Agreement. Where <<TELECOM SERVICE PROVIDER>> shall accept the Order from <<BUYER>>, <<TELECOM SERVICE PROVIDER>> shall provide the Services required by <<BUYER>>, and by <<SERVICE PROVIDER>> on behalf of

<<BUYER>>, within a timeframe, quality, security and reliability level agreed with between <<BUYER>>, <<TELECOM PROVIDER>> and <<SERVICE PROVIDER>>.

The SERVICE PROVIDER shall provide <<TELECOM PROVIDER>> with a complete Telecom diagram of the set-up along with the details of connectivity at the Locations and services will be provisioned to the <<BUYER>> accordingly. It is the responsibility of SERVICE PROVIDER, to ensure and of <<TELECOM SERVICE PROVIDER>> to provide proper Telecom monitoring and Telecom management as per SLA like uptime, proper bandwidth etc. and to submit the SLA performance report of the <<TELECOM SERVICE PROVIDER>> to the <<BUYER>> on monthly/as and when required basis.

- The Telecom links will be provided by <<TELECOM SERVICE PROVIDER>> and the SERVICE PROVIDER will monitor and report any problems on behalf of <<TELECOM SERVICE PROVIDER>> to <<BUYER>>.
- Where it is necessary, due to materiel breach by the <<TELECOM SERVICE PROVIDER>>, the <<BUYER>> shall instruct the <<SERVICE PROVIDER>> to replace the <<TELECOM SERVICE PROVIDER>> with another <<TELECOM SERVICE PROVIDER>>. In case of replacement of <<TELECOM SERVICE PROVIDER>>, the SERVICE PROVIDER shall terminate forthwith all agreements/contracts other arrangements with such <<TELECOM PROVIDER>> and find suitable replacement for such <<TELECOM PROVIDER>> to the satisfaction of the <<BUYER>> at no additional charge. The <<SERVICE

PROVIDER>> has to execute the contract as per agreed schedule and SLA and as per contractual provision entered between

<<BUYER>> and <<SERVICE PROVIDER>>.

- <<SERVICE PROVIDER) shall ensure that Requisite Services from <<TELECOM SERVICE PROVIDER>> for project area (town) are available on time when its own system/works that are to be installed/ executed/implemented under PO no .....with

<<BUYER>>, are ready for testing & commissioning.

- The <<TELECOM SERVICE PROVIDER>> shall not use the establishments and services installed under this agreement for organizations other than

<<BUYER>>.

4. SERVICE TERM

The term of the Services is initially for ..... years (as per CONTRACT) from the date of commencement of service, and if required, thereafter, shall be extended from time to time by written consent of the parties. The Service Commencement Date shall be set forth in accordance with the Purchase Order placed vide…… / to be placed by <<BUYER>> on <<TELECOM SERVICE PROVIDER>>**.**

5. TERMINATION OF SERVICE

The Termination of this Agreement and Services shall be as per provisions of Termination clause as appearing in main CONTRACT

6. RESPONSIBILITIES OF THE PARTIES

a) Responsibility of <<BUYER>>

- To monitor the project progress against time frame & quality and performance with, quality, security and reliability levels of required services as per agreement with <<SERVICE PROVIDER)>> and <<TELECOM SERVICE PROVIDER)>>
- To disburse the payment to the <<TELECOM SERVICE PROVIDER>> upon achievement of the SLA based on performance reports/ SLA reports.
- To provide safe access and conditions to <<SERVICE PROVIDER>> and <<TELECOM SERVICE PROVIDER>>'s employees or appointed personnel while in the premises

b) Responsibility of <<SERVICE PROVIDER>>

- To arrange through a licensed Telecom service provider, Telecom services, Internet Bandwidth and connectivity, incidental thereto as specified in the Scope of Work in the agreement between <<SERVICE PROVIDER>> and <<BUYER>>.
- The Service Providers overall liabilities and responsibilities shall in no case be less or more than the liabilities as mentioned in the contract, with respect to 'The Project',

executed between the Service Provider and the Buyer. Ensuring Timely execution of the part of the order related to required Bandwidth for the project.

- To provide <<TELECOM SERVICE PROVIDER>> with a complete Telecom diagram of the set-up along with the details of connectivity at the Locations and services provisioned to the <<BUYER>>
- Proper Telecom monitoring and Telecom management as per SLA like uptime, proper bandwidth etc. and submit SLA report to the BUYER on monthly/as and when required basis.
- To monitor and report any problems on behalf of <<TELECOM SERVICE PROVIDER>>.
- To ensure that the <<TELECOM SERVICE PROVIDER>> comply with all relevant and applicable provisions of the Contract.
- To obtain and arrange for the maintenance in full force and effect of all applicable government approvals, consents, licenses, authorizations, declarations, filings, and registrations as may be necessary and advisable for the performance of all the terms and conditions of this Agreement.

c) Responsibility of <<SUB-CONTRACTOR>>

- To provide Telecom services, Internet Bandwidth and connectivity, incidental thereto as specified in the Scope of Work as per CONTRACT placed by <<BUYER>> to <<SERVICE PROVIDER>> and <<TELECOM SERVICE PROVIDER>>.
- To provide the Services (as per SLA) required by <<BUYER>>, and by <<SERVICE PROVIDER>> on behalf of <<BUYER>>, within the timeframe, quality, security and reliability level agreed with between <<BUYER>>, <<TELECOM SERVICE PROVIDER>> and <<SERVICE PROVIDER>>.
- Not to use the establishments and services installed under this agreement for organizations other than <<BUYER>>.
- To raise direct invoices against the works/services performed, as per the terms of the Purchase Order with <<BUYER>>.
- To ensure compliance of Indian Telecom regulation & statutory requirements while performing the works/services under this agreement.
- To obtain and arrange for the maintenance in full force and effect of all government approvals, consents, licenses, authorizations, declarations, filings, and registrations as may be necessary and advisable for the performance of all the terms and conditions of this Agreement.

7. INVOICE AND PAYMENT

a. <<Telecom Service Provider>> shall raise direct invoices against the Requisite Services so rendered, as per the terms of the Contract and <<BUYER>> shall directly make the payment to <<Telecom Service Provider>> based on the SLA report and confirmation made by <<SERVICE PROVIDER>>.

b. The other terms and conditions shall remain applicable as per

<<BUYER's>> CONTRACT No. .....with <<SERVICE PROVIDER>>.

8. **DISPUTES WITH REGARDS TO INCORRECT INVOICING**

Disputes regarding incorrect Invoicing shall be governed by <<BUYER's>> CONTRACT No. with <<SERVICE PROVIDER>>.

9. **ACCESS TO PREMISES**

<<BUYER>> shall allow or obtain the required permission to enable <<TELECOM SERVICE PROVIDER>> employees or authorized personnel, appointed distributors, agents, or subcontractors to enter always during the normal working hours of <<BUYER)>>into the premises where the Services are provided for periodical Inspection with seven (7) days prior notice, installing, maintaining, replacing, and removing equipment hardware and/or software prior to, during and after the provision of the Services, as well as to Inspect the Telecom and/or to the CPE or any other equipment used in or in connection with the Services. The <<BUYER>> shall render all assistance in this regard and shall provide safe access and conditions for <<TELECOM SERVICE PROVIDER's>> employees or appointed personnel whilst in the premises. <<TELECOM SERVICE PROVIDER's>> employees or appointed personnel shall comply with security and confidentiality policies and procedures while on the <<BUYER>>'s premises.

10. **NOTICES**

Any party may deliver notices to the other by personal delivery or by postal delivery at -
<<BUYER>> ……
<<SERVICE PROVIDER>> ……
<<TELECOM SERVICE PROVIDER)>. ……
Notices shall be deemed delivered on the date of actual receipt.

11. **ENTIRE UNDERSTANDING**

This Agreement constitutes the entire understanding of the parties related to the subject matter hereof. The agreement may be amended only in writing when it is signed by <<TELECOM SERVICE PROVIDER>>, <<SERVICE PROVIDER>> and <<BUYER>>.

12. **MISCELLANEOUS**

The terms of this Agreement shall not be construed to constitute a partnership, joint venture, or employer/employee relationship between the parties. This Agreement along with any other relevant document constitutes the whole of the agreement and understanding between the parties about the subject matter.

a) In the event of any provision of this Agreement being held or becoming invalid, unenforceable or illegal for any reason, this Agreement shall remain otherwise in full force apart from the said provision which will be deemed deleted. The parties shall however attempt to replace the deleted provision with a legally valid provision that reflects the same purpose of the deleted provision to the greatest extent possible.
b) Headings used in this Agreement are for the convenience and ease of reference only and shall not be relevant to or affect the meaning or interpretation of this Agreement.
c) No forbearance, relaxation or inaction by any party at any time to require the performance

of any provision of this Agreement shall in any way affect, diminish, or prejudice the right of such party to require the performance of that or any other provision of this Agreement or be considered to be a waiver of any right, unless specifically agreed in writing.

d) Each Party shall obtain and arrange for the maintenance in full force and effect of all government approvals, consents, licenses, authorizations, declarations, filings, and registrations as may be necessary and advisable for the performance of all the terms and conditions of this Agreement.

e) The <<Telecom Service Provider>> and <<SERVICE PROVIDER>> shall ensure compliance of Indian Telecom regulation & all other statutory requirements while performing the works/ services under this agreement.

13. **APPLICABLE LAW**

The Agreement shall be governed by and construed in accordance with Indian Law. Subject to arbitration provision stated hereinafter the Courts at << >> shall have the jurisdiction.

14. **ARBITRATION**

Any Disputes which may arise out of this Agreement, and which cannot be settled in discussions or negotiations between the Parties, shall be referred to the appropriate management or higher authorities of the respective parties to resolve such disputes in good faith. In case no settlement is reached the parties shall refer it to a sole arbitrator appointed and selected by parties. Arbitration shall be conducted in accordance with the provisions of the Arbitration and Conciliation Act, 1996 or any other subsequent modifications or enactments thereof. The venue for Arbitration proceedings shall be << Place>>. The Arbitration shall be conducted in English Language and the award shall be binding upon all Parties.

15. **LIMITATION OF LIABILITY**

Limitation & liability with respect to Main Agreement and this Agreement shall be governed by <<BUYER's>> Contract with <<SERVICE PROVIDER>. For the sake of clarity, the parties agree that this Limitation of Liability shall be a part of overall limitation of liability for the entire scope of work under the contract, with respect to 'The Project', executed between the Service Provider and the Buyers.

IN WITNESS WHEREOF the parties hereto have executed these presents the day and year first above written.

SIGNED AND DELIVERED BY

(on behalf of BUYER)
Signature

……..

Name & Designation

In the presence of

……..

Name & Designation

Address ……..	Address ……..
SIGNED AND DELIVERED BY (on behalf of BUYER) Signature ……..	In the presence of ……..
Name & Designation	Name & Designation
Address ……..	Address ……..

9.25 Annexure 25: Application wise user estimations - Concurrent User Category

Below is the list of concurrent user's category for estimation of Infra, software licensing and Server Sizing etc.

Sl	User type	Concurrent Users (approx.)
1.	Communication officer	256
2.	Communication supervisory	15
3.	Feedback/ outbound users	36
4.	Dispatch supervisory HQ and OMCs	63
5.	Dispatch Supervisory DCRs	267
6.	Field PRV 4W and Inspection 4 W	4578
7.	Field PRV 2W	2100
8.	Thana and Police chowki users	1800
9.	Fire Department User: District Fire HQ and One Fire HQ	76
10.	Fire Department Users Field	1100
11.	GRP 65 GRP stations, 6 SRP control rooms,1 DIG, 1IG and one HQ	74
12.	Medical users for transfer of events on API	40
13.	UPSRTC (50 pink buses, 200 new buses and 12,000 old buses)	12250
14.	UPSRTC control room	1
15.	181 Desk at UP112	5
16.	1090 Women Power for call transfer to other 1090 control rooms	20
17.	Safe City (10 cities) – 10 command centres	10
18.	Safe Cities vehicles – 10 cities approx.	300
19.	Smart City -01 all from Lucknow ICCC	1
20.	UPHP (Uttar Pradesh Highway Police)- vehicles	50
21.	Disaster Management call transfer of the call to desk	01
22.	CM Helpline call transfer to call to desk	10
23.	UP Metro Control centre (4 locations)	4
24.	CRIS helpline transfer	1

9.26 Annexure 26: Application wise user estimations - Application Category

Below is the list of application design estimation considering approx. full load of the system and future scalability:

Sl	Application	Application design for full load (approx.)
1.	IP PBX	1 lot for 66 lakhs signals per day
2.	IP Phone software / Soft phone	500
3.	Outbound Dialler software	500
4.	Automatic Call Distribution (ACD)	1.3 lakhs post IVRS per day
5.	Call Telephony Integration (CTI)	1.3 lakhs post IVRS per day
6.	Voice recording	25,000 per day
7.	Contact Centre Reporting System	1.3 lakhs post IVRS
8.	IVRS	1.3 lakhs post IVRS
9.	Multimedia System	25,000 events per day
10.	Core Computer Aided Dispatch (CAD) Application	25,000 events per day
11.	MDT/Mobile CAD application	4500 4W +2100 2W + 78 Inspection 4W+ 65 GRP + 1100 Fire tenders
12.	Mobile Application for Senior Officers, Police Station Officers and Field staff (Supervisory App)	24 at HQ, 4 OMCs, 78 districts SSPs, 78 Additional SP at Districts, 312 Dy SP and 1500 at field
13.	UP112 Portal (Citizen Portal)	
14.	Enterprise Management System (EMS)	1400 assets
15.	Mobility Device management (MDM)	4500 4W MDTS, 6600 4W & 2W PRVs Phone, 6600 GPS, + 65 GRP MDT + 78 MDT 4w Inspection+78 Smart phone 4 W Inspection
16.	Inventory Management Software with RFID tags and readers	50,000 assets
17.	Human Resource Management Software	70,000
18.	Facial Recognition Attendance System with geotagging	70,000
19.	Biometric Attendance	1,000
20.	Patrol Management System	6678 PRVs
21.	GIS Application	54 layers
22.	GIS Data Capturing Mobile Application	1 lot already 20 lakhs PI, additional 10% so 2 lakhs POIs

Sl	Application	Application design for full load (approx.)
23.	GIS Map Geo-Fencing Process	Base map 1 unit
24.	GIS Map Data	Base map 1 unit
25.	LBS (Location Based Services)	13000 post IVR calls per day
26.	Auto Arrive	6600 PRV
27.	Geo Fencing of PRVs	6678 PRV
28.	GPS Solution	6678 PRV and 1100 Fire
29.	Fleet Management Solution	6678 PRV and 1100 Fire
30.	PRV Location Tracking by Citizen	25,000 events per day
31.	ELS/ALS	25,000 post IVR calls per day
32.	Video Conferencing	6678 PRVs, 78 SSPs and commiserates, 1 HQ, 78 DCRs, 2 OMCs
33.	Document Management System (DMS)	24 HQ, 4 at OMCS, 20 others
34.	Number Masking	25,000 events per day
35.	Directory Services	As per requirement
36.	API Gateway	As per requirement
37.	Identity Management Software (IMS)	As and when required for 70000 staff
38.	Chatbot	25,000 events per day
39.	e-learning	70,000 staff
40.	ROIP	78 DCRs, 1 HQ, 2 OMCs, 6678 PRVs
41.	PTT (Push to Talk)	78 DCRs, 1 HQ, 2 OMCs, 6678 PRVs

9.27 Annexure 27: List of Locations

Categorization of Districts/Commissionerate			
#	Sl.	Category	Districts/Commissionerate
1	**1**	**A**	Lucknow Commissionerate
2	**2**	**A**	Kanpur Commissionerate
3	**3**	**A**	Gautam b. Nagar Commissionerate

Categorization of Districts/Commissionerate			
#	**Sl.**	**Category**	**Districts/Commissionerate**
4	**4**	**A**	Varanasi Commissionerate
5	**5**	**A**	Ghaziabad
6	**6**	**A**	Prayagraj
7	**7**	**A**	Gorakhpur
8	**8**	**A**	Agra
9	**9**	**A**	Meerut
10	**10**	**A**	Aligarh
11	**11**	**A**	Bareilly
12	**1**	**B**	Unnao
13	**2**	**B**	Hardoi
14	**3**	**B**	Jaunpur
15	**4**	**B**	Sitapur
16	**5**	**B**	Pratapgarh
17	**6**	**B**	Azamgarh
18	**7**	**B**	Barabanki
19	**8**	**B**	Ayodhya
20	**9**	**B**	Mathura
21	**10**	**B**	Mirzapur
22	**11**	**B**	Moradabad
23	**12**	**B**	Jhansi
24	**13**	**B**	Saharanpur
25	**14**	**B**	Firozabad
26	**15**	**B**	Muzaffarnagar

Categorization of Districts/Commissionerate			
#	**Sl.**	**Category**	**Districts/Commissionerate**
27	**1**	**C**	Mau
28	**2**	**C**	Amethi
29	**3**	**C**	Budaun
30	**4**	**C**	Ghazipur
31	**5**	**C**	Ballia
32	**6**	**C**	Kannauj
33	**7**	**C**	Banda
34	**8**	**C**	Sonbhadra
35	**9**	**C**	Basti
36	**10**	**C**	Kanpur dehat
37	**11**	**C**	Fatehpur
38	**12**	**C**	Bahraich
39	**13**	**C**	Kushinagar
40	**14**	**C**	Deoria
41	**15**	**C**	Ambedkar nagar
42	**16**	**C**	Gonda
43	**17**	**C**	Sultanpur
44	**18**	**C**	Shahjahanpur
45	**19**	**C**	Raebareli
46	**20**	**C**	Kheeri
47	**21**	**C**	Bulandshahr
48	**22**	**C**	Amroha
49	**23**	**C**	Bijnor

Categorization of Districts/Commissionerate			
#	**Sl.**	**Category**	**Districts/Commissionerate**
50	**24**	**C**	Sant ravi das nagar
51	**25**	**C**	Fatehgarh
52	**26**	**C**	Hamirpur
53	**27**	**C**	Sambhal
54	**28**	**C**	Lalitpur
55	**29**	**C**	Etah
56	**30**	**C**	Sant kabir nagar
57	**31**	**C**	Chandauli
58	**32**	**C**	Jalaun
59	**33**	**C**	Siddharth nagar
60	**34**	**C**	Kaushambi
61	**35**	**C**	Pilibhit
62	**36**	**C**	Hathras
63	**37**	**C**	Hapur
64	**38**	**C**	Mainpuri
65	**39**	**C**	Chitrakoot
66	**40**	**C**	Maharajganj
67	**41**	**C**	Etawah
68	**42**	**C**	Kasganj
69	**43**	**C**	Auraiya
70	**44**	**C**	Rampur
71	**45**	**C**	Shamli
72	**46**	**C**	Balrampur

Categorization of Districts/Commissionerate			
#	**Sl.**	**Category**	**Districts/Commissionerate**
73	**47**	**C**	Bagpat
74	**48**	**C**	Shravasti
75	**49**	**C**	Mahoba
76	**50**	**C**	Lucknow rural
77	**51**	**C**	Kanpur outer
78	**52**	**C**	Varanasi rural

Summary			
	SL	**Count**	**Category**
	1	**11**	**Category A**
	2	**15**	**Category B**
	3	**52**	**Category C**

List of Locations based on type

Sl.	TYPE	Location
1	Commissionerate	Lucknow Commissionerate
2	Commissionerate	Kanpur Commissionerate
3	Commissionerate	Gautam b. Nagar Commissionerate
4	Commissionerate	Varanasi Commissionerate
5	District	Prayagraj
6	District	Agra
7	District	Ghaziabad

Sl.	TYPE	Location
8	District	Gorakhpur
9	District	Meerut
10	District	Aligarh
11	District	Bareilly
12	District	Unnao
13	District	Hardoi
14	District	Jaunpur
15	District	Sitapur
16	District	Pratapgarh
17	District	Azamgarh
18	District	Barabanki
19	District	Ayodhya
20	District	Mathura
21	District	Mirzapur
22	District	Moradabad
23	District	Jhansi
24	District	Saharanpur
25	District	Firozabad
26	District	Muzaffarnagar
27	District	Mau
28	District	Amethi
29	District	Budaun
30	District	Ghazipur
31	District	Ballia
32	District	Kannauj
33	District	Banda
34	District	Sonbhadra

Sl.	TYPE	Location
35	District	Basti
36	District	Kanpur dehat
37	District	Fatehpur
38	District	Bahraich
39	District	Kushinagar
40	District	Deoria
41	District	Ambedkar nagar
42	District	Gonda
43	District	Sultanpur
44	District	Shahjahanpur
45	District	Raebareli
46	District	Kheeri
47	District	Bulandshahr
48	District	Amroha
49	District	Bijnor
50	District	Sant ravi das nagar
51	District	Fatehgarh
52	District	Hamirpur
53	District	Sambhal
54	District	Lalitpur
55	District	Etah
56	District	Sant kabir nagar
57	District	Chandauli
58	District	Jalaun
59	District	Siddharth nagar
60	District	Kaushambi
61	District	Pilibhit

Sl.	TYPE	Location
62	District	Hathras
63	District	Hapur
64	District	Mainpuri
65	District	Chitrakoot
66	District	Maharajganj
67	District	Etawah
68	District	Kasganj
69	District	Auraiya
70	District	Rampur
71	District	Shamli
72	District	Balrampur
73	District	Bagpat
74	District	Shravasti
75	District	Mahoba
76	District	Lucknow rural
77	District	Kanpur outer
78	District	Varanasi rural
79	Police Range	Agra
80	Police Range	Aligarh
81	Police Range	Kanpur
82	Police Range	Jhansi
83	Police Range	Lucknow
84	Police Range	Ayodhya
85	Police Range	Bareilly
86	Police Range	Moradabad
87	Police Range	Meerut
88	Police Range	Saharanpur

Sl.	TYPE	Location
89	Police Range	Prayagraj
90	Police Range	Chitrakoot
91	Police Range	Varanasi
92	Police Range	Azamgarh
93	Police Range	Mirzapur
94	Police Range	Gorakhpur
95	Police Range	Basti
96	Police Range	Devipatan
97	Police Zone	Agra
98	Police Zone	Kanpur
99	Police Zone	Lucknow
100	Police Zone	Bareilly
101	Police Zone	Meerut
102	Police Zone	Prayagraj
103	Police Zone	Varanasi
104	Police Zone	Gorakhpur
105	Other Location	DGP Headquarters
106	Other Location	Radio Headquarters
107	Other Location	Home Control – Lok Bhawan
108	Other Location	FIRE Headquarters
109	Other Location	108 Headquarters
110	Other Location	Suraksha Headquarters
111	Other Location	INT. Headquarters
112	Other Location	PAC Headquarters
113	Other Location	GRP Headquarters
114	Other Location	DGP Office
115	Other Location	GRP Agra

Sl.	TYPE	Location
116	Other Location	GRP Prayagraj
117	Other Location	GRP Gorakhpur
118	Other Location	GRP Lucknow
119	Other Location	GRP Moradabad
120	Other Location	GRP Jhansi
121	Other Location	GRP Kanpur
122	Other Location	Ram Janm Bhoomi Ayodhya
123	Other Location	Krishna Janm bhoomi Mathura
124	Other Location	Kashi Viswanath Temple Varanasi
125	Other Location	SDRF Headquarters
126	Other Location	Women Power Line 1090
127	Other Location	Law & Order Headquarters
128	Other Location	Technical Services Headquarters
129	Other Location	Traffic Headquarters

9.28 Annexure 28: List of POIs and layers

Details of GIS Data layers with attributes

Layer No	Layer Name	Description
1.	District Boundaries	Name coded to Polygon
2.	Different districts layers for Districts	
3.	Colonies	Name coded to Polygon
4.	Boundary or Area of Police Station	Name coded to Polygon
5.	Jurisdiction limits	Name coded to Polygon
6.	Arterial Roads	Symbol
7.	Main Roads	Symbol

Layer No	Layer Name	Description
8.	Important Roads	Symbol
9.	Industrial area	Symbol
10.	Shopping area	Symbol
11.	Parks and Gardens	Symbol
12.	Railway Stations	Symbol
13.	Water bodies	Symbol
14.	Police Stations	Symbol
15.	Hospitals	Symbol, Name
16.	Fire stations	Symbol
17.	Hotels	Symbol, Name
18.	Restaurants	Symbol, Name
19.	Banks	Symbol
20.	Cinemas	Symbol, Name
21.	Auditorium	Symbol, Name
22.	Post and telegraph offices	Symbol
23.	Historical Places	Symbol, Name
24.	Petrol Pump	Symbol
25.	Airline and travel agency	Symbol
26.	Museums	Symbol, Name
27.	Apartments	Name, House Number (where available)
28.	Buildings	Average 25 buildings per district. Names would be finalized by UP112
29.	Industries	Name
30.	Library	Name
31.	Parks	Name
32.	Railway Stations	Name
33.	Railway Reservation Centre	Name
34.	Institutions	Name
35.	Shopping Centre	Name

Layer No	Layer Name	Description
36.	Water feature	Name
37.	Blood Bank	Symbol
38.	Place of worship	Name
39.	Information Centre	Symbol, Name
40.	Art Gallery	Symbol, Name
41.	Education and Training Institutions	Name
42.	Courts	Name
43.	Clubs	Name
44.	Offices	Name
45.	Hostels	Name
46.	Centre Lines of Arterial, Main and Important Roads	One Ways Defined
47.	Rail Lines	Symbol
48.	Other Roads Outlines	Symbol
49.	Arterial road label	Labels of Arterial Roads
50.	Main road label	Labels of Main Roads
51.	Other road label	Labels of Other Roads
52.	ss	Name of locally called famous name
53.	Annotation layer	All-important names of Industries,
54.	Geo fencing of Police boundaries	Up to Police station level

Details of district wise POIs count

Sl. No	District Name	POIs Count
1.	AGRA	261251
2.	ALIGARH	55777
3.	AMBEDKAR NAGAR	23461
4.	AMETHI	17127
5.	AMROHA	24601

Sl. No	District Name	POIs Count
6.	AURAIYA	15589
7.	AYODHYA	29492
8.	AZAMGARH	55139
9.	BAGPAT	15544
10.	BAHRAICH	19298
11.	BALLIA	20615
12.	BALRAMPUR	10419
13.	BANDA	22299
14.	BARABANKI	49587
15.	BAREILLY	46802
16.	BASTI	28354
17.	BIJNOR	54307
18.	BUDAUN	31598
19.	BULANDSHAHR	46354
20.	CHANDAULI	15183
21.	CHITRAKOOT	5358
22.	DEORIA	20035
23.	ETAH	23686
24.	ETAWAH	23433
25.	FATEHGARH	19469
26.	FATEHPUR	34699
27.	FIROZABAD	33967
28.	GAUTAM B. NAGAR	586805
29.	GHAZIABAD	565292
30.	GHAZIPUR	43698
31.	GONDA	25583
32.	GORAKHPUR	68633
33.	HAMIRPUR	22331
34.	HAPUR	18807
35.	HARDOI	35386
36.	HATHRAS	18355

Sl. No	District Name	POIs Count
37.	JALAUN	36877
38.	JAUNPUR	38860
39.	JHANSI	46559
40.	KANNAUJ	19536
41.	KANPUR NAGAR	429245
42.	KANPUR DEHAT	8612
43.	KASGANJ	19050
44.	KAUSHAMBI	10361
45.	KHERI	32246
46.	KUSHINAGAR	26085
47.	LALITPUR	17306
48.	LUCKNOW	426647
49.	MAHARAJGANJ	15630
50.	MAHOBA	16474
51.	MAINPURI	20386
52.	MATHURA	58904
53.	MAU	21322
54.	MEERUT	122922
55.	MIRZAPUR	23833
56.	MORADABAD	31634
57.	MUZAFFARNAGAR	74285
58.	PILIBHIT	19945
59.	PRATAPGARH	28164
60.	PRAYAGRAJ	127926
61.	RAEBARELI	23399
62.	RAMPUR	18461
63.	SAHARANPUR	53011
64.	SAMBHAL	20178
65.	SANT KABIR NAGAR	8387
66.	SANT RAVI DAS NAGAR	14821

Sl. No	District Name	POIs Count
67.	SHAHJAHANPUR	18157
68.	SHAMLI	20927
69.	SHRAVASTI	3849
70.	SIDDHARTH NAGAR	11001
71.	SITAPUR	26073
72.	SONBHADRA	12644
73.	SULTANPUR	31806
74.	UNNAO	14520
75.	VARANASI	209932
76.	**GRAND TOTAL**	**4548309**

9.29 Annexure 29: List of Consumables

Sl. No.	Consumable Item	Frequency
1	Charger of Mobile phone	Twice in project tenure
2	Battery of MDT	Twice in project tenure
3	Charger of MDT	Twice in project tenure
4	Cartridges for Printer	As per requirement
5	Battery of VHF Sets	Twice in project tenure
6	Charger of VHF Sets	Twice in project tenure
7	Battery for Laptops	Twice in project tenure
8	Charger for tablets	Twice in project tenure
9	Battery for tablets	Twice in project tenure
10	Earthing at all locations	Twice in project tenure
11	Charger for Body Worn Camera	Twice in project tenure
12	Battery for Body worn Camera	Twice in project tenure
13	Headphones	As per requirement
14	Y Jacks	As per requirement
15	Screen guard of Mobile Phones and tablets	As per requirement
16	Rugged Cover for Mobile Phones and tablets	As per requirement
17	All Mobile Phones	After 3 years

Note- All breakdown or accidental or physical damage will be covered under warranty by MSI

Service or repair due to normal and heavy usage wear and tear and any incidental damages
- *Non-remedial work, including but not limited to reprogramming and product configuration*
- *Repair of problems caused by physical damage, operator error including but not limited to:*

o Excessive dirt or contamination affecting performance
o Spillage of liquids and other foreign substances on products
o Scratched, contaminated and or damaged optical components

o Loose or missing parts, broken, cracked, disfigured, scratched displays, windows, housings or triggers
o Broken or cracked plastic parts (internal or external)
o Damaged external cables

9.30 Annexure 30: Preventive Maintenance Schedule

S No	Item/ Description	Preventive Maintenance Schedule
A	**Hardware at DC**	Monthly/Fortnightly/Quarterly/Half yearly/Yearly
1	Biometric	Monthly
2	SAN Storage	Quarterly
3	VTL	Quarterly
4	Database server	Quarterly
5	Blade chassis	Quarterly
6	Rack	Quarterly
7	Blade Server-2 CPU	Quarterly
8	Blade server-4 CPU	Quarterly
9	Load Balancer	Quarterly
10	Battery bank required to be changed (272 Nos.) for 200KVA UP-3Nos.	Monthly
11	Core Switch	Quarterly
12	Managed Access Switch	Quarterly
13	SAN Switch	Quarterly
14	Aggregation Switch	Quarterly
15	Internet Router	Quarterly
16	Core router	Quarterly
17	Global Load Balancer	Monthly
18	Server for Vehicle Mounted Camera	Monthly
19	Web Application Firewall	Monthly
20	NextGen Firewall	Monthly
21	Security Incident & Event Management (SIEM)-(AMC only)	Monthly

S No	Item/ Description	Preventive Maintenance Schedule
22	Data Leakage Prevention (DLP)	Monthly
23	Network Access Control (NAC)	Monthly
24	Storage for Vehicle Mounted Camera and Body Worn Camera	Quarterly
B	**Hardware at Command Center**	
1	Biometric	Monthly
2	Desktops including Hindi Keypad on Keyboard with two monitors with OS and Antivirus	Quarterly
3	Desktops including Hindi Keypad on Keyboard with triple monitors with OS and Antivirus	Quarterly
4	Desktops including Hindi Keypad on Keyboard with single monitor with OS and Antivirus	Quarterly
5	Desktop Thin client including Hindi Keypad on Keyboard	Quarterly
6	IP Phones with Headset	Quarterly
7	Laptop	Quarterly
8	Tablets-Android with Stylus	Quarterly
9	Printer, scanner and copier (multi-function)	Monthly
10	Heavy Duty printer	Monthly
11	Laser jet printer	Monthly
12	Paper shredder	Quarterly
13	Smart TV – 32 Inch	Quarterly
14	Smart TV – 42 Inch	Quarterly
15	Smart TV – 55 Inch	Quarterly
16	3 Conference room with equipment of capacity 15 people	
17	Display device	Monthly
18	Audio System	Monthly
19	Control System	Monthly
20	2 Conference rooms with equipment of capacity 10 people	
21	Display device	Monthly

S No	Item/ Description	Preventive Maintenance Schedule
22	Audio System	Monthly
23	Control System	Monthly
24	2 Conference rooms with equipment of capacity 8 people	
25	Display device	Monthly
26	Audio System	Monthly
27	Control System	Monthly
28	3 Conference room with equipment of capacity 20 people	
29	Display device	Monthly
30	Audio System	Monthly
31	Control System	Monthly
32	1 Meeting room with equipment of capacity 30 people	
33	Display device	Monthly
34	Audio System	Monthly
35	Control System	Monthly
36	2 Board rooms with equipment of capacity 30 people	
37	Display device	Monthly
38	Audio System	Monthly
39	Control System	Monthly
40	2 training rooms with equipment of capacity 25 people	
41	Screen	Quarterly
42	Projector	Quarterly
43	Audio system	Quarterly
44	Lapel Microphone	Quarterly
45	2 training rooms with equipment of capacity 50 people	
46	Screen	Quarterly
47	Projector	Quarterly
48	Audio system	Quarterly

S No	Item/ Description	Preventive Maintenance Schedule
49	Lapel Microphone	Quarterly
50	1 Training rooms with equipment of capacity 50 people (35 Dos live training room)	
51	Screen	Quarterly
52	Projector	Quarterly
53	Audio system	Quarterly
54	Lapel Microphone	Quarterly
55	Streaming Solution Device	Quarterly
56	Desktops with triple monitors with OS and Antivirus	Quarterly
57	IP phone with headset	Quarterly
58	Tabletop microphone	Monthly
59	VHF static radio device	Monthly
60	Access Switch	Quarterly
61	MDT	Monthly
62	1 training rooms with equipment of capacity 100 people	
63	Screen	Quarterly
64	Projector	Quarterly
65	Audio System	Quarterly
66	Lapel Microphone	Quarterly
67	1 Training rooms with equipment of capacity 100 people (75 Cos live training room)	
68	Screen	Quarterly
69	Projector	Quarterly
70	Audio System	Quarterly
71	Lapel Microphone	Quarterly
72	Access Switch	Quarterly
73	Tabletop microphone	Monthly

S No	Item/ Description	Preventive Maintenance Schedule
74	Streaming Solution Device	Quarterly
75	Desktops with double monitors with OS and Antivirus	Quarterly
76	IP phone with headset	Quarterly
77	Video Conference equipment for 15 locations	Monthly
78	Digital light processing (DLP) video wall	Quarterly
79	Radio Gateway	Monthly
80	Digital Radio Channel License for RoIP Server	Monthly
81	VHF static radio device	Monthly
82	lattice Mast and antenna for VHF static set	Monthly
83	Network Rack	Quarterly
84	Managed Access Switch-24 ports	Quarterly
85	Interactive Screen for EOC	Quarterly
C	**Hardware Component at Field**	
1	Desktops including Hindi Key pad on Keyboard with single monitor with OS and Antivirus	Quarterly
2	Desktops including Hindi Key pad on Keyboard with two monitor with OS and Antivirus	Quarterly
3	Mobile Data Terminal Devices (MDT) minimum 7 inches screen	Quarterly
4	Smart Phone-2W	Quarterly
5	LED TV 43" for DCR	Quarterly
6	UPS 1 kVA	Monthly
7	UPS 2 KVA	Monthly
8	Network Rack	Quarterly
9	IP Phone with Headset	Monthly
10	VHF 4W antenna	Monthly
11	Lattice Mast and antenna for VHF static set	Monthly
12	VHF static radio device	Monthly

S No	Item/ Description	Preventive Maintenance Schedule
13	Battery of VHF Handheld Radio Device And Charger of Battery pack	Monthly
14	VHF Handheld radio device	Monthly
15	Managed Access Switch 24 Ports	Quarterly
16	Intranet Router 20Mbps	Quarterly
17	RFID Reader and Controller	Monthly
18	RFID Tags	Quarterly
19	ROIP Solution	Monthly
20	Radio Over IP Gateway	Monthly
21	ROIP Advance digital software	Monthly
22	Digital Radio Channel License for RoIP Server	Monthly
23	Digital Subscriber License for RoIP Server	Monthly
24	Dispatcher Software License	Quarterly
25	Earthing	Half Yearly
26	ID Card Printer	Quarterly
27	Others,Passive	Quarterly
D	**Hardware Components at OMC**	
1	Desktops including Hindi Key pad on Keyboard with two monitors with OS and Antivirus	Quarterly
2	Desktops including Hindi Keypad on Keyboard with triple monitors with OS and Antivirus	Quarterly
3	Desktops including Hindi Keypad on Keyboard with single monitors with OS and Antivirus	Quarterly
4	Laptop	Quarterly
5	IP Phones with Headset	Quarterly
6	Printer , scanner and copier(multi-function)	Monthly
7	Laser jet printer	Monthly

S No	Item/ Description	Preventive Maintenance Schedule
8	Heavy Duty printer	Monthly
9	VHF static radio device	Monthly
10	Lattice Mast and antenna for VHF static set	Monthly
11	Radio Gateway	Monthly
12	Digital Radio Channel License for RoIP Server	Monthly
13	2 Meeting rooms with equipment of capacity 20 people	
14	Display device	Quarterly
15	Audio System	Quarterly
16	Control System	Quarterly
17	Smart TV - 32 Inch.	Quarterly
18	Smart TV - 42 Inch	Quarterly
19	Printer , scanner and copier(multi-function)	Monthly
20	Network Rack	Quarterly
21	Managed Access Switch 24 ports	Quarterly
22	Intranet Router - 500Mbps	Quarterly
23	UPS 20 kVA	Monthly
24	Biometric	Quarterly
25	Auto-phase sequence corrector in OMCs	Quarterly
26	voltage control stabilization at OMCs	Quarterly
27	Smartphone for Vehicles	Monthly
28	GPS devices for Vehicle	Quarterly
29	Vehicle Mobile Responder	Monthly
30	IP Phones with Headset	Quarterly
31	Desktop with 2 Monitors	Quarterly
32	24 Port Switch	Quarterly
33	Router 20Mbps	Quarterly

S No	Item/ Description	Preventive Maintenance Schedule
34	UPS 1KVA with 30min backup	Monthly
35	MDT 7" for GRP Station	Monthly
36	IP Phones with Headset(3 New and 6 old)	Quarterly
37	Desktop with two Monitors	Quarterly
38	24 Port Switch at SRP stations	Quarterly
39	24 Port Switch at IG,DIG and HQ	Quarterly
40	Router 20Mbps	Quarterly
41	UPS 1KVA with 30min backup	Monthly
42	Camera for Video Conferencing	Monthly
43	VC at SP office	Monthly
44	Desktop with single Monitors	Quarterly
45	24 Port Switch	Quarterly
46	Router 20Mbps	Quarterly
47	UPS 1KVA with 30 min backup	Monthly
48	IP Phones with Headset	Quarterly
49	Camera for Video Conferencing	Monthly
E	**Miscellaneous**	
1	Dish TV Connection for Television	Quarterly
2	Furniture at DCR	Half Yearly
F	**Cyber Security Assets**	
1	Web Application Firewall	Quarterly
2	NextGen Firewall	Quarterly
3	Security Incident & Event Management (SIEM)-(AMC only)	Quarterly
4	Data Leakage Prevention(DLP)	Quarterly
5	Network Access Control(NAC)	Quarterly
G	**In-fleet Components_4W PRV**	
1	MDT Cradle	Quarterly

S No	Item/ Description	Preventive Maintenance Schedule
2	GPS/AVLS Device (one Per Vehicle)	Quarterly
3	Smart Mobile Phone	Monthly
4	Body worn Camera	Monthly
5	32GB Surveillance grade SD Card Class10	Monthly
6	Docking Station/Charger	Monthly
7	Roof top PTZ Camera	Monthly
8	MNVR with 1TB Storage	Monthly
9	PTZ Control unit with Keyboard	Monthly
10	7" LCD Monitor	Monthly
11	Accessories for fitting the Camera	Monthly
H	**Connectivity**	
1	RF Link Testing	Daily
2	Activation of CUG Mobile	Monthly
3	Redundant Connectivity through RF line	Quarterly
4	Redundant Connectivity through CUG Mobile	Quarterly

9.31 Functional Requirement Specifications - FRS

A. Contact Center Solution

1. IPPBXs

IPPBX Server and Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
IPSG.REQ.001A	Overview of Solution	IPPBX is a software-based appliance that transfer calls received on SIP channels to the IP network		
IPSG.REQ.002A	Overview of Solution	The software identifies the correct location and automatically route the calls to the respective UP112 officers		
IPSG.REQ.003A	Overview of Solution	IPPBX with voice gateway will be available at UP112 HQ as well as 2 OMCs		
IPSG.REQ.004A	Overview of Solution	All outbound calls from the UP112 gets routed to SIP channels through IP PBX system		

IPPBX Server and Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
IPSG.REQ.005A	Overview of Solution	Provision to broadcast “Greeting Message” whenever a call is received on the system		
IPSG.REQ.001	General Requirement	IPPBX (Hardware & Software) shall be provided in high availability configuration.		
IPSG.REQ.002	Technology	The system should support IP or SIP as well as TDM. The TDM can be supported through an external Gateway.		
IPSG.REQ.003	Interface	Should be compatible with all telecom interfaces or Telecom Service providers		
IPSG.REQ.004	Type of Interfaces	It should be compatible with ISDN PRI, Analogy trunks, H.323 trunk, SIP trunk. It should also provide facility to		

IPPBX Server and Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		integrate with GSM, Radio devices.		
IPSG.REQ.005	Type of Extension Support	Analogy, Digital, IP, SIP(3rd party SIP phone), Wireless IP Phone		
IPSG.REQ.006	Expansion of Extensions	IP Telephone extensions should be expanded based on quantities of data switch ports available.		
IPSG.REQ.007	System Design	The IP PBX should be modular, expandable, embedded IP server-gateway/server-based architecture, having Unix or Linux or equivalent operating system software based platform. The system shall have hot standby/Active-Active arrangement so that it should continue to		

IPPBX Server and Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		operate in case of failure or maintenance of main processor or power supply or interfacing card or CPU etc. The system should support IP or SIP as well as TDM. The TDM can be supported through an external Gateway.		
IPSG.REQ.008	Conferencing	Conference bridge that can manage multiple calls (min 5) simultaneous conferees.		
IPSG.REQ.009	ACD And CTI Support	Support for ACD Call Centre with CTI and advance call routing		
IPSG.REQ.010	Call Center Communication Support	Support Standard SIP based IP Platform, Session Initiation Protocol over an MPLS or Multiple Label Switching Protocol for		

IPPBX Server and Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		connectivity of call center to other call center communications,		
IPSG.REQ.011	Outbound Calling Support	The system shall allow outbound calling from the IP Phones.		
IPSG.REQ.012	General Requirement	The system shall support local announcements and music on hold.		
IPSG.REQ.013	General Requirement	The system shall be able to provide interface to ISDN PRI		
IPSG.REQ.014	Features	The system shall be able to provide following features like Basic Call Setup, Name and Number Support, Transit Counter, Called or Calling or Busy or Connected Name and Number, Name Identification, Diversion (Call forwarding),		

IPPBX Server and Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		Diversion (Call forwarding) with Reroute, Call transfer.		
IPSG.REQ.015	General Requirement	The system shall have inbuilt Web/Application-based software for administration and maintenance of the system. It shall provide the following features: ► The software shall provide GUI based interface for configuration and management of the system. ► The Software shall provide real-time information or alerts and reports regarding health status e.g., up, or down status, performance & resource utilization		

IPPBX Server and Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		statistics etc. of the system and its components. ► The system shall maintain the accounting and authorization logs of the users accessing the components of the telephony system. The logs shall include information about users who have login into the system. ► It shall be possible to schedule tasks. The tasks could be one or more operations that the user can specify to run at a predetermined date and time. ► It shall provide reports about station alarms, trunk analysis, processor occupancy, system capacity etc.		

IPPBX Server and Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		The system shall have inbuilt Web/Application-based software for administration and maintenance of the system. It shall provide the following features: ► The software shall provide GUI based interface for configuration and management of the system. ► The Software shall provide real-time information or alerts and reports regarding health status e.g., up, or down status, performance & resource utilization statistics etc. of the system and its components.		

IPPBX Server and Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
IPSG.REQ.016	General Requirement	The IP PBX system should provide complete inbuilt encryption capabilities or features without any external firewall, with the ability to encrypt all traffic (media and call control signalling) between IP phones, soft phones, call controllers and all other associated endpoints via a strong encryption algorithm like IPsec or SRTP etc.		
IPSG.REQ.017	General Requirement	The system shall provide features viz. silence suppression, comfort noise and voice activity detection.		

IPPBX Server and Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
IPSG.REQ.018	General Requirement	It shall provide some features as given below but not limited to these feature list. It can be expanded further based on requirement ► Call forward all, call forward while busy, call forward if no answer ► Call hold, Call Drop, and retrieve ► Call Waiting and Retrieve (with configurable audible alerting) ► Call Join ► Call status (state, duration, number) ► Conference for at least 5 parties ► Missed call information on IP phone ► Directory dial from phone ► Hands-free, speakerphone ► Last number redial		

IPPBX Server and Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		► Malicious Call ID and Trace ► Abbreviated Dial, Speed Dial		
IPSG.REQ.019	General Requirement	The system should have IP address and connected to the network		
IPSG.REQ.020	General Requirement	The system must support log services for both Internal and External commands		

IPPBX Server and Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		and configuration history for 30 days		
IPSG.REQ.021	General Requirement	Call Details Record (CDR) solution available for CO and event supervisor should be extended to all the Line phones at UP112 HQ		
IPSG.REQ.022	General Requirement	During non-availability of communication officers in case of SIP for handling calls, the calls from citizens should land on basic extensions.		
IPSG.REQ.023	General Requirement	CDR solutions to be upgraded for extended feature of fetching extension numbers		

IPPBX Server and Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
IPSG.REQ.024	General Requirement	Integration of SIP channels and failover to land line as communication channels. There should be flexibility to design the configuration of call landing. Also, all the caller related details should be available to the communication officer at basic extension		
IPSG.REQ.025	General Requirement	Introduction of Session Initiation Protocol (SIP) based IPBX would ease in multiple channels landing directly from Telecom service providers		
IPSG.REQ.026	Scalability	IP PBX system should be scalable in future to receive calls from multiple integrations		

IPPBX Server and Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
IPSG.REQ.027	Redundancy	Redundancy should be built in the IP PBX system to avoid single point of failure at OMCs as well		
IPSG.REQ.028	Support	24x7 round-the-clock monitoring by Systems Diagnostic Tools where applicable, to respond to system-generated alarms on Supported Products		

2. IP Phone Softphone Licenses

IP Phone Softphone Licences				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
IPSP.REQ.001A	Overview of Solution	MSI to provide with Soft Phone Application for Android/Window/iOS which		

IP Phone Softphone Licences				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		shall be a SIP-based softphone that will use Wi-Fi or cellular data network connection to make and receive voice and video calls, send messages and see user presence		
IPSP.REQ.001	General Requirement	It should be bundled packet with IPPBX System		
IPSP.REQ.002	General Requirement	It shall be provided to all officer with login credentials and allow the authorized user to make call using softphone without IP Phones		
IPSP.REQ.003	General requirement	It should support VOIP, Video, Instant Messaging & Presence		
IPSP.REQ.004	General Requirement	This application shall have all the available features of IP phones		

IP Phone Softphone Licences				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
IPSP.REQ.005	General requirement	Should support Virtual Desktop Infrastructure (VDI), Windows & Non-Windows OS		
IPSP.REQ.006	General requirement	Should Support H.323 & SIP		
IPSP.REQ.007	General requirement	Should support Lan, VPN Less Mobility & Quick Access to common controls		
IPSP.REQ.008	General requirement	LDAP integration for directory lookup		
IPSP.REQ.009	General requirement	Should Provide Telephony (Dial, Answer, Drop, Transfer, Conference, Hold, etc.) and Media Controls (Mute, Volume, Agent Greetings, etc.)		

3. Outbound Dialler

Outbound Dialler				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
OBD.REQ.001A	Overview of solution	This software shall be used for the making outbound calls from the officers to return missed call, call in case of SMS, email, or other input sources		
OBD.REQ.002A	Overview of solution	Feedback calls: The outbound dialler software have a feature to make calls to the caller whose complaints as per system have been closed. The feedback connected through		

Outbound Dialler				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		the ACD with the available communication officer		
OBD.REQ.003A	Overview of solution	Conference facility: This facility is required in situations wherein the officer makes a conference call with the caller and the field officer from police to connect both on same call for more clarification.		
OBD.REQ.001	General Requirement	The dialler should be an integrated part of the proposed contact center solution		
OBD.REQ.002	General Requirement	The Officer should be able to dial the distress caller number in case of emergency		
OBD.REQ.003	General Requirement	The dialler should support outbound preview dialling, either automated or Officer-initiated		
OBD.REQ.004	General Requirement	The dialler should provide campaign management tool for		

Outbound Dialler				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		supervisors to manage the campaigns		
OBD.REQ.005	General Requirement	The dialler should have the capability to fetch missed calls data from the ACD and dial out whenever the Officer is available		
OBD.REQ.006	General Requirement	The system should be able to perform a screen pop with caller information based on the campaign		
OBD.REQ.007	General Requirement	The dialler should support campaign management for data selection.		
OBD.REQ.008	General Requirement	The dialler should support Do not call list		
OBD.REQ.009	General Requirement	In case any citizens redial 112 number, post call disconnects or call failure, and is finally able to connect with UP112.		

Outbound Dialler				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		Then, the number that got reconnected should be deleted from outbound dialler queue		

4. Automatic Call Distributor (ACD)

Automated Call Distributor				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
ACD.REQ.001A	Overview of the solution	Routing of the calls to UP112 centre and the available Communication Officers (COs) will be carried out by ACD		
ACD.REQ.002A	Overview of the solution	ACD employ a rule-based routing strategy		

Automated Call Distributor				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
ACD.REQ.003A	Overview of the solution	ACD enable to identify available COs and transfer the call accordingly		
ACD.REQ.004A	Overview of the solution	Call routing to the officers is based on the “longest idle basis”		
ACD.REQ.005A	Overview of the solution	ACD seamlessly integrate with IP PBX system		
ACD.REQ.001	General Requirement	ACD (Hardware & Software) shall be provided in high availability configuration.		
ACD.REQ.002	General Requirement	ACD should be capable to identify Officers availability into the state call center and route the call to the identified call center. ACD should support selective call routing based on		

Automated Call Distributor				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		Officer capability. E.g., 112, 181 and 108		
ACD.REQ.003	General Requirement	The ACD system shall be able to handle call & IP Phone as per capacity defined in scope		
ACD.REQ.004	General Requirement	ACD functionality should be supported to propose Operating system		
ACD.REQ.005	General Requirement	System should support skill base routing, multiple group support, priority handling and Queue status indicator. It is desirable that calls to certain trunk groups or to certain dialled numbers be assigned a higher priority than other calls and that calls which overflow from another split be queued ahead of other calls.		

Automated Call Distributor				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
ACD.REQ.006	General Requirement	System should support all call center COs as per requirement on a server and can be scalable by 50% minimum of existing Officer		
ACD.REQ.007	General Requirement	The ACD should support help or assist on COs phone. COs can use this functionality to request help from the split supervisor. This functionality automatically dials the split supervisor's extension and connects the COs to the supervisor. Current call should go on hold as the COs use this functionality.		
ACD.REQ.008	Call overflow	The system should support call overflow routing e.g., if there is a queue in particular ACD group and another group is sitting idle, system should be able to transfer the calls to another group based on the		

Automated Call Distributor				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		settings defined by the administrator.		
ACD.REQ.009	Virtual Seating or Free Seating	The proposed system must support the concept of virtual seating. COs can log-on from any "soft phone" instrument within the system. COs on the proposed system will be logically defined, rather than requiring a "soft phone" extension and termination. Each CO on the system must have an individually assigned log- on identification number which permits individual statistics to be collected by the ACD management information system.		
ACD.REQ.010	General Requirement	Automatic call distributor device should have capability to distribute the calls based on Skill level of the COs like		

Automated Call Distributor				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		efficiency of the COs and workload		
ACD.REQ.011	General Requirement	Automatic call distributor device should have Least Occupied COs details		
ACD.REQ.012	General Requirement	Automatic call distributor device should have some functionality where Supervisor can observe the COs pattern or silently monitor the COs.		
ACD.REQ.013	General Requirement	Automatic call distributor device should have functionality to provide best service to the caller like listen only, listen, and talk only etc.		
ACD.REQ.014	General Requirement	Automatic call distributor device should have local treatment for IP & ISDN		

Automated Call Distributor				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
ACD.REQ.015	General Requirement	Automatic call distributor device should allow to compare specified skills, identify the skill that will provide the best service to a call, and deliver the call to that resource. If no COs are currently available in that skill, the call is queued. To respond to changing conditions and operate more efficiently		
ACD.REQ.016	General Requirement	Automatic call distributor device should have expected Time for waiting in routing and		
ACD.REQ.017	General Requirement	Automatic call distributor device should have Call Center Location Preference Distribution		
ACD.REQ.018	General Requirement	Automatic call distributor device should have Call Center Support for Locally Sourced Music and Announcements for calls that have been put on wait		

Automated Call Distributor				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
ACD.REQ.019	General Requirement	Automatic call distributor device should have an integrated call center functionality for IP or non-IP COs.		
ACD.REQ.020	General Requirement	Automatic call distributor device should support load balancing of all calls		
ACD.REQ.021	General Requirement	Automatic call distributor device should support for multiple announcements be played to a caller.		
ACD.REQ.022	General Requirement	Automatic call distributor device should be able to track remote activity. The tracking for off-premises Officers must be the same as that for on-premises COs.		
ACD.REQ.023	General Requirement	Automatic call distributor device should support to provide COs to be seen in a real-time view on a supervisor’s workstation &		

Automated Call Distributor				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		Officer's activity should also show up on standard report		
ACD.REQ.024	General Requirement	Automatic call distributor device should redirect unanswered calls.		
ACD.REQ.025	General Requirement	Automatic call distributor device should provide the capability to the supervisors for logout Officers from their own voice terminal without having to go to the COs desk & it could be possible from a remote location.		
ACD.REQ.026	General Requirement	The proposed system should support all states call center environment with multiple distinct sites as a single virtual call center operation. It should also have a capability to allocated call between sites based upon COs skills, COs		

Automated Call Distributor				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		availability, queue times, and other criteria.		
ACD.REQ.027	General Requirement	Automatic call distributor device should support automated load-balancing capabilities and customized conditional routing capabilities. Proposed system should allow the comparisons to be made in queue conditions before routing calls so that split, or skills are not overloaded, or it can be made in queue conditions after routing calls to determine if calls should be re-routed to alternate destinations.		
ACD.REQ.028	General Requirement	Automatic call distributor device should be able to collect request information, such as a zip code or account code before the call is sent to a CO and then route the call based		

Automated Call Distributor				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		upon that information. The system must have the ability to prompt a caller for information in terms of digit		
ACD.REQ.029	General Requirement	All calls for each ACD group (Skilled or Hunt) must be redirected to a different extension after hours. Supervisors must be able to activate this from their voice terminal. Each group may have different hours of operation.		
ACD.REQ.030	General Requirement	Automatic call distributor device should provide alternate routing automatically based upon time of day and day of week		
ACD.REQ.031	General Requirement	Automatic call distributor device should use the estimated wait time or average speed of answer to make routing decisions.		

Automated Call Distributor				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
ACD.REQ.032	General Requirement	The routing commands of the Automatic call distributor device should obtain information from another source like TSP interface or a database before routing the call		
ACD.REQ.033	General Requirement	Both COs and supervisors should be notified via the telephone indicators when thresholds are reached for individuals and groups.		
ACD.REQ.034	General Requirement	Automatic call distributor device should have a capability for COs to record personalized greetings that can be played to the caller prior to connection to the COs.		
ACD.REQ.035	General Requirement	Calls can be queue to an individual CO. CO should be notified, and a delay announcement be provided if the call queues for an		

Automated Call Distributor				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		individual CO who is on another call.		
ACD.REQ.036	General Requirement	Automatic call distributor device should support to force the CO to be put into an ACW (After call work) state for a predefined period to provide rest time between calls, pace calls to the Officers, or limit the amount of time a CO spends in completing wrap-up work		
ACD.REQ.037	General Requirement	Automatic call distributor device should be capable to define certain COs as “reserve” CO for certain skill sets.		
ACD.REQ.038	General Requirement	When interflowing calls between sites, automatic call distributor device should take advantage of Network Call Transfer and Deflection provided by the public switch telephone network to redirect an incoming ISDN call without		

Automated Call Distributor				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		requiring trunks to be tied up at the original destination after the call rerouting takes place.		
ACD.REQ.039	General Requirement	Automatic call distributor device should allow to change or add or remove COs skill dynamically while COs are on calls.		
ACD.REQ.040	General Requirement	Call should be routed to IP Phone and call related signal should be exchanged with the PC attached to the respective COs		
ACD.REQ.041	General Requirement	ACD or CTI should provide interface to signal call release, call hold, requests from call taker COs		
ACD.REQ.042	General Requirement	ACD system shall allow a call facility for CO. If a call taker enters clerical mode, that will be signalled to ACD call will not		

Automated Call Distributor				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		be routed to that CO until it becomes free.		

5. Computer Telephony Integration (CTI)

Computer Telephony Integration (CTI)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
CTI.REQ.001A	Overview of Solution	CTI shall allow interaction between telephone and a computer to be integrated		
CTI.REQ.002A	Overview of Solution	CTI run on a server and act as a common interface for integration of all the software applications deployed		
CTI.REQ.003A	Overview of Solution	CTI functionalities support relevant screen pop-ups on the officers' screen based on call location detection		
CTI.REQ.004A	Overview of Solution	CTI pass events and information of officers' status		

Computer Telephony Integration (CTI)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		and changes in officer status as well as incoming calls to the computer applications		
CTI.REQ.001	General	The CTI shall be capable of integrating with other application like CRM as per requirement.		
CTI.REQ.002	General	The OS hosting on the core CTI functionality shall be a flavour of UNIX or LINUX or Windows or any other supporting OS		
CTI.REQ.003	General	The CTI platform shall be able to provide the caller's CLI (Caller Identification) information. It shall be possible to send & populate Officers Desktop with CLI information		
CTI.REQ.004	General	The CTI link shall be able to pass events and information of Officer states and changes in Officer states as well as incoming calls to the computer applications, e.g.: - If the		

Computer Telephony Integration (CTI)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		customer calls from the same no. from which caller had called earlier (registered or unregistered), the CTI platform shall be able to automatically fetch and display at least last 5 service requests details for that customer.		
CTI.REQ.005	General	The CTI shall maintain the accounting and authorization logs of the users accessing the components of the telephony system. The logs shall include information users who have logged-in into the system and the specific commands entered by them.		
CTI.REQ.006	General	Management Access to the system shall be secure. Access mechanisms viz. SSH, HTTPS shall be used to facilitate user authentication, authorization, accounting (AAA) using LDAP or Active directory or Directory services etc. and provide		

Computer Telephony Integration (CTI)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		information about users who have login into the system and the specific commands entered by them.		
CTI.REQ.007	General	It shall have web-based GUI console for administration, configuration & management of the system, Real-time information or alerts and reports regarding health status e.g., up, or down status, performance & resource utilization statistics etc. of the system shall be available through this console.		
CTI.REQ.008	General	The system shall be SNMP (Simple Network Management Protocol) manageable such as SNMP v1, SNMP v2c and SNMP v3 protocols. It shall be able to send SNMP traps to the configured Network Management System (NMS).		

Computer Telephony Integration (CTI)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
CTI.REQ.009	General	All calls pertaining to social media platforms, such audio and video calls from WhatsApp and skype shall be catered by contact center		

6. Voice Recording System and Quality Monitoring

Voice recording and Quality monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
VRS.REQ.001A	Overview of Solution	The voice recording happens for all incoming and outgoing calls		
VRS.REQ.002A	Overview of Solution	System store voice recording of entire conversation between caller and officer both for incoming call and outgoing call even when calls are		

Voice recording and Quality monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		transferred from one center to another Control room of the UP State		
VRS.REQ.003A	Overview of Solution	Voice recording of all the calls is maintained at the DC/DRC for the period of entire project. One-month live call data also be maintained post which it can be archived. Critical data is flagged even after archival on SAN based suitable accessible storage. This will help in post event analysis, if required for judicial purposes		
VRS.REQ.004A	Overview of Solution	System needs to be designed such that unauthorized person cannot modify/ move/ delete any voice recordings		
VRS.REQ.005A	Overview of Solution	Authorized personnel from UP112 shall be able to access the recordings as		

Voice recording and Quality monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		required by them. The recording shall be available to the staff without any delay.		
VRS.REQ.006A	Overview of Solution	Recording should be parallel available from CO terminal as well as live recording should be fetched from recording backup location		
VRS.REQ.007A	Overview of Solution	System enables search for the voice recordings through various fields and filters such as date, time, caller name, location, case file number, officer etc.		
VRS.REQ.001	Recording	Voice Recording system shall be provided in high availability configuration.		
VRS.REQ.002	Recording	The recording software must use the recording interface provided by ACD or PBX API and should		

Voice recording and Quality monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		provide 100% voice call recordings.		
VRS.REQ.003	Recording	The recording software must provide a single license that can support recording on all IP Phones.		
VRS.REQ.004	Recording	The recording software must be able to record calls coming on any type of trunk line like PRI/SIP and system should also record internal calls.		
VRS.REQ.005	Recording	The recording software should also be able to record IP endpoints		
VRS.REQ.006	Recording	The software should support SIP, IP and TDM (Time Division Multiplexing) endpoints		
VRS.REQ.007	Recording	The software should record inbound calls and outbound calls		

Voice recording and Quality monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
VRS.REQ.008	Recording	The software should support for search and replay of calls		
VRS.REQ.009	Recording	The software should have Rules-based storage and recording		
VRS.REQ.010	Recording	"Tag" or classify calls with user-defined labels for simplified search and replay		
VRS.REQ.011	Quality Recording	The software shall provide screen recording by 5% of total recording for quality and training purpose		
VRS.REQ.012	Quality Recording	The software should allow for voice only, data only, or voice and data recording based on specific event triggers		
VRS.REQ.013	Quality Recording	The software should support selective recording based upon user-defined business rules		

Voice recording and Quality monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
VRS.REQ.014	Quality Recording	The system should show the status of the Officers, which Officers are logged on.		
VRS.REQ.015	Quality Recording	The software should allow for the automatic refresh of the logged-on Officer display.		
VRS.REQ.016	Quality Recording	The software should be able to provide real-time Officer monitoring.		
VRS.REQ.017	Storage	The software shall be able to provide online, and offline storage capability in any combination.		
VRS.REQ.018	General Requirement	Should provide facility to store voice digitally in central database or to a hierarchical file system in any of the standard format like wav, mp3 etc.		
VRS.REQ.019	Storage	Archival to network attached storage or network		

Voice recording and Quality monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		drive should be included as a standard component with the recording platform		
VRS.REQ.020	General Requirement	Recording of each call should be stored in the system. Recording should be available for citizen to download the file through citizen mobile application also.		
VRS.REQ.021	General Requirement	100% call recording should be available for all internal, external, or basic extension-based calls on real time basis without any delay		
VRS.REQ.022	General Requirement	All calls recorded by system should have feature of parallel listening enabled		

7. Contact Center Reporting System

Contact Center Reporting System				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
RS.REQ.001A	Overview of Solution	Reporting system has a provision to provide the Contact Center reports like call handling, Average handle time of the call etc.		
RS.REQ.002A	Overview of Solution	System enables to export the report in different kind of format like pdf, text, xls etc.		
RS.REQ.001	General	The reporting system (hardware or software) shall be provided in hot standby configuration.		
RS.REQ.002	General	Reporting System Should be able to support Automatic call distributor (ACD)		
RS.REQ.003	General	The system should support up all the configure Officers		
RS.REQ.004	General	The system shall provide both real-time information and historical reports.		

Contact Center Reporting System				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
RS.REQ.005	General	The system shall allow the user to set threshold on the Contact Center parameters, which shall be notified in the form of different colour on the screen of the users		
RS.REQ.006	Search or filter Criteria	There shall be provision to sort and filter the reports based on various criteria via date and time, Officer ID etc.		
RS.REQ.007	Report Type	Following category of real-time information & historical reports shall at least be available with specific dates and time with options of hourly, daily weekly, and monthly, yearly in report criteria. i. ACD Reports: Officer Login and Logout Reports ii. Officer State Changes Report iii. Queue Reports iv. Abandon Call Reports		

Contact Center Reporting System				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		v. Call by Call Details Report vi. Officer or Call taker Performance Reports: Average Hold Time per Officer or call taker, Average Call Handle Time per Officer, No. of calls handled per hour or per shift per Officer, Login & Logout duration per Officer vii. Call volume reports - number of calls during each hour, number of abandoned calls, number of incomplete calls, busy signals and rollovers, length of calls, percentage of calls answered and serviced vs. total calls received, etc.		
RS.REQ.008	Summary and Detailing	Both summary and detailed reports shall be available by the system		
RS.REQ.009	Detail Report	Display call detailed reports including caller numbers,		

Contact Center Reporting System				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		dialled number, call transfers etc.		
RS.REQ.010	Outcalls Detail	Allow reports on outcalls made using system to which number and by which Officer or call taker		
RS.REQ.011	Call's data Detail	Provides detailed data for calls in which the caller waited in queue, using the following parameters: i. Queue time ii. Caller abandons iii. Specified set of skills		
RS.REQ.012	Hold Call Detail	Provide details of calls in which the caller is placed on hold, using the following parameters: i. Hold time ii. Number of holds per call iii. Caller abandoned from hold iv. Officer or Call taker disconnected first		

Contact Center Reporting System				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
RS.REQ.013	Customization reports feature	The reporting platform shall provide report customization capability.		
RS.REQ.014	Report format	It shall be possible to export, save and print the reports in various formats viz. Excel, pdf, and text files		
RS.REQ.015	Statistics	The system shall provide Officers with the real time statistics on their desktop in form of a wallboard. Officers should get a notification if they exceed any pre-defined thresholds in form of a colour change on this wallboard. e.g. the wallboard display changes if a live call duration exceeds a threshold defined for calls		
RS.REQ.016	Schedule Report	It shall have feature to schedule generation of reports and automatic delivery of scheduled reports to e-mail. It shall also allow automatic		

Contact Center Reporting System				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		delivery of both manually generated and scheduled reports to a file directory or folder		
RS.REQ.017	Archive	It should be possible to archive or store certain data for more than one year. Such selected data could be electronically flagged to enable easy classification and then separate storage also.		
RS.REQ.018	BI Integration	System should be capable to integrate the data with BI tools for data analysis		
RS.REQ.019	BI Integration	System should be redesigned, and all the details shall be available for single view for better monitoring and performance tracking. Even Database level access is required for fetching data as per requirement or reporting		

Contact Center Reporting System				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		system needs to be redesigned completely.		
RS.REQ.020	BI Integration	Search mechanism would be built to index the files and search the available structured and unstructured data		
RS.REQ.021	General Requirement	Contact center reporting system shall be available to relevant officers on web browser via link with login credentials		

8. Multimedia System (Email, Chat, SMS)

Multimedia System				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
MS.REQ.001A	Overview of Solution	Multimedia System act as an interface to receive inputs from various sources such as SMS, email, chats etc. and convert the input to CAD format		
MS.REQ.002A	Overview of Solution	It sends notifications to the screen of the identified Communication Officer		
MS.REQ.003A	Overview of Solution	System enables to detect the location from the GPS coordinates received from mobile application, IoT, panic button of vehicles etc.		
MS.REQ.004A	Overview of Solution	System has the capability to register the mobile applications/ IoT/ devices/ panic buttons etc. before the data can be received from the same		
MS.REQ.001	General Requirement	Multimedia system shall be provided in high availability configuration		
MS.REQ.002	General Requirement	The system should allow non-voice communication channel like email, web chat and SMS to be routed to Non-voice Officer based on skill set and Officer availability		

MS.REQ.003	Email Channel	System should give queuing priority to emails received from users		
MS.REQ.004	Email Channel	System should assign different queuing priorities to the first email a user sends and all subsequent emails they send as part of the same conversation		
MS.REQ.005	Email Channel	System should automatically inform the contact (via email) that their email has been received		
MS.REQ.006	Email Channel	System should be capable to distribute mails based on keywords in the subject or the body of the emails. Different rules can be used to route the mail to the right Officer or queue		
MS.REQ.007	Chat Channel	The Web chat solution is required for users that prefer web chat as a medium to communicate with the Officer		
MS.REQ.008	Chat Channel	The web chat solution must route the chat user to the respective non voice Officer in the relevant state		
MS.REQ.009	Chat Channel	An administrator should be able to configure the standard chat messages that will be presented during establishment of a chat session		
MS.REQ.010	SMS	The proposed solution is required for the users that prefer SMS as a medium		

MS.REQ.011	General	Required multiple communication channels shall be supported through a unified platform		

9. Number Masking

Number Masking				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
NM.REQ.001A	Overview of Solution	The communication between Caller and PRVs should be route through UP 112 Contact center to avoid misuse by sharing the direct contact number of PRV		

Number Masking				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
NM.REQ.001	Masking	Number masking shall be integrated with telephony interface with citizen and PRV interface at both the sides		
NM.REQ.002	Centralized Calling	Caller number and PRV number should be masked, and the communication should be done using the dedicated centralized number for contact center at Control room. Application shall have feature of activating or deactivation number masking of PRV to Caller and vice versa on need basis		
NM.REQ.003	Recording	All the voice calls between PRV to Caller and vice versa should be recorded at the voice logger of Control room.		
NM.REQ.004	Failover	In case of any issue with Number Masking Framework, there should be an admin-initiated failover mechanism using which all the numbers should be automatically demasked and relevant SMS Should be sent to Complainant & PRV		
NM.REQ.005	Reference	The Number masking solution shall be capable of handling Emergency Project (UP112) handling more than 25,000 event Per day.		

Number Masking				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
NM.REQ.006	Recording	Voice recording between Citizen and PRV staff shall also be available for 15 days and MSI has to provision the storage for the same		

B. Computer Aided Dispatch (CAD) – Web and Mobile Based

1. Computer Aided Dispatch (CAD)

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.001A	Overview of the solution	The CAD System will display the information entered by the CO for actionable calls. It would display the event details as mentioned by the CO		
CAD.REQ.002A	Overview of the solution	The CAD will dispatch PRVs based on a predefined algorithm. The conditions will include actionable events type, response action methodology, day, and time of occurrence, PRV availability and number of vehicles required, jurisdiction, proximity, specialization,		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
		available equipment on duties resources and logical AND/OR combination within rules.		
CAD.REQ.003A	Overview of the solution	The CAD shall be freely customizable to include such varying SOPs and operational requirements		
Call Taking Module				
CAD.REQ.001	All Communication Channel	The CAD software should be capable to receive call (Mobile, Landline), SMS, chat,Wattsapp, email, VOIP (like Skype to Skype), social media like Facebook, Twitter, IOT (internet of things) sensors, panic button and mobile apps to create an appropriate case and send the relevant case for Auto Dispatch.		
CAD.REQ.002	Communication Channel – Call	1. Automatic display of data on CAD: The software should be able to display caller name, caller number and caller address on CO's desktop from Location Detection Interface or ELS/ ALS Data 2. Manual Data entry: CO should be capable to enter the location of the caller on CAD Screen and specify/ select gender of the citizen making call.		
CAD.REQ.003	Communication Channel – SMS	The software should be able to automatically create an event using SMS data (Phone No. & Message) as the SMS shall get displayed on the officer desktop		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.004	Communication Channel – SMS	The CO should be able to assess the SMS case and send the case to Outbound call officer or Event supervisor after assessment		
CAD.REQ.005	Communication Channel – Email	The software should be able to automatically create a case using Email data (Email content) with attachment if any and display on the officer desktop.		
CAD.REQ.006	Communication Channel – Email	The software should be able to send the case to Outbound dialler or event supervisor after assessment.		
CAD.REQ.007	Communication Channel – VOIP	The software should be able to be integrated with VOIP channel like Skype where officer can speak with the users on skype and can-do chat on Skype and officer can create a case into CAD based on case assessment.		
CAD.REQ.008	Communication Channel – IOT	The software should be able to receive the data from Internet of things (IOT) devices like sensors, panic button with location of the user & display on the officer desktop.		
CAD.REQ.009	Communication Channel – IOT	The officer should be able to send the case to the Outbound dialler Or Event Officer after assessment		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.010	Communication Channel – Chat	The software should have a functionality where officer can receive the chat which is initiated by the web user in real time through UP-112 portal. The officer should be able to chat with the user in real time with the user.		
CAD.REQ.011	Communication Channel – Chat	If an officer is offline, then the citizen should be able to send the messages to chat window and message should be received as an email to officer		
CAD.REQ.012	Communication Channel – Chat	The software should be able to automatically create a case using Chat history (Message and any attachment during chat) and display on the officer desktop		
CAD.REQ.013	Communication Channel – Chat	The software should be able to create a case with chat history and should be able to send the case to Outbound dialler Or Event Officer after assessment.		
CAD.REQ.014	Communication Channel - social media	The CAD should be able to create case with data received from Facebook, Twitter, WhatsApp, or any social networking site with the help of two open-source API. These other two open-source API will be decided at later stage. This case will be created manually by officer into CAD software		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.015	Merger the cases for voice and social media	The CAD should merge the cases if the citizen is calling from call and sharing the data through social media (Facebook, twitter, WhatsApp) like images, audio file, video file in the system. Data should be collated in one case in these kind of scenarios		
CAD.REQ.016	Communication Channel - Mobile Application	The CAD software should be integrated with Mobile Apps (registered with NexGen UP112 to receive location of the caller and caller number.		
CAD.REQ.017	Call Classification	The officer should be able to classify the case into distress case, enquiry case, departmental case, administrative, crank case, outbound call case etc. All such Classifications must be logged in the system. NexGen UP112 can add more classification at later stage. System will facilitate the CO to classify and transfer the call to available CO and Event Supervisor based on regional languages and dialects of UP state. This will ease the communication with users calling form different geo region of the state		
CAD.REQ.018	Call Transfer or Call Forward	CAD will provide feature to classify the volunteers of different foreign languages like Spanish, German, Thai, Nepali etc. available at various time slots round the clock. CO should be able to transfer and arrange		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
		conference call between event supervisor and volunteer of foreign language to assist the foreigner CAD officer should be capable to transfer the call to the contact center officer in other states or same state or transfer to dialled number by the officer Caller's Call should not be disconnected during call forwarding or Transferring into the system		
CAD.REQ.019	SMS Case Transfer	A case to be considered where SMS is sent in Hindi and can't be read by the officer. Provision for profile of officers to be available to forward the SMS to appropriate officer		
CAD.REQ.020	Duplicate Calls	An incident may attract more than one call, but each call is important as it may give details about eyewitnesses and other supportive evidence. The system should suggest the possibility of a duplicate call based on the location, time, classification etc. Duplicate calls should be cross referenced for easily retrievable through Grouping.		
CAD.REQ.021	Duplicate Calls	It should be possible to merge duplicate calls depending upon the situation. To achieve this, the system should have the capability for cross referencing		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
		of Case. Whenever a call is merged, the system should not generate a new dispatch.		
CAD.REQ.022	Duplicate Calls	The software should alert the communication officer, Dispatch officer, Supervisor etc. or about the possibility of a single incident - Duplicate call situation		
CAD.REQ.023	Voice Recording	Integration with Voice recording software provided by MSI. The voice recording solution shall be able to produce the voice recording of call on real time basis.		
CAD.REQ.024	Case History	In some cases, previous history of the caller can be important. It should be possible to create a reject list where crank callers could be added.		
CAD.REQ.025	Case creation and Appraisal	System should facilitate Case creation, by providing 'a drop-down menu for various functions like creation of a Case, files attachment, location of nearby Case and other information related to a Case should be recorded and updated.		
CAD.REQ.026	Soft Phone Integration	The software should have a capability of a Telephone window allowing officers to dial, answer, end a call, keep the call-in busy status, and free a specific call. The functionality should also provide the status of incoming and outgoing calls.		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
		Soft phone should have a feature to select the state for call forwarding or transferring or conference call.		
CAD.REQ.027	Emergency Call	The software should have capabilities to create Hot Calls like fire in a building, disaster emergency. The officer should fill minimum information for a Hot call. CO and Event Supervisor should receive the alert or notification for the same. Officer should be able to initiate action for quick response. To facilitate quick response to emergency calls or hot calls, there should be special and dedicated hot call button in the officer software.		
CAD.REQ.028	Case Status Display and Search	The officer GUI screen must be provided with 'Case Status Window' displaying the status of all Case like 'Pending', 'Open', 'Dispatched', 'Closed' etc. The software should be able to search the Cases using various search option. Like Case status, Case ID, phone number, Date & Time, over the time, Case Type etc.		
CAD.REQ.029	Archive Search	The officer should be able to search the archive records from the system.		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.030	Location of Interest (LOI)	Once a Location of the incident is marked in the map, the officer shall have the facility to see for various 'Location of Interest (LOI)' in the vicinity of a case location like nearest Hospital, Blood Bank, Fire brigades. (Applicable in Event Supervisor module also).		
CAD.REQ.031	Display of Station Name	The software should have the facility in the system to populate within it, the relevant Police Station name, Police Zone name (Based on Case Location through GIS), Police officers etc., Hospitals, Fire stations/Fire PRVs (Fire brigades), whenever a new case is created to save precious time in effective response to a distress call.		
CAD.REQ.032	Update Existing Case	The software should allow the officer to update or modify existing case details for any additional or supplementary information related to the same. Also, there should be provision to attach relevant files like pdf, Word etc. to the event, for ensuring an effective response.		
CAD.REQ.033	Alert Notification	Software should have capability to alert an officer or supervisor if a case is not attended in pre-defined time duration.		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.034	Pre-defined Q&A	A freely configurable structured query script should be available within the software to assist the officer with pre-defined Q&A to ask for during the call, SMS response and web response. Based on the Case and Case subtype, the response for officer should be prompted.		
CAD.REQ.035	User-defined Alarm	The application should be configured with user-defined alarm modules that will be flashed on all the other screens in case of major incident, for ex. Terrorist attack.		
CAD.REQ.036	Case Cancel or Close	The Case like rally should be expired automatically by the system once the time defined for the Case gets over or software should have a provision that supervisor can close or cancel or postponed the Case manually into the system		
CAD.REQ.037	Call back	Officer should be able to call back the caller with the click of the mouse.		
CAD.REQ.038	Caller Address conflict handling	It should be possible to find the numbers whose subscriber information and caller information recorded by the officer are different and generate a report for the concerned agency.		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.039	Case Acknowledgement	System should be capable to send an SMS to the caller stating the Case Number, acknowledgment, brief text of the complaint and caller or non-Caller can verify the status through email or SMS to Non-Emergency helpline		
CAD.REQ.040	Incident scheduling and Mapping	Incident-scheduling functionality should be available in proposed software for future Cases like, VIP Visit, Rally, Festival etc. The software shall have provisions of setting the date and time for the particular Case, automatic Case should be generated on that date.		
CAD.REQ.041	Incident scheduling and Mapping	The Scheduled Case feature should allow operators to create, edit, delete, and search for a scheduled Case.		
CAD.REQ.042	Language Support	It should be possible to switch between English, Hindi language. Software should have support for Hindi, English language. Display and input both functionality of given languages should be provided in the application.		
CAD.REQ.043	General Requirements	The system should support the use of primary incident type and a sub incident type to narrow down certain generic incidents. For example, a primary incident type could be "Robbery", sub incident type could be "Commercial", "Residential" etc.		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.044	Call Conference	officer should be able to do conference call with officers in same center or operation mirroring center or other dialled number by the officer. Caller's Call should not be disconnected during the conference call by the system		
CAD.REQ.045	Other officer Status for Call Conference or Forward Call	officer should be able to see the officer's status (like busy or Free) with officer extension and forward or transfer or conference call with the caller		
CAD.REQ.046	Transfer Call	Officer should be able to transfer the call to the dispatch officer to further assessment in emergency case		
CAD.REQ.047	Outbound Call	officer should be able to see any type of call like Missed call or Drop Call Case and can call back from the application.		
CAD.REQ.048	Outbound Call	officer should be able to dial the international number in case of international caller is in distress and contact to the proposed system.		
CAD.REQ.049	General Requirement	CAD Should have a capability to merge or split the case if the cases are of same type or different however it all depends on the situation		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.050	General Requirement	The software should have the facility to receive the information from the other government agencies like Ministry of surface and transport data, existing emergency response system.		
CAD.REQ.051	Intelligent Login facility	The software should have a feature called intelligent Log-in & Log-out facility where same user should not be able to Log-in simultaneously at different machines when operating on LAN.		
CAD.REQ.052	Standard Operating Procedures (SOP's)	The software should have capabilities to set the Standard Operating Procedures (SOP) for officers. The same needs to be invoked during Case creation by the officer. It should also be possible to remodel the Case, Case sub types, priorities and type of service required by using a remodelling tool.		
CAD.REQ.053	Location History Storage and Optimization	The software should store or update the location history of the caller in CAD database. This history should be gradually increased and optimized in the system as per requirement		
CAD.REQ.054	Physically Challenged Citizen	The CAD software should have a capability to categorise the citizen during the case analysis where the citizen is physically challenged such as Blind, Dumb, deaf and allocate the case to appropriate officer who handle these kind of citizens		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.055	Physically Challenged Citizen	The officer should be able to communicate with physically challenged citizen through SMS, Mobile chat like WhatsApp, Facebook, twitter, video relay services etc.		
Dispatch module				
CAD.REQ.056	Dispatch vehicles to incident sites	The Software should suggest the patrol units of jurisdiction and/ or closest to the location of incident. Auto dispatch shall identify the unit(s) to dispatch for better response time.		
CAD.REQ.057	Dispatching	The Case, once classified and detailed by the communication officer, shall be processed for auto dispatch		
CAD.REQ.058	Case Information	The software should display all the information entered by the communication officer (CO) for a case. It should display the location as identified by the CO on the map. The Event supervisor should also have the option of relocating the case.		
CAD.REQ.059	Dispatch Decision	The software should suggest vehicle for dispatch based on a pre-defined algorithm. The conditions could include jurisdiction, proximity, specialization, on duties resources etc.		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.060	MDT Notification	The CO/Event Supervisor should be able to send SMS Or GPRS on MDT device, send push notification into MDT CAD application. CO/Event Supervisor should be able to call the vehicle person through driver in case of emergency also		
CAD.REQ.061	Police Station Supervisor	The CO/Event Supervisor should be able to send SMS to the nearest police station supervisor and broadcast the same to multiple receivers if required.		
CAD.REQ.062	Case Status by Vehicle	The CO/Event Supervisor should be able to enter the status of the case as reported by the Responding Vehicle as an option, if the MDT cannot update the status directly.		
CAD.REQ.063	Call Taking and Dispatching	Upon discovering that a call is of an emergency nature, the officer should be able to alert the CO/Event Supervisor and other official users. They should begin dispatching as the call proceeds. Therefore, the case form should be displayed on the Dispatch console as it is being populated by the officer and updated.		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.064	Vehicle Tracking and Status update	The GIS map should display the assigned, unassigned Vehicles using appropriate and intuitive graphical symbols. The CO/Event Supervisor can command an assigned Vehicle to proceed to the case location through defined media or through dispatching the case information.		
CAD.REQ.065	Vehicle Tracking and Status update	The software should be capable of displaying the vehicles on the GIS map with colour coding according to their current status. Vehicle icon colour should change automatically with their change in status i.e., dispatch, en-route, at scene, available etc. The entire movement of a vehicle from being assigned to a case till arrival upon scene should be time stamped and monitored by the Dispatch Officer. Appropriate alerts should be generated when a PRV does not send its GPS location for a defined (changeable dynamically) time.		
CAD.REQ.066	Case Update	The software should have the capabilities to record all case related information changes or update made after the creation of case by the same or different officers, CO, Event Supervisor.		
CAD.REQ.067	Vehicle Playback	Proposed software should have the tools to provide the playback of the vehicle movement data, displayed on the integrated GIS Map.		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.068	Alarm for new case	The software shall provide an alarm or alert for every new case entered in the system		
CAD.REQ.069	GUI based Pre-Defined Route	The software should have the provision available within GUI for daily patrolling of the Police Vehicles and their patrol locations. Tools for route creation should be provided and Police vehicles assigned for regular patrolling, to those pre-defined routes as per the requirement of Police.		
CAD.REQ.070	Audio - Visual Indication	The Software should provide with an indicator to indicate that a case has exceeded the predetermined time in its current status.		
CAD.REQ.071	Case Status	There should be facility for case symbolization. To facilitate easy identification of case status (pending, open, closed), cases should be displayed on map with different colours.		
CAD.REQ.072	Geo-fencing	The proposed software should have geo-fencing capability. Software tools should facilitate in allocating areas for all patrolling Vehicles depending on Police needs. It should suggest alternate routes and nakabandi checkpoints		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.073	Shortest Path indication	There should be provision for shortest route to guide Vehicles. Auto dispatch feature can find from the GIS based map the shortest path from the dispatched vehicle to the case location and convey the shortest path direction to the dispatched vehicle. The shortest path feature allows user to identify the shortest path or route between the source and destination. The CO/Event Supervisor can direct the vehicle and assist them to reach the location using the shortest path.		
CAD.REQ.074	Display of resources & case on Map	There should be provision for display of field resources and case on map.		
CAD.REQ.075	Recording of all vehicle movements on map	There should be provision for recording of all vehicle movements on map - date wise, vehicle wise.		
CAD.REQ.076	Viewing	The software should facilitate viewing of cases and vehicle chronology. Status of all vehicles and cases on the map Police stations on the map.		
CAD.REQ.077	General Requirement	The CO or Event Supervisor should be able to dispatch the incidents to the Mobile Data Terminal fitted in the Police response Vehicles over GPRS or		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
		2G or 3G or 4G (not limited to) and SMS as per requirement		
CAD.REQ.078	Security	The system should be secure and feature an intelligent Log-in & Log-out facility. The same user should not be able to login simultaneously at different machines when operating on LAN.		
CAD.REQ.079	Interoperability	Software should be capable of swapping between Dispatch Officer-Supervisor based on the User authentication, without the need to have separate licenses in each category.		
CAD.REQ.080	Standard Operating Procedures (SOP's)	The software should have the capabilities to set the Standard Operating Procedures (SOP's) for Dispatch Officer. The same needs to be invoked during creation of case or dispatch the vehicles.		
CAD.REQ.081	case Attachments	The software should have a provision to attach any file to a case. The file could be an image, video, audio etc.		
CAD.REQ.082	case Attachments	When the case is listed in the case list, there should be an indication that a case has a file attachment. The indication can be any icon for attachment		
CAD.REQ.083	case Attachments	All case attachments should be stored in the CAD database for easier backup		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.084	General Requirements	A CO/Event Supervisor has the ability to create an incident for a vehicle per a vehicle's request based on the vehicle's observation of an activity (on view field case)		
CAD.REQ.085	General Requirements	A CO/Event Supervisor has the ability to dispatch a multiple number of vehicles on an incident or non-incident activity		
CAD.REQ.086	General Requirements	The originating CO/Event Supervisor will receive a notification when the stacked case has been worked by someone else		
CAD.REQ.087	General Requirement	A timer can be configured to notify the CO/Event Supervisor who originally stacked the call that the partial case has not been completed.		
CAD.REQ.088	Configuration & Creation of CAD Master Data base	The software or a separate interface should create or configure various master database as follows but not limited to these databases. The list may increase based on solution requirement and functional specification 1. Users & Roll creation of officers 2. Dispatch Zones or Groups & Police Stations 3. Vehicle's information 4. cases & cases Sub-type 5. Shift Master 6. Skill Master		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
		7. LOI Creation 8. Add Agencies 9. Schedule Report 10. Schedule Backup 11. Language setting and dictionary creation 12. Response Plan		
CAD.REQ.089	General Requirement	Solution should have fully integrated GIS module and be able to identify the location of the caller, vehicle location on pre-loaded map (GIS Maps) into officer desktop. It should have the capability and tools to view attribute details of any object.		
CAD.REQ.090	General Requirement	There should be provision to display map from other sources in addition to the GIS map which is used in the system.		
CAD.REQ.091	Web based GIS	GIS maps will be populated into the officer desktops for faster performance and data will be rendered on the maps from the center on real time		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.092	GIS Functionality	Software should support the following GIS Functionality - a) Event and address objects- for duplicate or repetitive calls b) GPS interface- for Patrol Vehicle tracking c) Any scale- map display d) Route module- regular & frequent monitoring of any location.		
CAD.REQ.093	GIS Interface	The user should be able to draw a fence on the map and determine points of interests that are within that fence. The POIs could be Hospitals, Health centres etc. The fence can be drawn as a polygon, rectangle, or a circle		
CAD.REQ.094	GIS Interface	The user should be able to find closest POIs (Hospitals, Police Stations etc.) from a point identified on the map OR from an event location or a MDT location.		
CAD.REQ.095	Real time location of the vehicle	The Software should enable the CO/Event Supervisor to see the real time vehicle location on the integrated GIS Map. Dispatching tools should have the facility to track the vehicle on the said map.		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.096	Ability to track vehicles in dispatch mode	Tools must be provided to facilitate the CO/Event Supervisor to be able to monitor the assigned vehicle in various modes like – Dispatch mode, End-route mode, Arrive mode and Available mode. The entire movement of a vehicle from being assigned to any incident till arrival upon scene should be time stamped and monitored by the CO/Event Supervisor. Software should have auto arrive feature and it functions when PRV reaches the event location, PRV staff shall not be provided the arrive button		
CAD.REQ.097	GIS Functionality	Software should support at least the following GIS Functionality - a) MDT interface- for Patrol Vehicle tracking b) Scale- map should be displayed as per solution requirement and can be scalable further c) Route module- regular & frequent monitoring of any particular location. b) Event and address objects - for each type of call and non-call case (in case of SMS, chat, email etc.)		
CAD.REQ.098	Shortest Path Indication	There should be provision for shortest route to guide Vehicles. CO/Event Supervisor can find from the GIS based map the shortest path from the dispatched vehicle to the event location and convey the shortest path direction to the dispatched vehicle. The shortest path feature allows user to identify the shortest path or		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
		route between the source and destination. The CO/Event Supervisor can direct the vehicle and assist them to reach the location using the shortest path.		
CAD.REQ.099	Case Location Free Draw	The software should support registering the Case locations not only in the form of point spots but also as line or polygon area. This is to handle situations wherein the affected or reported points is an area e.g., accident on a road segment or riot in an area. The CO/Event Supervisor should be able to freely draw to record such locations in the system.		
CAD.REQ.100	Hold Case	The software should support holding the Case for availability of specific vehicle or responding unit. Once the field unit is available it gets dispatched automatically to the specified Case		
CAD.REQ.101	Support for Mobile Devices	Should support a latest Android/iOS l		
CAD.REQ.102	Archive Search	The officer should be able to search the archive records in the system		
CAD.REQ.103	SMS Delivery	SMS should be delivered by the system whenever a vehicle is allocated for dispatch. The message should be delivered to the vehicle mobile phone, Supervisor,		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
		Police station officer, District HQ officer of that particular region or location of the caller, range officer etc.		
CAD.REQ.104	Notification	A Notification should be delivered by the system in the MDT CAD software whenever a vehicle is allocated for dispatch. The message should be delivered to the vehicle mobile phone, Supervisor, Police station officer, District HQ officer of that particular region or location of the caller, range officer etc.		
Supervisor Module				
CAD.REQ.105	Event monitoring	The software should facilitate supervision of Control Room operations. The Supervisor should be able to examine each event and ensure appropriate legal action is taken. The officer shall be able to call up the complainant to solicit feedback and satisfaction report. The Supervisor workstation should have the provisions for the functionalities of both communication officer and event supervisor. Supervisor should be able to issue instruction pertaining to an event while it is in progress.		
CAD.REQ.106	Dashboard	Supervisor should have a bird view dashboard to monitor the activity of the Communication officer, dispatch officers		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.107	General Requirements	Status of all Call Takers and RMO (ROIP Monitoring Officer) are updated in real time on the event supervisor's screen.		
CAD.REQ.108	General Requirements	The status of each call and the assignment of resources are updated on the view of supervisor.		
CAD.REQ.109	General Requirements	Supervisor shall have all facilities of call taker and RMO		
CAD.REQ.110	General Requirements	Supervisor should be able to issue instructions pertaining to an event or Case id while it is in progress.		
CAD.REQ.111	General Requirements	Planning & Scheduling for VIP movements: There should be provision for Planning and Scheduling of Events and Resource Movements. Events can be pre-planned in case of any future incidents. Resources can be pre-scheduled for dispatching in case of VIP movements		
CAD.REQ.112	General Requirements	Patrol Response Planning and Compliance: It should be possible for the operations commander and the web supervisors to plan the patrol response i.e., which static positions to hold, when, which areas need mobile patrolling, when.		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.113	General Requirements	The software should have the provision available within GUI for daily patrolling of the Police units and their patrol locations.		
CAD.REQ.114	Archive Search	The officer should be able to search the archive data in the system		
CAD.REQ.115	Digitization and Assignment of routes	The software should have the provision of tools for creation of digitized patrolling route (daily, weekly etc.) assign one or more Police vehicles to these pre-defined routes along with check points.		
CAD.REQ.116	Planning of Patrol, Response & compliance monitoring	It should be possible for the Supervisors to monitor the patrol response i.e., which static positions to hold, when, which areas need mobile patrolling, when. It should be possible to analyse the extent to which the prescription was followed by matching with actual AVLS information.		
CAD.REQ.117	System Settings	The Supervisor software should be able to undertake various system settings and configuration such as- Allotment of telephone extension number Screen setting (Single & Dual) Map Path Setting PRV icon display on GIS Map		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.118	Unlock of event	The Supervisor software should be able to unlock the assigned event in process and reassign to another RMO/PRV to take further action.		
CAD.REQ.119	Over the Air (OTA) Configuration	The Supervisor software GUI should have the provision to configure the GPS modems installed in the vehicles by sending the SMS commands such as vehicle location refresh rate, restart and any other commands supported by the GPS modem.		
CAD.REQ.120	Response Plan	The Supervisor software should be configure/ create the response plan based on Incident type like, Accident, Robbery, Terrorist attack etc.		
CAD.REQ.121	Patrol Planning and Compliance	a) The supervisor shall be able to assign stationary patrol locations and areas to be patrolled during a shift. It should also be possible for the supervisor to see if his instructions were complied. All this should be possible by simple operations of the mouse or a stylus. The Patrolling task should be assign using GIS map. b) Patrolling task shall be assigned to the patrol units. It should be possible to assign, report compliance and, review these Patrolling tasks. The Patrolling tasks would be surveillance of criminals, visit to senior citizens and victims, service of summons, warrants and other court processes, etc. It should be possible to add new kind of Patrolling tasks as well. There shall be		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
		several user-definable options for patrol charts like a chart for weekdays, another for Sundays and holidays, one for Fridays. c) Real time report of units deviating from the assigned chart shall be generated so that the RMO and the supervisors can take remedial action. Responding to a event does not constitute a deviation. d) In different colours/ icons it should be possible to see the prescribed patrol positions/ area patrols on map for a number of units or for one unit over a period of time.		
CAD.REQ.122	Patrol Planning Analysis on GIS Map	It should be possible to overlay patrol charts, actual positions and, crimes reported over a period of times. This is to analyse tactical the decisions. Were the patrol positions well chosen, did units adhere to it, even then which crimes occurred. It should be possible for the supervisors to watch the patrol response i.e., which static positions to hold, when, which areas need mobile patrolling, when. It should be possible to analyse the extent to which the prescription was followed by matching it with actual MDT information		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.123	Create and View BOLO database	It should be possible to Create and View the BOLO (Be on Look Out) database, such as stolen vehicle etc.		
CAD.REQ.124	Closure Case	The supervisor software should be able to close the cases		
Remote Viewer for Monitoring and Report Generation for Supervisor				
CAD.REQ.125	General Requirements	System shall send a SMS to the caller stating the event / Case Number, acknowledgment, brief text of the complaint and, the password for accessing his event /Case information on the police website		
CAD.REQ.126	General Requirements	Remote Viewer will be a web-based software monitoring tool to be used by the senior officers for monitoring of limited CAD functionalities using LAN/WAN (Intranet) or Internet		
CAD.REQ.127	Monitoring	The software should support monitoring of all events. Critical functionality which related to Police control room namely - Event Monitoring, Police Vehicles Fleet Monitoring, Reports, Charts and Analysis.		
CAD.REQ.128	GIS Map	The software should have integrated GIS map with Zoom In, Zoom Out, PAN functionalities. GIS map should display the current scale.		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.129	Event Monitoring	The software should support active event monitoring with detail information and location & Id on the map.		
CAD.REQ.130	Live Vehicle Tracking	The software should support live vehicle tracking of the response units with details. Like Vehicle Call sign, Police Station, Time Stamp, Speed and Current location.		
CAD.REQ.131	Play back history	The software should view vehicle history data of the response units with details. Like Vehicle Call sign, Police station, Time Stamp, Speed and Current location. Using various search option like Date wise, Latest No. of Records.		
CAD.REQ.132	Geo-fencing	The proposed software should have 'Geo-fencing' capability. Software tools should facilitate in allocating areas for patrolling units depending on Police needs and receive the Notification when vehicles cross the Geo-fence.		
CAD.REQ.133	Reports	The software should have in built web-based Reporting module which should be able to generate the reports as per the requirement of UP Police. The reporting module should have an ability to create various reports using various options like Date wise, Police Station, Police Zone, event Type, Sub Type etc.		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.134	Reports	The application should have a variety of reports (which includes but not limited to) following. Call Details Average Response Time Blank Calls, Crank Calls, Emergency Calls, Hot Calls, Information Calls Call per hour Police Station wise Response time Daily PCR Event Audit Logs Event Details, events Statistics Events Sub Type Fleet Summary Geo Fence IN / OUT Police Station / Police Zone wise Report Operator Status Operator activity Break code		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
		Vehicle activity, Daily activity summary, Dispatch response, stop Vehicle Status summary Vehicle Modem Maintenance Summary Vehicle Response Time Vehicle Stoppages Vehicle Daily Activity Summary Active event by event Types Zone and Police Station Wise Daily, Weekly Zone and Police Station Wise events & Vehicles Zone and Police Station wise event Count		
CAD.REQ.135	Dashboards	There shall be dashboards for different supervisory levels to give them graphical picture of the performance of those within their jurisdictions. Call Trend – day, week, and month Average Response Time for call taking, dispatching, and responding units. Event Type		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
		Police stations and Fire stations Vehicle Activity – Run Time and Halt Time event or case status (open, in progress, resolved, close etc.)		
CAD.REQ.136	Analysis	The reporting module should have an ability to create various GIS Analysis Reports. It should be possible to select the data on the basis of Police Zones, Police Stations, events, event Sub-type, Priority & date, and time. Incident Query Incident Count Repeat Incident		
CAD.REQ.137	Vehicle Dashboard	The reporting module should have inbuilt dashboard to view the performance and health check of GPS devices fitted in the patrol vehicles.		
Administrative tool for Supervisor				

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.138	Tools for Analysis	There should be software tools for response analysis, mapping, and hot spot analysis. It should be possible to select the data on the basis of jurisdictions, date and time of the day range and other data fields. It should be possible to create Thematic Maps like pin mapping, Incident count mapping and repeat Incident count Mapping. It should be possible to do detailed analysis at least the following ways – Hot Spot Analysis, Trend Analysis, Neighbourhood Analysis and Change over Time Analysis.		
CAD.REQ.139	Configuration & Creation of CAD Master Data base	The application software should offer administration tool for optimum utilization of resources, master database creation and other analytical purposes. It shall enable the Systems Administrator to define users & configure their access privileges		
CAD.REQ.140	Configuration & Creation of CAD Master Data base	The software should create / configure various master database like: Users & Roll creation of operators Dispatch Zones / Groups & Police Stations Vehicles Events & events Sub-type Shift Master		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
		Skill Master LOI Creation Add Agencies Schedule Report Schedule Backup Language setting and dictionary creation Response Plan		
CAD.REQ.141	General Requirements	CAD Mobile application is to provide the Mobile Workforce with full access to the police event data empowering them to make informed decisions while in the field. It will enable the mobile workforce to remain in communication with the command center allowing event assignment information to be delivered to the devices as required.		
CAD.REQ.142	Display Dispatch Message	The Mobile Application Software should display all the Dispatch related transactions assigned to the respective units. All the event information as dispatched by the auto dispatch system must be captured and displayed.		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.143	Update Dispatch Status	On activating an assigned event by the mobile unit staff, the mobile application software should also display the Event & Vehicle Status – i.e., dispatch, en-route, at scene, back to base and closed.		
CAD.REQ.144	Event Details	On activating an assigned event by the mobile unit staff, the mobile application software should also display event information – i.e., Event-id, Event-Type, Caller Phone Number, Caller Name, Caller Address, on browser and Event location on map window.		
CAD.REQ.145	MDT Software Interface	The system should have a provision for the MDT software to facilitate data communication link with the vehicle mounted location devices (GPS).		
CAD.REQ.146	MDT Software Interface	The MDT software should provide tools to manage all data message communication, including real-time vehicle positioning information, between the Dispatch Console and the vehicles.		
CAD.REQ.147	MDT Software Interface	The software must have facility to poll a specific GPS receiver of a vehicle to transmit its current positional information.		
CAD.REQ.148	MDT Software Interface	The software should have capability of detecting vehicles with speeding violations. In order to ensure the data security, the communication server software		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
		should be an integral part of the CAD software and not a 3rd party supply item.		
CAD.REQ.149	Remote Supervisory Interface	The CAD Software should support Remote Supervisory functions and provide CAD and GIS view. It should be possible for the Senior Officials in Districts, Police Stations belonging to jurisdictions etc. to update the status of the incident. Comprehensive Dashboard, Logs should be available for Jurisdictions and other officials.		
Message Communication Module				
CAD.REQ.150	Messaging	The CAD software should have an ability for messaging between officers (with in call center and other state call center)		
CAD.REQ.151	Messaging	The Messaging module should allow the operator to attach files to the message. These files could be any relevant information like images, videos, documents etc.		
CAD.REQ.152	Messaging	When a message with multiple attachments is opened, each attachment should open up in a tabbed interface within a message window to avoid too many windows being opened and cluttering the user's view		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.153	Messaging	The software should allow a message to be sent as a broadcast to all logged in users including, communication officer, Dispatch Officers, supervisors, and MDT users.		
Others				
CAD.REQ.154	General Requirements	The application software should be capable of integrating with Telephony system including IPPBX, ACD and CTI interface.		
CAD.REQ.155	General Requirements	System shall be capable of retaining logs for a period of 3 months		
CAD.REQ.156	General Requirements	After the Case has been logged in by the officer, the CAD shall send a SMS to the Caller stating the Case or Tracking Number along with a password as acknowledgement to the call made to the control room. The caller can use this number on department website (as and when available) to access the case progress details such as Action Taken Reports (ATR), file attachments, Remarks, or other information's as per the prevailing departmental policy for data sharing.		
CAD.REQ.157	Other agencies or even senior officers can	The software should have the provision to inform pre-defined case data to senior officers or other agencies		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
	be informed with pre-filled data about case via SMS			
CAD.REQ.158	Accuracy	Event Supervisor will be able to rate the accuracy of incident by CAD		
CAD.REQ.159	Acknowledgement of vehicle	CAD should have a facility which will tell the officer about the vehicle that it has been reached to distress caller location or not		
CAD.REQ.160	General Requirements	The software should be able to schedule & automatically generate reports. Web based Report module should have the ability to produce reports with appropriate charts and graphs		
CAD.REQ.161	General Requirements	The report generation tool should have the facility to provide the report in both printed and electronic format.		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.162	General Requirements	The application should have a variety of reports like: 1. Call Details 2. Event Details 3. Fleet Summary 4. Operator activity 5. Vehicle activity, Daily activity summary, dispatch response 7. Active Event by Event Types 8. Efficiency of call takers speed of response, longest idle time, etc. 9. Facility to generate the various graphical reports.		
CAD.REQ.163	General Requirements	System shall record radio communications; should have provision for integrating with radio system.		
CAD.REQ.164	General Requirements	System will facilitate for Fire services which will include dispatch of incidents related to Fire over MDTs of Fire Brigades and Fire stations. System will facilitate to find out location of MDTs over GIS and dispatch case to the nearest vehicle along with concerned fire station and District Control room		
CAD.REQ.165	General Requirements	Multiple pages of the application can be opened by CO simultaneously for comparing previous events		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.166	General Requirements	There should not be any non-allotted event in the system if any not allotted event is present it should be highlighted to officers		
CAD.REQ.167	General Requirements	UI interfaces need to get approved from NexGen UP112		
CAD.REQ.168	General Requirements	Application shall be easily scalable and need to be updated on regular time interval		
CAD.REQ.169	General Requirements	Police stations officers have to be provided with facility of downloading reports from CAD on basis of events occurring in their jurisdiction. So that station officers can view and update details about events and fill FIR details as per events captured in CAD system in their respective Thana jurisdiction		
CAD.REQ.170	General Requirements	There should be separate tab option available for hyper high priority events such as suicide/murder/ heinous crime/ ongoing crime where CO-RMO-PRV-CALLER all can connect just by one click at the same and help can be provided ASAP.		
CAD.REQ.171	General Requirements	There should be an edit option on application to add attachments post event creation. Addition of information should be possible, though post event submission deletions of any info shouldn't be possible even for COs.		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.172	General Requirements	For dissatisfied callers- system centric alert to be generated. For any repeated non-satisfied caller. Separate pop should come up to CO and Event Supervisor		
CAD.REQ.173	General Requirements	In case event is not closed for a caller and he calls again all details of 1st event should pop for CO for the caller (user from same number calling and his event isn't closed yet)		
CAD.REQ.174	General Requirements	For dispatch module of CAD shall provide pop-ups/ auto alerts for all the devices that are not operations or turned off such as integrated external GPS device, MDTs, or Mobile Sets		
CAD.REQ.175	General Requirements	System shall generate a complete report of non-available devices (external GPS, MDT, and mobile phone) at respective PRVs at various time slots.		
CAD.REQ.176	General Requirements	Fields such as Gender, Age Range to be available for COs. These fields shall be filled by a CO post and event is submitted to auto dispatch system.		
CAD.REQ.177	General Requirement	CAD application shall be integrated with EMS system for getting the relevant information that can be used for SLA calculation		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.178	General Requirement	CAD shall have feature that, in case if a Citizen calls and it got disconnected the details filled by CO shall be available to next COs for at least one day if the Citizen call again with same number.		
CAD.REQ.179	PRV category Identification	CAD shall have feature to assign the PRV based on category like Pink PRV, Highway PRV etc. and it shall also have feature of dispatching the PRV's based on the category		
CAD.REQ.180	Digitization of Manual Event	CAD system shall have feature to digitise the manual event created at the time of emergency situation or CAD failure. The manual event digitised should become part of CAD system for future use		
CAD.REQ.181	General requirement	ATR filling by PRV staff can be done by converting PRV staff voice into text Similarly, COs at social media desk shall be able to create an event using voice to text		
CAD.REQ.182	General requirement	System should have configurable built-in dashboard to display dispatch summary		
CAD.REQ.183	General requirement	Dashboards should be available both as web client and as standalone system		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.184	General requirement	Dashboards should display real time dispatch data.		
CAD.REQ.185	General requirement	Dashboards should also be displayed on GIS maps with interactive menu and customizable content.		
CAD.REQ.186	General requirement	System should continue limited operation when network connection to database is lost and recovery when connection is regained.		
CAD.REQ.187	General requirement	Dashboard should show overall status of the units and events in a district		
CAD.REQ.188	General requirement	Dashboard should show tiles - Map View, Interactive menus and customizable content within "cards"		
CAD.REQ.189	General requirement	System should provide web-based incident and event analysis		
CAD.REQ.190	Dashboards and Analytics	System should provide dashboard solution that delivers concise, dynamic summaries of contact center operations to desktops, wallboards and are available on move in tabs and mobile devices.		
CAD.REQ.191	Dashboards and Analytics	System should provide timely information through single point of reference to control room supervisors, managers and staff and make them continuously stay aware of operations and emerging trends that will enable them to take necessary action to ensure performance and effective use of resources.		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
CAD.REQ.192	Dashboards and Analytics	System should provide dynamic rolling summaries of short-term data histories illustrate variations and trends in key indicators, such as incident load and unit availability over user-configurable time periods (up to 24 hours)		
CAD.REQ.193	Dashboards and Analytics	System should provide pre-configured gadgets that allow administrators to quickly combine these into highly effective layouts that deliver users concise summaries of the information they need, including the distribution of events and resources, both spatially and temporally.		
CAD.REQ.194	Dashboards and Analytics	System should have following key capabilities: -- • Density Heat Maps – highlight the relative concentration and distribution of units / resources and incidents. • Thematic Maps – give a visual indication of the relative number of incidents or units within each functional boundary (e.g., beat, precinct, and district). • Pin Maps – show the distribution of individual units / resources and events, which can be placed on top of heatmaps and thematic maps to provide additional operational context (e.g., comparing concentrations of events with the current locations of units). • Presentation & Navigation – the map gadgets are interactive, allowing users to pan and zoom		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
		to see areas of interest in greater detail, choose overlays used for the contextual base maps, and configure the symbology used in thematic maps. • Live Data – charts provide summaries of live data to illustrate the relative proportion of counts for each category (e.g., the number of units by unit status, or the number of events categorized by priority). The display uses color-coded proportional bars and counts for each category. • Emerging Trends – a rolling visual track of variations in indices over user-specified time periods (up to 24 hours). They can track a single indicator or compare multiple indices such as the number of pending events against available units.		
CAD.REQ.195	Dashboards and Analytics	System administrators can add and configure one or more cards to track key indicators, such as the number of events of a specific nature, and simple operators, such as the ratio of available units to pending events.		
CAD.REQ.196	Dashboards and Analytics	System administrators can add tabs that show different views of data (e.g., by filtering units by whole state and/or districts). They can also define data filters to restrict the scope of data available to specific user profiles.		
CAD.REQ.197	Dashboards and Analytics	System should allow users outside the control room to view live operations, search live and historic information,		

Computer Aided Dispatch (CAD)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
		and create non-emergency events.		
CAD.REQ.198	Dashboards and Analytics	System should provide immediate access to up-to-the minute situational information for analysis and sharing.		

2. Mobile CAD application

Mobile CAD Application				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
MCAD.REQ.001A	General Requirement	The mobile CAD application installed in the MDT and Mobile devices issued to the PRVs and other allied agencies like FIRE, GRP for sharing event related information		
MCAD.REQ.002A	General Requirement	Mobile CAD Application shall receive the notification of the case detail which is sent by dispatch		
MCAD.REQ.003A	General Requirement	The application shares the current location of the vehicle to DC through a Web API configured in concerned mobile devices		
MCAD.REQ.001	General Requirement	MDT software is to provide the Mobile Workforce with full access to the assigned case with distress GIS Map location to empower them to make informed decisions while in the field.		
MCAD.REQ.002	General Requirement	The system will have feature of single sign on to authorize the user and this feature will be integrated with attendance module linked HRMS		

Mobile CAD Application				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
MCAD.REQ.003	General Requirement	MDT software will enable the mobile workforce to be in contact with Officer over the call, SMS, CAD Application notification etc.		
MCAD.REQ.004	General Requirement	The Event Supervisor shall send cases data to the PRV on its MDT and the PRV staff shall initiate the response by accepting the Case on the MDT. The software shall be capable of delivering the acknowledgment to the CAD software for receipt of case information on the MDT device		
MCAD.REQ.005	General Requirement	The Software should display all the Dispatch related transactions assigned to the respective PRVs.		
MCAD.REQ.006	Display Dispatch Message	On activating an assigned Case by the PRV staff, the Software should also display Case information – i.e. Case id, Case type, user Phone Number, username, user Address, into the Software and user location on map. The map should be provided by GIS Map service provider		
MCAD.REQ.007	Case Details	On activating an assigned case or incident by the mobile PRV staff, Software should also display the user or caller detail, location & PRV Status like dispatch, end-route, at scene, back to base and closed		

Mobile CAD Application				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
MCAD.REQ.008	Update Dispatch Status	It should also enable the MDT users to report case closure.		
MCAD.REQ.009	Communication	The MDT users should have the ability to provide information to the call center Officer or event Supervisor through SMS messages and case closing reports		
MCAD.REQ.010	Updated GIS MAP	MDT GIS map should be for defined local area (such as Police stations etc). And that updated data from central server can be refreshed into it remotely.		
MCAD.REQ.011	User Location	The Software should have the capability to display real-time location of the User on the map and tracking of the user on map		
MCAD.REQ.012	General Requirement	This application should be integrated with EMS application to create a ticket for IT help desk for any kind of issue into the center IT operation and can track the status as well.		
MCAD.REQ.013	Vehicle Location (AVLS Software Interface)	The software should be capable to send the location of the vehicle in real time to the data center.		
MCAD.REQ.014	Action Taken Report	It should also enable the MDT users to report Action Taken by attaching Audio Files, Image Files, Video Files		

Mobile CAD Application				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		and Text Entry. All Action Taken data should be available to Event Supervisor through logs. Drop down menu and free text shall be available for filling the ATR report. There shall be speech to text functionality for making an entry in ATR.		
MCAD.REQ.015	Communication	The Software should support GPRS Message or SMS Capabilities between the dispatch consoles and vehicle.		
MCAD.REQ.016	MDT User Status	The Software should have functionality to update the Status like Available, Away, Attending to cases, On Break, etc. of the police personnel.		
MCAD.REQ.017	Offline Support	MDT user should be able to update the transaction as required in the application even in case of poor or no network connectivity. All the transaction should be stored in the MDT devices and can be sync once the devices is connected		
MCAD.REQ.018	Software Update and GIS Map Update	The software should be capable to update or upgrade the version of the software including GIS maps installed in the MDT remotely		

Mobile CAD Application				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
MCAD.REQ.019	General Requirement	The application should be integrated with BI and Analytics application to receive and send the data on regular interval of time into the system.		
MCAD.REQ.020	General Requirement	Require automatic refresh and data push from MDM to keep application and hardware live		
MCAD.REQ.021	General Requirement	There should be a functionality of sending Hindi Messages from CAD to MDT/Mobile and MDT/Mobile to MDT/Mobile		
MCAD.REQ.022	General Requirement	The Software should support GPRS Message or SMS Capabilities between the dispatch consoles and PRV vehicle.		
MCAD.REQ.023	General Requirement	MDT user should be able to update the transaction as required in the application even in case of poor or no network connectivity. All the transaction should be stored in the MDT devices and can be sync once the devices is connected.		
MCAD.REQ.024	General Requirement	Mobile application for MDT/Mobile of Fire services shall have additional features such as contact facility to UP112, District control room and concerned fire stations. Application shall also have list of fire causes like chemical, jungle fire, cylinder blast fire and call closure mechanism.		

Mobile CAD Application				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
MCAD.REQ.025	General Requirement	GIS related application with MDT/Mobile CAD: Field officers would be able to access the location of the caller, nearby vehicles, nearby police station etc. on the MDT GIS MDT GIS would also help in finding shortest route to the incident site MDT GIS Data capture shall be used to collect the field location provincial data and sync with central GIS server If network is not available in MDT, it should be saving the latitude and longitude coordinates and once network is again available MDT shall be able to push stored coordinates to DC		
MCAD.REQ.026	General Requirement	This application login shall have user authentication.		
MCAD.REQ.027	Forgot Password	The application should have a functionality like forgot password etc. in case user lost its password. An auto email should be generated to the user with temp password and user can rest the password after entering the temp password into the application		
MCAD.REQ.028	Event monitoring	The application should facilitate supervision of Center operations. The Senior officer should be able to examine each case in the system for necessary action		

Mobile CAD Application				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
MCAD.REQ.029	Notification	The officer should be able to receive a notification into the application if the case is assigned to vehicle which is associated to its police station vehicle and user can track the status of the case. If no vehicle is available is available in officer area, then notification should be generated into the Application		
MCAD.REQ.030	Case Update	Police station officer should be able to update the case into the system which is assigned to its police station vehicle.		
MCAD.REQ.031	Application Setting	The Supervisor software should be able to undertake various system settings and configuration such as given below. These features are for sample purpose. It may increase on later stages -Allotment of Telephone extension number -Screen setting (Single & Dual) - Register MDT devices - Register MDT SIM card		
MCAD.REQ.032	Event Creation by ROIP	This application shall have feature of creating event with ROIP		

Mobile CAD Application				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
MCAD.REQ.033	OS Support	Mobile application should be available on latest versions of Android OS platform and be upgradable or portable with latest updates in the application		

3. Police Station Module

Police station Module				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
PSM.REQ.001 A	Overview of Solution	Police station module will be integrated part of CAD		
PSM.REQ.002 A	Overview of Solution	Police station module shall assist police station level to the action taken by them on the particular events/cases being transferred to them by PRVs		
PSM.REQ.003 A	Overview of Solution	This module shall be available on Intranet UP112 and whitelisting of the Mac address of this application shall be open to the available network at police station level		
PSM.REQ.001	General Requirement	Police station staff shall be able to comment about GD/FIR/NC/ any other comments for the events		

Police station Module				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		closed and transferred by PRVs to respective police station		
PSM.REQ.002	General Requirement	Event Supervisor at HQ will check the closure report from the field team and close the case if satisfied with the field team's response. At the end of the operation, PRV staff shall hand over the case to local Police that does require local Police intervention. The local Police will download details of the action taken report from a web link and initiate the case file and update status in the UP112 system		
PSM.REQ.003	General Requirement	Police stations staff shall have facility to mention and add extra details in an event such corresponding chauki/ halka, corresponding beat number, corresponding village/ ward/ mohallah along with feasibility to provide any other details or remarks.		
PSM.REQ.004	General requirement	Police station module of UP112 shall be available to CCTNS team of technical services and any other police unit on need and request basis.		

Police station Module				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		User based login credential shall be provided to authorised person to access the details of Police station Module.		

4. Emergency Monitoring System

Emergency Monitoring System				
Sr.No	Functional/Technical Parameters	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMOS.REQ.001	General requirements	The Command & Control solution should be implemented and Compliance to the industry open standards based Commercial-of the-shelf (COTS) products.		
EMOS.REQ.002	General requirements	System must provide a comprehensive API (Application Program Interface) or SDK (Software Development's Kit) to allow interfacing and integration with existing systems and future application and sensors which shall be deployed on the field.		

Emergency Monitoring System				
Sr.No	Functional/Technical Parameters	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMOS.REQ.003	General requirements	The platform should be able to normalize the data coming from different subsystems and provide secure access to that data using data API(s) to application developers		
EMOS.REQ.004	General requirements	The solution should use the latest application architecture models of Service-oriented Architecture for better interoperability and performance		
EMOS.REQ.005	General requirements	The platform must be able to normalize the data from various data sources		
EMOS.REQ.006	General requirements	The platform must be able to integrate data from different sub- systems and provide a unified view of the sub-system data over visualization dashboards		
EMOS.REQ.007	General requirements	The platform must have the capability to perform actuations of the resources through the APIs provided by the sub-systems		
EMOS.REQ.008	General requirements	The platform must be compatible to work on web browsers/client's software.		
EMOS.REQ.009	General requirements	The platform must have the ability to ingest data into time-series or document-oriented charts		

Emergency Monitoring System				
Sr.No	Functional/Technical Parameters	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMOS.REQ.010	General requirements	Platform and CAD System should be from different OEM as data can be analysed transparently to support interoperability		
EMOS.REQ.011	General requirements	Platform Will work as a Top Layer on CAD System to provide the data interface layer to external agencies.		
EMOS.REQ.012	General requirements	Platform should be capable to integrate the existing systems like GIS and CAD System etc.		
EMOS.REQ.013	General requirements	CAD system to share all the relevant API along with Database details to integrate both systems seamlessly		
EMOS.REQ.014	General requirements	All external integrations like pushing or extracting data from various agencies should be in scope of this platform. MSI has to consider minimum 20 such integrations.		
EMOS.REQ.015	Role based Access Control (RBAC)	Platform must have the ability to assign appropriate features access levels to the roles that are derived from the default roles		
EMOS.REQ.016	Role based Access Control (RBAC)	Platform must have the ability to assign appropriate domains access to the roles that are derived from the default roles		

Emergency Monitoring System				
Sr.No	Functional/Technical Parameters	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMOS.REQ.017	Role based Access Control (RBAC)	Platform must have the ability to assign appropriate region access to the roles that are derived from the default roles		
EMOS.REQ.018	Role based Access Control (RBAC)	Platform must have the ability to assign appropriate roles to the Users, and the users created would be able to see the data and access the features basis the role that has been assigned		
EMOS.REQ.019	Custom Query Builder	Platform should provide user to search the system data based on the query designed by operator dynamically		
EMOS.REQ.020	Custom Query Builder	User should be able to save these query templates for future use		
EMOS.REQ.021	Custom Query Builder	Search data can be taken as Print report in form of Excel/CSV or PDF		
EMOS.REQ.022	Custom Query Builder	Searched Data can be shown as Tabular format as well as		
EMOS.REQ.023	Mass Notification System	Provide a single web-based dashboard to send notifications to target audiences using multiple communication methods including SMS, E-mail.		
EMOS.REQ.024	Performance Analysis	Platform should provide the Insight of data available at data center		

Emergency Monitoring System				
Sr.No	Functional/Technical Parameters	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMOS.REQ.025	Performance Analysis	platform should be able to generate the real time performance monitoring for all the resources like Call taker , dispatch officers , supervisors and PRVs.		
EMOS.REQ.026	Performance Analysis	Easy to access the resources performance data for specified Time selection like for Today,week,month and year.		
EMOS.REQ.027	Performance Analysis	Platform should be able to generate real time dashboard for district wise performance		
EMOS.REQ.028	Performance Analysis	Platform should be able to generate the dashboard for maximum events handled by a District , Police Station and PRVs associated.		
EMOS.REQ.029	Performance Analysis	All data should be drilled down to last level to get the desired result		
EMOS.REQ.030	Performance Analysis	Platform should display the real time average response of resources for Today , week, month and year.		
EMOS.REQ.031	Post Event Analysis	Solution should be displaying all events related details by just entering the events ID		
EMOS.REQ.032	Post Event Analysis	Post events analysis should have complete information of Similar events generated within predefined time		

Emergency Monitoring System				
Sr.No	Functional/Technical Parameters	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMOS.REQ.033	Post Event Analysis	Administrator should have the ability to change the predefined time period for displaying the similar events		
EMOS.REQ.034	Post Event Analysis	Complete history of alert action should be visible under post events analysis		
EMOS.REQ.035	Post Event Analysis	System should rate the alert execution based on certain parameter such as, closing time, priority, Action perform etc		
EMOS.REQ.036	Post Event Analysis	Supervisors remotely can access the system and monitor the events received, action taken status, response etc.		
EMOS.REQ.037	Post Event Analysis	Supervisor should be able to add remarks against events		
EMOS.REQ.038	Post Event Analysis	Supervisor should be able to start rate an event after analysing the complete details on single page.		
EMOS.REQ.039	Predictive and Business Analytics	Platform should be capable of generating various dashboard in form of charts,cards,tabular etc.		
EMOS.REQ.040	Predictive and Business Analytics	Platform should be capable enough to showcase GIS analytics like Heat map, clustering of events and extract the relevant data from custom drawn shapes from Map		

Emergency Monitoring System				
Sr.No	Functional/Technical Parameters	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMOS.REQ.041	Predictive and Business Analytics	Platform should create prediction models based on the data available in CAD in past years.		
EMOS.REQ.042	Predictive and Business Analytics	Platform should predict the Event count, PRV performance, District Performance and other parameters suggested by stakeholders.		
EMOS.REQ.043	Predictive and Business Analytics	Prediction model accuracy should be increased as per the timelines of data model maturity increases.		
EMOS.REQ.044	Predictive and Business Analytics	Platform should be able to predict the performance/response time of available resources like Call takers , dispatchers supervisors and PRVs.		
EMOS.REQ.045	Social Media Analysis	Social Media Analysis should be integral part of analytics platform		
EMOS.REQ.046	Social Media Analysis	No separate license should be required for this		
EMOS.REQ.047	Social Media Analysis	It should integrate with open-source APIs to monitor insights of the social media platform.		
EMOS.REQ.048	Social Media Analysis	It should integrate with Facebook,Twitter,Instagram and multiple RSS feeds		

Emergency Monitoring System				
Sr.No	Functional/Technical Parameters	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMOS.REQ.049	Social Media Analysis	Tool Should Provide insights of these platform like Total Followers New Followers New Accounts You Follow Male % Female % Primary Age Group Primary Location		
EMOS.REQ.050	Social Media Analysis	# of Positive Sentiments # of Negative Sentiments # of Neutral Sentiments, Total Engagements # of Individual Engagements by Type (retweets, likes, comments, link clicks, shares, etc.) Engagement Rate % Increase/Decrease Mentions Received, Total Page Views, Influencer analysis, Keyword search, most trending topics, latest trends		
EMOS.REQ.051	Multi Agency Interface	Platform should be capable of integrating multiple agencies to provide or get the data into 112 System and		

Emergency Monitoring System				
Sr.No	Functional/Technical Parameters	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		same should be provided to CAD System as and when required.		
EMOS.REQ.052	Multi Agency Interface	Platform should present some selected high priority events based on keyword, district or any other parameters.		
EMOS.REQ.053	Multi Agency Interface	Platform User should be able to sort the received data base on time , source and priority of information.		
EMOS.REQ.054	Multi Agency Interface	Platform Should provide the maker and checker functionality for received Data from different sub systems like different helplines , smart cities and different sources		
EMOS.REQ.055	Multi Agency Interface	Operator should be able to visualize the received data and can take action like create an event in CAD or reject the event creation with proper remarks		
EMOS.REQ.056	Multi Agency Interface	Platform should record the time for each action perform on received data so that chronology can be generated at later stage.		
EMOS.REQ.057	Multi Agency Interface	System should allow the configuration sub system wise for automated alert creation like some system can be exempted from the validation process		

Emergency Monitoring System				
Sr.No	Functional/Technical Parameters	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		so that emergency can be responded quickly		

C. Supervisory and Monitoring

1. Enterprise Management System (EMS)

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.001	General	For effective operations and management of IT Operations, there is a need for an industry-standard Enterprise Management System (EMS). Given the expanse and scope of the project, EMS becomes very critical for IT Operations and SLA Measurement. Some of the critical aspects that need to be considered for operations of IT setup of are: a) Network Fault Management b) Network Performance Management c) Network Configuration Management d) Server Performance Monitoring e) Network Traffic Analysis f) Centralized Log management g) Centralized and unified Dashboard h) Centralized and customizable service level reporting i) Helpdesk for Incident management j) Asset Management		
EMS.REQ.002	General	The Monitoring Solution should provide Unified Architectural design offering seamless common functions including but not limited to: Event and Alarm management, Auto-discovery of the Network environment, Correlation and root cause analysis, Reporting and analytics		
EMS.REQ.003	General	The OEM of the proposed solution shall be from leading OEM		
EMS.REQ.004	General	There should be a tight integration between infrastructure metrics and logs to have the single consolidated console of Infrastructure & security events.		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.005	General	Consolidate IT event management activities into a single operations bridge that allows operator quickly identify the cause of the IT incident, reduces duplication of effort and decreases the time it takes to rectify IT issues.		
EMS.REQ.006	General	The Operator should be able to pull up security events related to a given Configuration Item, from a single console which also has NOC events, and use the security events to triage the problem. This way the Operator gets consolidated system/network event details and security events (current and historical) from the same console and save time in troubleshooting / isolating the issue.		
EMS.REQ.007	General	The solution should have capability to perform cross domain correlation with alarm correlation built-in algorithms from Network, Systems and other domain events as well as KPI patterns, also correlation should not be limited to only parent-child or service mapping relationships		
EMS.REQ.008	General	The operator should be able to build correlation rules in a simple GUI based environment where the Operator should be able to correlate cross domain events		
EMS.REQ.009	General	Scalability – The system should be capable of supporting at least 15 thousand network flow per second on single server with capability to capture each unique traffic conversations		
EMS.REQ.010	General	The solution shall provide future scalability of the whole system without major architectural changes.		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.011	General	The Solution shall be distributed, scalable, and multi-platform and open to third party integration such as Cloud, Virtualization, Database, Web Server, Application Server platforms etc.		
EMS.REQ.012	General	The monitoring module of proposed solution must not use any third-party database (including RDBMS and open source) to store data in order to provide full flexibility and control on collected data.		
EMS.REQ.013	General	All the EMS modules should be from same OEM and should be tightly integrated for single pane of glass view of enterprise monitoring		
DETAILED SPECIFICATIONS: EMS				
Consolidated Dashboard				
EMS.REQ.014	Consolidated Dashboard	The platform must provide complete cross-domain visibility of IT infrastructure issues		
EMS.REQ.015	Consolidated Dashboard	The platform must consolidate monitoring events from across layers such as Network, Server, Application, Database etc		
EMS.REQ.016	Consolidated Dashboard	The solution should support single console for automated discovery of enterprise network components e.g. network device, servers, virtualization, cloud, application and databases		
EMS.REQ.017	Consolidated Dashboard	The solution must support custom dashboards for different role users such as Management, admin and report users		
EMS.REQ.018	Consolidated Dashboard	The solution must allow creating custom data widget to visualize data with user preferences e.g. Refresh time, time span, background colour, unit conversion		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.019	Consolidated Dashboard	The solution must support custom query-based widget with multiple visualization methods including Chart, Gauge, Grid, Top N list etc. to visualize and represent collected data with ease.		
EMS.REQ.020	Consolidated Dashboard	The solution must provide comprehensive query language to pull and plot complex visualization with multiple arithmetic operator such as top, sum, min, max etc.		
EMS.REQ.021	Consolidated Dashboard	The solution must support out of the box data widgets for Metric, Log and network flow data with multiple visualization methods such as gauge, grid, charts, Top N etc.		
EMS.REQ.022	Consolidated Dashboard	The solution should provide superior view of infrastructure health across system, networks, application and other IT Infrastructure components into a consolidated, central console		
EMS.REQ.023	Consolidated Dashboard	There should be only one dashboard/interface to collected network/server/application/log data after correlation and consolidation across the IT landscape to reduce/correlate number of metrics/alarms		
Network Performance Management				
EMS.REQ.024	Network Performance Management	The solution must provide discovery & inventory of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level.		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.025	Network Performance Management	The solution must support custom device template to support Generic SNMP devices as well as extensive support on traffic encryption including SNMP v3 with AES-256 encryption		
EMS.REQ.026	Network Performance Management	The NMS should provide very powerful event correlation platform/engine and thus must filter, correlate & process, the events that are created daily from network devices. It should assist in root cause determination and help prevent flooding of non-relevant console messages.		
EMS.REQ.027	Network Performance Management	It shall provide Real time network monitoring and Measurement offend-to-end Network performance & availability to define service levels and further improve upon them.		
EMS.REQ.028	Network Performance Management	The Network performance operator console should provide operators with seamless transitions from fault data to performance data. For example - select a NMS fault event and fault drill down must also provide historical, near real time and correlated data without switching the page		
EMS.REQ.029	Network Performance Management	The solution should have the ability to do "baseline" performance metrics and determine normal operating values and patterns by self-learning algorithms on a day, week, month, etc. and ability to configure threshold on these values. The solution should also have built in algorithms to start the monitoring with zero threshold configurations		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.030	Network Performance Management	The proposed system should be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user choose algorithms that is more relevant to specific KPI in case of false positive		
EMS.REQ.031	Network Performance Management	The agents should be extensible and customizable allowing incorporation of any required monitoring source not included in the out-of-the-box monitoring policies. With capabilities to collect and analyse performance data from the operating system and installed applications and use historical patterns to establish performance baselines.		
EMS.REQ.032	Network Performance Management	All baseline thresholds should have lower bound, higher bound, polarity, deviation set point and reset point for ease of use.		
EMS.REQ.033	Network Performance Management	System should have anomalies detection, outlier detection and stop alarm flooding with these dynamic thresholds.		
EMS.REQ.034	Network Performance Management	The solution should be capable of performing prediction- based anomaly detection to identify unusual or unexpected events and measurements within the monitored environment.		
EMS.REQ.035	Network Performance Management	The Solution should provide AI and ML capabilities to help in preventing of Network problems before they occur The Solution should include unsupervised learning module to gather real time network data and which learns the behaviour of devices, applications, and users on the network It should be capable to bring together and correlate network and application data to predict anomaly and performance issues		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.036	Network Performance Management	The solution must provide agentless and agent-based method for managing the nodes and have the capability of storing events / data locally if communication to the management server is not possible due to some problem. This capability will help to avoid losing critical events.		
EMS.REQ.037	Network Performance Management	The NMS admin console must provide the ability to start, stop and restart the agent on target server infrastructure and the agent should provide collection capabilities not limited to just KPIs but also support collecting raw logs as well as packets.		
EMS.REQ.038	Network Performance Management	The proposed solution must provide agentless as well as agent-based monitoring for server infrastructure. The agents should be to set polling interval as low as 1 second with low overhead on target server infrastructure		
EMS.REQ.039	Network Performance Management	The proposed solution should include a distributed search engine data-store to ingest various types of textual, numerical, geospatial, structured and unstructured data.		
EMS.REQ.040	Network Performance Management	The NMS admin console must provide operators with seamless automation to extract fields from collected logs via drag and drop functionality to avoid log parsing complexity of collected logs from various syslog/ windows/ application sources.		
EMS.REQ.041	Network Performance Management	It shall provide Real time network monitoring and Measurement offend-to-end Network performance & availability to define service levels and further improve upon them.		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.042	Network Performance Management	The EMS solution shall keep historical rate and protocol data for a minimum of 30 days (most recent) in its short-term operating database. All data in that database shall have a maximum 1- minute window granularity. User shall be able to select any 1-minute window over the last 30 days and display unique utilization and protocol data for every monitored interface		
EMS.REQ.043	Network Performance Management	The proposed solution should be able to take back up of running and start-up configuration of network devices. It should also provide versioning for backup to track changes.		
Fault Management				
EMS.REQ.044	Fault Management	The proposed solution must should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.		
EMS.REQ.045	Fault Management	The Platform must include an event correlation automatically fed with events originating from managed elements, monitoring tools or data sources external to the platform. This correlation must perform event filtering, event suppression, event aggregation and event annotation		
EMS.REQ.046	Fault Management	The proposed solution should provide alert console with alert summary such as no. of correlated alert, network alert, server alert, virtualization alert, cloud alert, application alert etc.		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.047	Fault Management	The system must have provision to overlay alert on reported metric to understand alert triggering behaviour across multiple drill down pages		
EMS.REQ.048	Fault Management	The proposed solution should have drill-down and correlation page to correlate cross domain historical data points and result should be exported as image and tabular format.		
EMS.REQ.049	Fault Management	The proposed solution should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.		
EMS.REQ.050	Fault Management	Powerful correlation capabilities to reduce number of actionable events. Topology based and event stream-based correlation should be made available.		
EMS.REQ.051	Fault Management	The solution must offer relevant remedy tools, graphs in context of a selected fault alarm/event		
EMS.REQ.052	Fault Management	The proposed monitoring solution should have capability to configure actions-based rules for set of pre-defined alarms/alerts enabling automation of set tasks.		
EMS.REQ.053	Fault Management	The Platform must support Event or Alarm Correlation integrations with service desk to trigger automated creation of incidents, problems management		
EMS.REQ.054	Fault Management	The solution should classify events based on business impact and also allow defining custom severity levels and priority metrics such as Ok, Critical, Major, Down, Info etc with colour codes		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.055	Fault Management	The solution should allow creation of correlation or analytics rules for administrators		
EMS.REQ.056	Fault Management	The proposed solution must provide default event dashboard to identify, accept and assign generated alarms		
Log Management				
EMS.REQ.057	Log Management	The proposed solution must provide a common classification of event irrespective of the log format		
EMS.REQ.058	Log Management	The proposed solution must provide the ability to store/ retain both normalized and the original raw format of the event log as for forensic purposes for the period of 3 months and allow to extend it to further with additional hardware without any disruption to the ongoing data collection		
EMS.REQ.059	Log Management	The proposed solution should provide a minimum log compression of 8:1 for ensuring log compression to reduce overall log index storage space for the raw log format		
EMS.REQ.060	Log Management	The log data generated should be stored in a centralized server. The period up to which the data must be available should be customizable.		
EMS.REQ.061	Log Management	The proposed solution must support logs collected from commercial and proprietary applications. For assets not natively supported, the solution should provide the collection of events through customization of connectors or similar integration		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.062	Log Management	The proposed solution must support log collection for Directories (i.e., AD, LDAP), hosted applications such as database, web server, file integrity logs etc. using agents		
EMS.REQ.063	Log Management	The Log receiver or log collection component must store the data locally if communication with centralized collector/receiver is unavailable.		
EMS.REQ.064	Log Management	The proposed solution must support log collection from Network infrastructure (i.e. switches, routers, etc.). Please describe the level of support for this type of product.		
EMS.REQ.065	Log Management	The system shall support the following log formats for log collection: Windows Event Log, Syslog, Access Log Data, Application Log data, Any Custom Log data, Text Log (flat file), JSON Data		
EMS.REQ.066	Log Management	The collection devices should support collection of logs through Syslog, syslog NG and also provide native Windows Agents as well as Agentless (PowerShell) connectors		
EMS.REQ.067	Log Management	The proposed solution must provide alerting based upon established policy		
EMS.REQ.068	Log Management	The proposed solution must provide SDK and Rest API to write custom connectors and collectors to pull log and monitoring data from third party system		
EMS.REQ.069	Log Management	The proposed solution must provide UI based wizard and capabilities to minimize false positives and deliver accurate results.		
EMS.REQ.070	Log Management	The proposed solution must collect, index the log messages and support full text searching for forensic investigation		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.071	Log Management	The proposed solution must support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an email message.		
EMS.REQ.072	Log Management	The solution must provide pre-defined log correlation rules to detect suspicious behaviour		
EMS.REQ.073	Log Management	The solution must support real-time and scheduled alerting timeline while creating a log policy to catch specific log pattern		
EMS.REQ.074	Log Management	The solution should support applying regex pattern in real-time to extract vendor specific log data for reporting and alerting purpose		
EMS.REQ.075	Log Management	The system shall have the capability to drag and drop building of custom search queries & reports		
EMS.REQ.076	Log Management	The system shall be capable of operating at a sustained 5000 EPS per collection instance. The system shall provide the ability to scale to higher event rates by adding multiple collection instance		
Network Flow-based Traffic Analysis				
EMS.REQ.077	Network Flow-based Traffic Analysis	The proposed traffic monitoring system must be able to track all network flow (including netflow v1-v9, Jflow, Sflow and IPFix) of traffic on the network and identify malicious behaviour with all IP conversations.		
EMS.REQ.078	Network Flow-based Traffic Analysis	The proposed system must provide details of applications, hosts, and conversations consuming WAN bandwidth to isolate and resolve problems.		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.079	Network Flow-based Traffic Analysis	The proposed system must provide baseline network flow policy to detect anomaly in traffic usage behaviour		
EMS.REQ.080	Network Flow-based Traffic Analysis	The solution must provide flow data explorer with capability to analyse extracted data using multiple columns, chart type, group by operators and filters. System must also provide dashboard to flow data explorer drill down capability.		
EMS.REQ.081	Network Flow-based Traffic Analysis	The proposed solution must be able to monitor and report on a variety of unique protocols (used in the overall deployed solutions) per day and display utilization data for each protocol individually. This capability must be available for each monitored interface uniquely.		
EMS.REQ.082	Network Flow-based Traffic Analysis	The proposed solution must keep historical rate and ip to ip, ip to protocol, protocol to protocol conversation data for a minimum of 3 months (most recent) in its current long term operating database. All data in that database must have a maximum 15 minute window granularity.		
EMS.REQ.083	Network Flow-based Traffic Analysis	The proposed solution should include a distributed search engine data-store to ingest various types of textual, numerical, geospatial, structured and unstructured data.		
EMS.REQ.084	Network Flow-based Traffic Analysis	Should support use of policies that can detect violations based on blacklist/whitelist matches.		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.085	Network Flow-based Traffic Analysis	The proposed solution must keep historical rate and protocol data for a minimum of 60 days (most recent) in its short-term operating database. All data in that database must have a maximum 1-minute window granularity with option change retention period		
EMS.REQ.086	Network Flow-based Traffic Analysis	The system must support the ability to create reports that allow the user to search all IP traffic over a specified historical period, for a variety of conditions. o Search for any traffic using a specific configurable destination port, or port range. o Search for any protocol in use by a specific host, interface or list of hosts or interfaces.		
Service Desk - Incident Management				
EMS.REQ.087	Service Desk - Incident Management	The proposed helpdesk system shall provide flexibility of logging, viewing, updating and closing incident manually via web interface		
EMS.REQ.088	Service Desk - Incident Management	The proposed helpdesk solution should have achieved Pink VERIFY certification on at least 6 available ITIL processes (a documentary proof of the same should be provided at the time of bidding).		
EMS.REQ.089	Service Desk - Incident Management	Each incident shall be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.		
EMS.REQ.090	Service Desk - Incident Management	The proposed helpdesk system shall be able to provide flexibility of incident assignment based on the workload, category, location etc.		
EMS.REQ.091	Service Desk - Incident Management	The proposed solution should automatically provide suggested knowledge base articles based on Incident properties with no programming		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.092	Service Desk - Incident Management	The proposed solution should automatically suggest available technicians based on workload, average ticket closure time assigning tickets with no programming		
EMS.REQ.093	Service Desk - Incident Management	The proposed solution should tightly integrate with monitoring system to provide two-way integration - E.g. when system down alarm created, it should automatically create ticket and assign it to technician, in case system comes up before ticket is resolved by technician, it should automatically close the ticket to minimize human efforts		
EMS.REQ.094	Service Desk - Incident Management	The proposed system must not create more than one ticket for same recurring alarm to avoid ticket flooding from Monitoring system		
EMS.REQ.095	Service Desk - Incident Management	The proposed solution should allow administrator to define ticket dispatcher workflow which automatically assign incoming tickets based on rules defined in workflow. E.g. Network fault keyword tickets gets assigned to network technician automatically within NOC team		
EMS.REQ.096	Service Desk - Incident Management	The proposed helpdesk system shall provide grouping access on different security knowledge articles for different group of users.		
EMS.REQ.097	Service Desk - Incident Management	The proposed helpdesk system shall have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues		
EMS.REQ.098	Service Desk - Incident Management	The proposed solution should allow Technician to relate Incidents to Problem, Change and vice versa to have better context while working on any of ticket type		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.099	Service Desk - Incident Management	The proposed helpdesk system shall support tracking of SLA (service level agreements) for call requests within the help desk through service types.		
EMS.REQ.100	Service Desk - Incident Management	The proposed helpdesk system shall integrate tightly with the Knowledge tools and CMDB and shall be accessible from the same login window		
EMS.REQ.101	Service Desk - Incident Management	The proposed helpdesk solution should be equipped with chatbot functionality for identifying the intent of the query and provide an accurate answer and suggest options to confirm or resolve the issue.		
EMS.REQ.102	Service Desk - Incident Management	The chatbot should have NLP functions (Natural Language Processing) to analyse the context of the query.		
EMS.REQ.103	Service Desk - Incident Management	Proposed solution should not be dependent on any third-party NLP algorithm. It should be inbuilt in the product.		
EMS.REQ.104	Service Desk - Incident Management	Proposed helpdesk should have support of inbuilt conversational AI.		
EMS.REQ.105	Service Desk - Incident Management	Proposed helpdesk should support custom theme option including colour scheme of GUI, Fonts and custom logo placement.		
Asset Inventory Management				
EMS.REQ.106	Asset Inventory Management	A configuration management database shall be established which stores unique information about each type Configuration Item CI or group of CI.		
EMS.REQ.107	Asset Inventory Management	The proposed solution allows scheduling periodic report to check current software and hardware inventory		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.108	Asset Inventory Management	The proposed solution must allow attaching CI record to generated service tickets		
EMS.REQ.109	Asset Inventory Management	The Proposed solution should provide end to end Asset Life Cycle Management: Makes it easier to handle the complete life cycle of an asset, that is, all stages/modules from procurement to disposal		
EMS.REQ.110	Asset Inventory Management	The Proposed solution should support maintaining AMC/Warranty Information with Alerting when about to expire also provide Asset Deletion capabilities enabled with workflow engine		
EMS.REQ.111	Asset Inventory Management	The Proposed solution should support Software License Metering: Helps to understand the software license compliance and the use of unauthorized software in the organization and helps to act proactively to curb illegal usage and problems associated with it.		
EMS.REQ.112	Asset Inventory Management	The proposed solution should provide Asset Dashboards/Reporting: Graphical representation all the assets based on Category, location, aging of the asset, customer, which can be further level down to the incident record ID		
EMS.REQ.113	Asset Inventory Management	The proposed solution should provide out of the box purchase and contract management modules to support end to end asset life cycle		
EMS.REQ.114	Asset Inventory Management	The proposed solution must provide asset baselining to manage and track asset effectively.		
EMS Other Key Requirements:				

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.115	Other Requirements	"The proposed EMS solution should have at least 2 deployments (in state/central Government/ PSU) in India with 10,000 devices being monitored in each of these deployments in last five years. Reference PO copy and completion/ sign-off document need to be submitted at the time of submission."		
EMS.REQ.116	Other Requirements	The solution and it's data store should have the feature to be run on virtual appliance and deployable on Linux operating systems to reduce the overall TCO		
IT Operation Analytics Platform				
EMS.REQ.117	IT-Operation Analytics Platform	The solution should provide a pluggable framework to make use of APIs. The framework should support ingestion of data from other applications, export of data from the solution using APIs as well as orchestration of triggers. This solution should provide the ability to use this capability to integrate with other applications for automating tasks and workflows.		
EMS.REQ.118	IT-Operation Analytics Platform	The analytics platform / solution should be built on purely unsupervised machine learning and should monitor all users and all assets in the data center.		
EMS.REQ.119	IT-Operation Analytics Platform	Analytics platform should be built on distributed architecture with Big Data platforms e.g. Hadoop data nodes, control nodes, elastic search nodes, and packet processor to classify & correlate logs with Speed, Accuracy & Focus.		
EMS.REQ.120	IT-Operation Analytics Platform	The proposed solution should be able to consume data from multiple data sources like network devices, operating systems, application etc and should provide centralized view and status of the entire IT landscape.		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.121	IT-Operation Analytics Platform	The proposed solution must be able to provide the following capabilities:		
		Monitor the health of the services from GUI		
		Track issues using the alerts		
		Use aggregation policies to organize and take actions upon alerts		
		Create dashboards to visualize IT and business services and their relationships		
		Troubleshoot issues using deep dives		
		Create multi-KPI alerts and correlation searches to alert conditions that may impact service		
EMS.REQ.122	IT-Operation Analytics Platform	One single syntax that can be used universally for search queries, alerts, reports or dashboards. Also single syntax to do security and IT operations analytics		
EMS.REQ.123	IT-Operation Analytics Platform	The solution should have the capability to provide a schema-less structure giving the ability to add as many fields/columns in the index. The solution should support any number of fields in a particular row of data and should be able to store any amount of data in a particular field.		
EMS.REQ.124	IT-Operation Analytics Platform	The proposed solution must provide a service view that serves as the starting point for monitoring IT operations and enables the visibility of the health of the IT environment at a glance.		
EMS.REQ.125	IT-Operation Analytics Platform	The service view can be configured in tile or tree view and allows further drill down to more detailed information to investigate services with poor health scores.		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.126	IT-Operation Analytics Platform	The proposed solution must provide an alert view page to see alerts for issues that are currently impacting services or may potentially impact services.		
EMS.REQ.127	IT-Operation Analytics Platform	The solution should have capability of conducting detailed analytics, business intelligence analytics, machine learning, pattern analysis, trends & spikes, anomaly detection, etc.		
EMS.REQ.128	IT-Operation Analytics Platform	The proposed solution must allow customisation of visualizations of IT services and key business metrics, and map KPIs to these visualizations to easily view the health and performance of what matters most.		
EMS.REQ.129	IT-Operation Analytics Platform	The customisation capabilities are:		
		Import custom icons for use in the dashboard		
		Configure a shape or icon in your dashboard to act like a KPI or ad hoc search widget.		
		Configure threshold to determine the colour of the widget which indicates the current status of the metric.		
		Configure background colour for a dashboard.		
		Configure drilldowns to another dashboard or a custom URL.		
EMS.REQ.130	IT-Operation Analytics Platform	The proposed solution must provide an investigative tool to help identify and analyse issues in the IT environment.		
		To view KPI search results over time		
		To zoom-in on KPI search results		
		To visual correlate root cause		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		To stack and organize deep dive lanes to create contextual views of metrics across your services		
EMS.REQ.131	IT-Operation Analytics Platform	Utilize NOC-style dashboards for insight into resource consumption of desired systems		
EMS.REQ.132	IT-Operation Analytics Platform	Provides automated investigations, which makes spotting trends and assessing root cause both faster and more accurate		
EMS.REQ.133	IT-Operation Analytics Platform	Has superior indexing, search, stream and machine learning capabilities		
EMS.REQ.134	IT-Operation Analytics Platform	Proposed solution should remove “context switching time” between separate monitoring and troubleshooting tools by correlating metrics and logs in one unified experience		
EMS.REQ.135	IT-Operation Analytics Platform	The solution should also offer the flexibility to the administrator to write customized parsers to understand data format and ensure that 100% of the fields present in the same are indexed individually as per their specific field names to support granular analytics.		
EMS.REQ.136	IT-Operation Analytics Platform	The solution should have inbuilt interactive dashboards to highlight the anomalies/ alerts and showcase the results of detailed analytics, business intelligence analytics etc.		
EMS.REQ.137	IT-Operation Analytics Platform	The solution should have the capability to provide a schema-less structure giving the ability to add as many fields/columns in the index. The solution should support any number of fields in a particular row of data and should be able to store any amount of data in a particular field.		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.138	IT-Operation Analytics Platform	The solution should have inbuilt reporting templates for generating reports for administrators, middle management and senior management		
EMS.REQ.139	IT-Operation Analytics Platform	The platform should facilitate execution of analytics in near real time and timely detection of notable events of threat.		
EMS.REQ.140	IT-Operation Analytics Platform	The platform should provide in-memory analytics & GUI-based capabilities for fast analytics data exploration, data preparation, model building and model deployment to enable faster analytics deployment and faster response times for execution of models.		
EMS.REQ.141	IT-Operation Analytics Platform	The platform should provide basic & advanced analytics capabilities including AI and ML algorithms such as Neural Networks (various forms), Random Forests, Gradient boosting, SVM, etc. to help create-your-own analytical models. The platform should be capable to process and analyse both structured and unstructured data formats in batch and real-time. The platform should have text analytics capabilities to process textual information featuring in various logs, categorize key terms and contextualize those into notable events.		
EMS.REQ.142	IT-Operation Analytics Platform	The solution should have inbuilt interactive dashboards to highlight the anomalies/ alerts and showcase the results of detailed analytics, business intelligence analytics etc.		
EMS.REQ.143	IT-Operation Analytics Platform	The platform solution should be deployable on Linux operating systems to reduce the overall TCO		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EMS.REQ.144	IT-Operation Analytics Platform	Ability to do full-text search on any field in the ingested data based on: Google-like free text search, Selectable Time ranges, Specific or relative time windows down to the month/day/minute/second, Boolean logic (and, or, not, etc),Regular expressions, Wild card syntax, Statistical analyses including: Count of occurrences, distinct count of occurrences, sum, Most common values or least common values of a field, Minimum, maximum, Average, mean, mode, median, Standard deviation, variance, The identification of anomalous values in results that may be irregular, or uncommon, The statistical correlation between fields ,Clustering of events together based on their similarity to each other as a single event, Truncate outlying numerical values in selected fields to assist in statistical correlation, First and last seen value, Percentile, Predicted values (search that looks at historical data to mathematically predict future values), Perform a union, diff, or intersection of individual or multiple search results, Search for relationships between pairs of fields by comparing the values of one field to a reference field and value pair		
EMS.REQ.145	IT-Operation Analytics Platform	The proposed solution should be able ingest 50 GB/day data. There should be no limitation on the number of servers, users or log sources integrated with the solution and it should not have an impact on the license in case servers, users or data source		

Enterprise Management System (EMS)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		count changes, till the time data ingestion size remains 50 GB/day.		
EMS.REQ.146	Overview of solution	EMS will be integrated to all monitoring applications like MDM, ROIP, helpdesk and ticketing tool will be integrated part. Even cyber security tools are to be integrated with EMS		
EMS.REQ.147	Enterprise Management System	EMS tool displaying all SNMP devices and MDT with filed health status of PRVs should be displayed on the video wall in centre. Ticketing system must enable for IT incidents and SLA tool be set-up by TSP on priority		
EMS.REQ.148	Enterprise Management System	Real-time visualization of service level targets, agreement compliance data, penalties, and rewards.		
EMS.REQ.149	Enterprise Management System	EMS shall be available as mobile/web application on MDT/Smartphone for logging complains about IT related issues by PRVs staff in low network area		
EMS.REQ.150	General Requirement	EMS shall have single click dashboard to review all faulty equipment's like MDT, Wireless etc.		

2. Inventory Management

Inventory Management				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IM.REQ.001A	Overview of Solution	MSI should provide an inventory management software to maintain the inventory items used for this project such as Hardware, Furnitures, PRV In-fleet components, Building Infra Components, DCRs equipment's etc. System should be able to monitor inventory on an ongoing basis used for this project.		
IM.REQ.002A	Overview of Solution	All such assets shall be RFID tagged and all the districts and HQ would be provided with RFID reader		
IM.REQ.003A	Overview of Solution	This would ease the stock checking and tracking of assets at central level.		
IM.REQ.004A	Overview of Solution	BAR Code generation to be available, inventory license limitation shall not be there to capture centrally		
IM.REQ.001	General Requirement	Ability to Create unique item numbers for inventory items		
IM.REQ.002	General Requirement	Ability to Monitor inventory on an ongoing basis		

Inventory Management				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IM.REQ.003	General Requirement	Ability to Maintain accurate on-hand balances		
IM.REQ.004	General Requirement	Ability Capture “other” (unknown) stock items other than items pre-identified		
IM.REQ.005	General Requirement	Ability to add requirement		
IM.REQ.006	General Requirement	Ability to generate requisition form		
IM.REQ.007	General Requirement	Ability to Plan material replenishments, based on user requisition		
IM.REQ.008	General Requirement	Ability for E-tendering process and capture item on rental basis		
IM.REQ.009	General Requirement	Ability to Perform online funds checking before creating requisitions		
IM.REQ.010	General Requirement	Ability to seek approval for payment online and E-check generation		
IM.REQ.011	General Requirement	Ability to generate quotation calling form		
IM.REQ.012	General Requirement	Ability to generate store entry information when item received in the store		

Inventory Management				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IM.REQ.013	General Requirement	Ability to create section master and issue the item to particular section		
IM.REQ.014	General Requirement	Ability to maintain list of available vendors or supplier for different items		
IM.REQ.015	General Requirement	Ability to generate comparison chart for a particular item		
IM.REQ.016	General Requirement	Ability to generate Supply Order or Purchase Order		
IM.REQ.017	General Requirement	Ability to create suppler master		
IM.REQ.018	General Requirement	Ability to assign an item to the particular group		
IM.REQ.019	General Requirement	Ability to create group master		
IM.REQ.020	General Requirement	Ability to generate gate entry information when item received in the office		
IM.REQ.021	General Requirement	Ability to generate pending PO when item received is not in good condition		
IM.REQ.022	General Requirement	Ability to generate pending requisition		

Inventory Management				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IM.REQ.023	General Requirement	Ability to Add Attachments to Items		
IM.REQ.024	General Requirement	Ability to View Item Information		
IM.REQ.025	General Requirement	Ability to Assign Items to Catalogues		
IM.REQ.026	General Requirement	Ability to Define Item Relationships		
IM.REQ.027	General Requirement	Ability to Assign Sub-inventories to an Item		
IM.REQ.028	General Requirement	Ability to Assign Items to a Sub-inventory		
IM.REQ.029	General Requirement	Ability to Define Item Revisions		
IM.REQ.030	General Requirement	Ability to Delete Item after the approval from supervising authority Ability to generate alert, if not followed		
IM.REQ.031	General Requirement	Ability to Assign Lot Numbers		
IM.REQ.032	General Requirement	Ability to Maintain Lot Number Information		

Inventory Management				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IM.REQ.033	General Requirement	Ability to Establish lot control for an item		
IM.REQ.034	General Requirement	Ability to Establish lot expiration (shelf life) control		
IM.REQ.035	General Requirement	Ability to Establish lot number uniqueness		
IM.REQ.036	General Requirement	Ability to display item lot information		
IM.REQ.037	General Requirement	Ability to update expiration date and disable status information		
IM.REQ.038	General Requirement	Ability to view supplier lot information		
IM.REQ.039	General Requirement	Ability to view material transactions for an item lot:		
IM.REQ.040	General Requirement	Ability to view on–hand availability for an item lot:		
IM.REQ.041	General Requirement	Ability to Maintain Serial Number		
IM.REQ.042	General Requirement	Ability to Issue Material from Inventory		

Inventory Management				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IM.REQ.043	General Requirement	Ability to generate serial numbers		
IM.REQ.044	General Requirement	Ability to Enter Replenishment Count		
IM.REQ.045	General Requirement	Ability to Transfer Inter–Organization		
IM.REQ.046	General Requirement	Ability to Return to Stores		
IM.REQ.047	General Requirement	Ability to Update Average Cost		
IM.REQ.048	General Requirement	Ability to see your changes reflected in the Interface Managers window		
IM.REQ.049	General Requirement	Ability to search an item by typing some of the initial letters		
IM.REQ.050	General Requirement	Ability to view Direct organization transfer		
IM.REQ.051	General Requirement	Ability to view In-transit receipt		
IM.REQ.052	General Requirement	Ability to view In-transit shipment		

Inventory Management				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IM.REQ.053	General Requirement	Ability to capture issue voucher parameters		
IM.REQ.054	General Requirement	Ability to define Shipping Methods		
IM.REQ.055	General Requirement	Ability to define Movement Statistics Parameters		
IM.REQ.056	General Requirement	Ability to Link Movement Statistics to Invoices		
IM.REQ.057	General Requirement	Ability to View Material Transactions		
IM.REQ.058	General Requirement	Ability to View Transaction Summaries		
IM.REQ.059	General Requirement	Ability to maintain audit trail of entire Transaction		
IM.REQ.060	General Requirement	Ability to Viewing Pending Transactions		
IM.REQ.061	General Requirement	Ability to View On–hand Quantities along with expiry dates for consumables		
IM.REQ.062	General Requirement	Ability to raise an alert if balance quantity attains minimum level		

Inventory Management				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IM.REQ.063	General Requirement	Ability to View Item Supply or Demand Information together with chart-based increase or decrease demand history of an item		
IM.REQ.064	General Requirement	Ability to Reserve Available Inventory		
IM.REQ.065	General Requirement	Ability to Summarize Demand History		
IM.REQ.066	General Requirement	Ability to maintain history of maintenance of Inventory items with alert facility to the concerned authority		
IM.REQ.067	General Requirement	Ability to seek approval for payment online and E-check generation		
IM.REQ.068	General Requirement	Ability to maintain service history of Inventory items with cost incurred previously		
IM.REQ.069	General Requirement	Ability to Define a Forecast Rule		
IM.REQ.070	General Requirement	Ability to Enter and Reloading Item Safety Stocks		
IM.REQ.071	General Requirement	Ability to Reorder Point Planning		

Inventory Management				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IM.REQ.072	General Requirement	Ability to Enter and Processing Replenishment Counts		
IM.REQ.073	General Requirement	Ability to Maintain Accounting Periods		
IM.REQ.074	General Requirement	Ability to support both process and discrete organization		
IM.REQ.075	General Requirement	Dual Unit of Measure Tracking for on hand inventory and every Inventory transaction		
IM.REQ.076	General Requirement	Ability to search stock items by Name, Manufacturer, date of purchase etc.		
IM.REQ.077	General Requirement	Ability to view inbound in-transit material, summary view across organizations of inbound, receiving and on-hand material and availability by serial		
IM.REQ.078	General Requirement	Shall be integrated with RFID based solution and managing the inventory of all the tagged items		
IM.REQ.079	General Requirement	Inventory check to be done by MSI to support the department. However, stock inventory under Inventory application to be managed by department with the help of MSI.		

3. Citizen Portal

Citizen Portal				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
CP.REQ.001A	Overview of solution	MSI should develop portal which can be interface provided for the citizens to interact with the emergency response system		
CP.REQ.002A	Overview of solution	Portal should have some standard content as provided by UP112		
CP.REQ.003A	Overview of solution	It should provide option to citizens to register their phones or devices along with GIS coordinates of their homes, offices, schools etc. to be able to connect with UP 112 and OMC in case of emergency It should have provision to initiate email, chat with the officer of UP state		
CP.REQ.001	General requirement	The Portal should be hosted at the data center infrastructure being installed by the MSI		
CP.REQ.002	General requirement	The Portal should be state of the art with user friendly interface, informative, interactive, and easily accessible.		
CP.REQ.003	Citizen Registration	The Portal should be able to register citizens on the website.		

Citizen Portal				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
CP.REQ.004	Citizen Registration	The registration should include data such as name, contact information, mobile number, IoT device detail, email, address, photo ID, gender, blood group, emergency contacts etc. These fields are for sample purpose. It may modify or increase on later stages.		
CP.REQ.005	Citizen Registration	The information collected from the registration should be verified with one time password on the Citizen mobile number.		
CP.REQ.006	Citizen Registration	Once the Citizen has registered, the Citizens would be prompted to download the mobile application		
CP.REQ.007	Search Functionality	The Portal should be searchable to query registration patterns, users, regional specifics etc.		
CP.REQ.008	Portal Features	The Portal should have the following features for citizens:		
		Overview about emergency helpline services		
		Brief statistics of emergency helpline like No. of cases registered, No. of resolutions etc.		
		Administrative setup for UP112		

Citizen Portal				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		Access to various literature related to rules and regulations		
		Feedback and RSS feed.		
		News Section		
		Contact us		
		Link for administrators for various modules or components including components for security, database, user administration etc.		
		Information related to Rights to Information Act that may be required to be made public.		
		Information about various acts and sections relevant to emergency helpline services and all services of UP Police		
		MIS reports for citizen, UP112 and identified stakeholders. MIS reports from the BI application also need to be integrated with the portal.		
		The Portal shall be linked to social media sites (Facebook, twitter etc.) and count should be displayed of no. of likes of the UP-112 Portal		

Citizen Portal				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		An effective presence on all major social media platforms like Facebook, twitter, YouTube, Instagram etc. will be created and kept undated. This will be integrated with the citizen portal		
		The Portal shall have link for downloading the application from App stores (Android, iOS, Windows etc.)		
		The Portal shall provide the steps for downloading, installation and using the application.		
		The Portal shall also have a short video on how to use the mobile application.		
		The Portal should have a section on Frequently Asked Questions (FAQ) with pre-defined answers.		
		The Portal should have a contact information on emergency numbers or non-emergency numbers etc.		

Citizen Portal				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
CP.REQ.009	Chat Window	The Portal should be integrated with Chat Window functionality where citizen can do the chat with call center Officer. Citizen should be able to initiate the chat after giving the location of the chat location, citizen name and contact number.		
CP.REQ.010	Common requirements of Portal	The portal should meet and compliant the web design and security guidelines of Govt. of India		
		The system should adhere to Best or Standard programming practices and other recommended security practices that can help authorized user to easily extend the functionality of the portal.		
		The system shall provide consistent look & feel, Themes, Navigation to the users and the standards defined for content, structure and presentation of the portal shall be applied and followed throughout the portal.		
		All the sections of the portal should be of dynamic nature and must be supported with easy content management and administration of the same.		
CP.REQ.011	Portal Administrator	The Portal should have administrator console where administrator can manage the content, users and can		

Citizen Portal				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		create portal dynamic menus (a common navigation bar should be included on all pages)		
		The Portal administrator should be able to modify or design custom look and feel of the portal with minimal change in software code.		
CP.REQ.012	Portal Administrator - Publishing	The system should allow the authorized user to publish Emergency Helpline news, articles, events etc.		
CP.REQ.013	Portal Administrator -News Content	The system should allow the user to upload the emergency helpline NEWS content with following details:		
		· News Heading		
		· Date of publication		
		· News source		
		· Reported by		
		· Newsroom		
		· News search key word		
		· News main content		

Citizen Portal				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		The system should allow the user to attach image related to news		
CP.REQ.014	Multimedia Support	The system should adhere to automatically format images and other rich media based on predefined standards for resolution, size etc.		
CP.REQ.015	Security	The system shall ensure virus check for all files that are uploaded in Solution e.g., detect malicious executables.		
CP.REQ.016	Security	Wherever documents are involved, the system should allow the user to assign a note or annotation to a document image.		
CP.REQ.017	Security	The system shall support provide support for HTTPs or SSL for secured data transfer and session timeouts.		
CP.REQ.018	Single Sign on Access	Internal user should be able to access the internet portal using single sign on and should be able to access the relevant application assigned to the user as per roles and permission		
CP.REQ.019	Internal Application Access	All the internal application like HRMS, Finance Management, Patrol Management etc. Should be able access by the internal user through this portal based on roles and permission to the user		

Citizen Portal				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
CP.REQ.020	Intranet portal access	Portal should be integrated with Intranet portal for internal user		
CP.REQ.021	Internal user detail	Information for Internal user on portal will be available to entire hierarchy of the field officer as per jurisdiction over the internet starting with station house officer, circle officer, additional SP city or rural area, SSP/SP, DIG, IG, IG (law and order), ADG (law and order), DGP based on user roles and permission		
CP.REQ.022	Audit Trail	The system shall display the date and time of last login when the user logs in.		
CP.REQ.023	Portal Content Management	The system should allow the authorized user, through a user-friendly GUI, to manage or edit the content of the various web pages. It shall allow authorized user to manage and maintain content of website in an efficient manner. User should be able to perform advanced update maintenance jobs on website content with minimal technical knowledge on website development.		
CP.REQ.024	Portal Content Management	The front-end user interface must be integrated with content management solution for easy management and change of theme design.		

Citizen Portal				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
CP.REQ.025	Portal Content Management	The system should allow the authorized user, through a user-friendly GUI, to design and create a web page dynamically and publish it through an approval workflow. It should provide feature to define the position of the web page like center frame, left frame, or right frame etc.		
CP.REQ.026	Portal Content Management	The system should allow the authorized user, through a user-friendly GUI, to create meta tag search of each web page.		
CP.REQ.027	Portal Content Management	It should allow the authorized user to upload any image, on the page and further allow him to define position of the image on web page		
CP.REQ.028	Portal Content Management	The system should allow the authorized user, through a user-friendly GUI.		
CP.REQ.029	Search Content	The system should be able to search the Fire, Medical, Police and other databases as per requirement.		
CP.REQ.030	Search Archive Content	The system should be able to search the archive content through internet portal		
CP.REQ.031	Reporting access	There should be user access control on Citizen portal		

Citizen Portal				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
CP.REQ.032	Portal Content Management	The system should allow the user for meta tag basis search option. The search result should show path of the web page with brief description of the page or else first 20-30 words of the page. Solution should further allow drill down to the page.		
CP.REQ.033	Mobile Compatibility	The portal should be accessible on Smartphone		
CP.REQ.034	IoT Integration	User can register their IOT devices with details on Portal		
CP.REQ.035	Public Information Centre	It will serve purpose of Public Information centre		

4. Web and Desktop Application for Monitoring - Police officials

Web and Desktop Applications for Monitoring- Police officials				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or no)**	**Deviation**
WDA.REQ.001A	Overview of Solution	Web application over MPLS network available to monitor the activities by Field officer and DCR in their jurisdiction.		

Web and Desktop Applications for Monitoring- Police officials				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or no)**	**Deviation**
WDA.REQ.002A	Overview of Solution	Officer can monitor the activity and location of PRV for the events and can perform appropriate action on requirement shall basis.		
WDA.REQ.003A	Overview of Solution	Web application all functionalities of mobile application		
WDA.REQ.001	General Requirement	Web application shall be available over MPLS network to monitor the activities by Field officer in their jurisdiction.		
WDA.REQ.002	General Requirement	Officer shall be able to monitor the activity and location of PRV for the events and can perform appropriate action on requirement basis		
WDA.REQ.003	General Requirement	Application shall have all the details and features of Police Officials mobile application		
WDA.REQ.004	General Requirement	Application shall be integrated with VTS		
WDA.REQ.005	General Requirement	Should have feature for monitoring like VTS, PMS etc from a single click		
WDA.REQ.006	General Requirement	UI shall be simple and graphic rich		
WDA.REQ.007	General Requirement	Modules such as visit request needs to be added in the module.		

5. Mobile application for Police Officials

- Proposed feature for the application

Mobile applications for Police Officials				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
Supervisor Application				
MA.REQ.001A	Overview of Solution	Mobile application to be provided to Field officer in their jurisdiction for monitoring purpose.		
MA.REQ.002A	Overview of Solution	Officer can monitor the activity and location of PRV for the events and can perform appropriate action on requirement basis		
MA.REQ.001	General Requirement	The Mobile Application shall provide feasibility of cases monitoring		
MA.REQ.002	General Requirement	This application will be having a login id and password to access the application.		
MA.REQ.003	Single Sign On (SSO)	The application should support single sign on feature to avoid need of re-login for various modules or sections		
MA.REQ.004	Forgot Password	The application should have a functionality like forgot password etc. in case user lost its password. An auto email should be generated to the user with temp password and user can rest the password after entering the temp. password into the application.		

Mobile applications for Police Officials				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
MA.REQ.005	User Dashboard	Supervisor should be able to see state, district, and city level data only on dashboard in graphical format based on pre-defined roles and permission to the user. User should be able to navigate and drill down the data to see the details on click event on dashboard on requirement basis into the application. Some of the features are given below for sample purpose: 1. Call Trend – day, week, and month 2. Average Response Time for call or non-call cases (SMS, chat, email etc.), dispatching and responding units. 3. Event Type 4. Police stations 5. Vehicle Activity – Run Time and Halt Time 6. Vehicle distance travelled 7. non-Call trend like email, SMS, chat etc. - day, week, and month etc. 8. Officer Key Performance Index (KPI) with details based 9. Shift details 10. View the performance and health check of MDT Devices fitted in the patrol vehicles 11. Should be integrated with other application like EMS to see the SLA, Networking data etc.		

Mobile applications for Police Officials				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
MA.REQ.006	Push Notification	the application should be able to receive the push notification for each case which is created and updated in UP112-Contact Center and OMC by the communication and dispatch Officers and other government users who are provisioned to access the application in the system		
MA.REQ.007	Unlock of Case	The software should be able to unlock the assigned case in process and reassign to another RMO/ PRV to take further action.		
MA.REQ.008	Case Update or Close	The application should be able to update or close the case in the application.		
MA.REQ.009	GIS Map Integration	The application should be integrated with GIS map application to see the vehicles' location of the state and should be able to send the SMS and notification in case of emergency to MDT Device of the vehicle		
MA.REQ.011	Call Button	The application should have a call button for the user to make a call. This should be linked to the mobile contact list.		
MA.REQ.012	Application Setting	The Supervisor application should be able to undertake various mobile application settings and configuration such as given below. These features are for sample purpose. It may increase on later stages - Disable the Push Notification		

Mobile applications for Police Officials				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
MA.REQ.013	General Requirement	Mobile application should be supported on iOS, Android, Windows OS platform and be upgradable or portable on any latest OS that may come in future.		
MA.REQ.014	General Requirement	Mobile application should be able to download from department website over the intranet		
MA.REQ.015	General Requirement	Application should respond promptly while loading contents while being user friendly		
MA.REQ.016	Calling	Mobile application shall have a call button for audio and video call to 112 system		
MA.REQ.017	General	The application shall get the data on real time basis i.e., event related details shall pop on supervisory application as it gets displayed on MDT		
MA.REQ.018	Platform	Should be easily accessible on play store/apple store with certain user authentication for download. Application shall also be downloadable through department's website over the internet/ intranet		
MA.REQ.019	Login	FORGOT PASSWORD option shall be available to users to retrieve their passwords.		
MA.REQ.020	Login	An auto email should be generated to the user with temp password and user can rest the password		

Mobile applications for Police Officials				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		after entering the temp password into the application		
MA.REQ.021	Login	The application should support single sign on feature to avoid need of re-login for various modules or sections		
MA.REQ.022	GIS	The application should be integrated with GIS map application to see the vehicles' location of the state Device of the vehicle		
MA.REQ.023	Dashboard	Each senior official should be able to see their state, district, and city level data dashboard. Each district user shall have restrictive view on other district's data. User should be able to navigate and drill down the data to see the details on click of event on dashboard on requirement basis into the application.		
MA.REQ.024	Recording	Caller and CO communication recording shall be available for high priority calls		
MA.REQ.025		OTP level authentication and Mac address binding for login to the application.		
Senior Officer at State Level				

Mobile applications for Police Officials				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
MA.REQ.026	General Requirement	The Mobile Application shall provide feasibility of case monitoring		
MA.REQ.027	General Requirement	This application will be having a login id and password to access the application.		
MA.REQ.028	Single Sign On (SSO)	The application should support single sign on feature to avoid need of re-login for various modules or sections		
MA.REQ.029	Forgot Password	The application should have a functionality like forgot password etc. in case user lost its password. An auto email should be generated to the user with temp password and user can rest the password after entering the temp password into the application.		
MA.REQ.030	User Dashboard	Each senior official should be able to see their state, district, and city level data only on dashboard in graphical format. It will be restricted to see the other state data. User should be able to navigate and drill down the data to see the details on click event on dashboard on requirement basis into the application. Some of the features are given below for sample purpose: 1. Call Trend – day, week, and month 2. Average Response Time for call or non-call cases (SMS, chat, email etc.), dispatching and responding units. 3. Event Type		

Mobile applications for Police Officials				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		4. Police stations 5. Vehicle Activity – Run Time and Halt Time 6. Vehicle distance travelled 7. non-Call trend like email, SMS, chat etc. - day, week, and month etc. 8. Officer Key Performance Index (KPI) with details based 9. Shift details 10. View the performance and health check of MDT Devices fitted in the patrol vehicles 11. Should be integrated with other application like EMS to see the SLA, Networking data etc.		
MA.REQ.031	Push Notification	The application should be able to receive the push notification for each case which is created and updated in its center by the supervisor		
MA.REQ.032	Call Button	The application should have a call button for the user to make a call. This should be linked to the mobile contact list.		
MA.REQ.033	Application Settings	The application should be able to undertake various mobile application settings and configuration such as given below. These features are for sample purpose. It may increase on later stages - Disable the Push Notification		
MA.REQ.034	General Requirement	Mobile application should be supported on iOS Or Android platform and be upgradable or portable on any latest OS that may come in future.		

Mobile applications for Police Officials				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
MA.REQ.035	General Requirement	Mobile application should be able to download from department website over the intranet		
MA.REQ.036	General Requirement	Mobile application will be formed considering Police and Fire department requirements		
MA.REQ.037	Real time event feature	1. This application shall get the event related data on real time basis. 2. The application shall be able to provide the call recording of communication between caller and communication officer but only on request basis. 3. The call recording feature shall be available up to SP and above level		

6. Patrol Management System

- Proposed feature for the application

Patrol Management System				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
PMS.REQ.001A	Overview of Solution	• The Patrol Management System enables us to define, assign and monitor the routes, allocation, and utilization of resources. A Patrol Management application also be installed on MDTs for managing the Patrol related activities of the PRVs. The application will cover the following: • Define landmarks • Define routes • Add/Update details of personnel available • Send and Receive patrols • Reports/MIS • This application shall also be able to capture details of arrests and seizures (if made) during patrols.		
PMS.REQ.001	General	Should be able to define the routes for PRV patrolling (based on Maps with PoI (Point of Interests or Landmarks) along the route		

Patrol Management System				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
PMS.REQ.002	General	Once the Routes have been defined, the System should be able to assign timings (Time taken for a PRV to travel from POI-1 to POI-2 along the defined route) and halt time at each PoI		
PMS.REQ.003	General	Once the timings have been assigned, System should be able to allocate manpower (PRV Police Personnel) for the defined and assigned Route. It should also be able to add or update details of personnel available		
PMS.REQ.004	General	System should be able to assign the PRVs and Drivers for the defined route should be able to send and receive patrol routes over device		
PMS.REQ.005	General	Patrol Management System should be so designed as to pick up locational data from the GIS system that is part of the solution. The locations of the patrol route traversed by a vehicle should get auto populated from the system with associated date and time stamp picked from the system and should be coupled with locations visited.		
PMS.REQ.006	General	It should be able to generate MIS in various formats as required for patrolling		

Patrol Management System				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
PMS.REQ.007	Login	PMS should provide authentication functionality for administrator with ID and Password which shall be deployed at central server generated through PMS server application.		
PMS.REQ.008	Login	PMS should provide normal users on the field a login with ID and password and if field user forgets his password, he can ask the Administrator for his user ID and password and the administrator can help him get his credentials centrally.		
PMS.REQ.009	Administrative Rights	In “Patrol Management System”, administrator shall be given some additional rights. Admin will be able to create any number of Users, depending on the requirements. He may rotate Coy or may view previous rotation details. He can Import or Export Officer or Official list and Import map along with its coordinates.		
PMS.REQ.010	Administrative Rights	Administrator shall be able to i. Create User with login, name, password etc. details ii. Can view duty rotation of PRV staff		

Patrol Management System				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		iii. Can import and export PRV staff list for patrolling iv. Can import maps and coordinates v. Can change images and store centrally vi. Other files access will be there in PMS. It will only be used when there is a need of addition or deletion in master file (Landmark, Location etc.). vii. PMS activities with a daily patrolling record day to day activity will be available. viii. System should allow the Circle Officer of Field Police and above with all Master Administrator rights to request route, assign timings and manpower. District Inspector shall have the rights of allocation of patrols and perform the above activities.		
PMS.REQ.011	User rights	PRV Police Personnel shall be able to: i. Import Master Files to see patrolling duties ii. Patrol Activities for day and week		

Patrol Management System				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		iii. Pending activities of patrolling of PRV iv. Reports to export about patrolling details v. Feed about start and finish about patrol vi. Change Images of landmarks		
PMS.REQ.012	Application Content	PMS will have master file which will have features like Open MAP for normal patrolling routes will be there		
	Application Content	PMS will have file which will have guide for best route options during day, night-time, other situations like traffic jam, rally		

Patrol Management System				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
PMS.REQ.013	Application Content	PMS will have master files for Landmarks which will show the prominent points under fall on the patrolling routes. It may be a local and provincial data like hospitals, locally called landmarks, malls, Police stations etc. While selecting the landmark certain point would be taken care of. such as: i. It should be static. ii. It should not be too large or scattered. For example, if someone want to select 'hospital' as a landmark then select the main gate of that hospital as an actual landmark. iii. To convert 27o 30' 45" into degree or decimal following formula may be used- 27 + 30 Or 60 + 45 Or 3600 = 27+ 0.5 + 0.012500= 27.512500 iv. PMS should not choose landmarks very close to each other. Distance between each landmark must not be less than 20 metres.		

Patrol Management System				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		27 + 30 Or 60 + 45 Or 3600 = 27+ 0.5 + 0.012500= 27.512500 iv. PMS should not choose landmarks very close to each other. Distance between each landmark must not be less than 20 metres. iv. PMS should not register unnecessary landmarks in PMS. v. Landmarks should be scattered in the entire patrolling routes		
PMS.REQ.014	Application Content	PMS will have Create Route option in field which will be authorized by the administrator and shall contain following options: i. Route with landmarks ii. Existing route table on upper right side iii. Map on the lower right side		
PMS.REQ.015	Application Content	PMS will be enabled on GPS devices which records and shows geo-coordinates (may say location) of any point on their route. It will record the geo-coordinate of points on routes in regular intervals which		

Patrol Management System				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		will further utilize showing route of the patrol party on map.		
PMS.REQ.016	Patrol activities	PMS application should have the following feature of patrol activities: i. Send Patrol: When any district is selected, all existing routes for that District will appear in the dropdown box “Route Name”. Select any one of them where PRV wants to send patrol. When route is selected, the landmarks falling on that route will appear in the lower table as well as on map. There will be a selection option of patrol ‘in’ and ‘out’ time with date. Also, option to fill “Reaching Time” and “Halt Time” (In minutes) at any Landmark. Further “Patrol Duration” and “Patrol Distance” will also appear at the bottom of screen.		

Patrol Management System				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		ii. There will also be an option to make any amendment in time or configuration of patrolling staff (Police Personnel as well as Drivers) iii. Receive Patrol: When send patrol is covered by PRV staff there would be option for PRV Staff to show “Actual Reaching Time” and “Actual Waiting Time” during route. These entries will be filled according to the narration of the PRV staff to record daily patrolling route of vehicles. iv. All details of patrolling routed will be filled using MDT devices v. There will be list of pending patrolling routes in application to show if PRV has not covered defined patrolling route for that day		
PMS.REQ.017	Patrol Order Sheet	Circle Officer and above rank officers can define Patrol order sheet. The Patrol order		

Patrol Management System				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		sheet will be sent to PRV through GPS over MDT which will consist of: i. Patrol Order sheet unique number ii. Date of Patrol iii. Patrolling routes information iv. Reaching Time v. Halt time vi. Detail of PRV staff vii. Single sign on of PRV staff PRV staff will fill required details and submit the order sheet back to respective officer. In charge officer will approve the Patrol order sheet submitted by PRV staff. There will also be option for printing the patrolling sheets through weblink.		
	Integration requirements	System needs to be integrated with central HRMS system for allocation of manpower (Police PRV personnel) for the defined Patrol Routes		
		System needs to be integrated with Fleet management application for assigning Drivers and Vehicles for the defined Patrol Routes		

Patrol Management System				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		Landmark should be prominent and static		
		Landmark should be recorded with Long/Lat		
PMS.REQ.018	Detailed MIS Reports	PMS will display patrolling reports for monthly, weekly, and daily basis of PRV		
		i. Reports can be monitored by web link from officers sitting in UP112-Contact Center, OMC and field ii. Reports will be designed considering factors like: iii. MIS reports must be able to display the performance of Circle Officers and above based on the activities performed by them using the Patrol Management Application iv. PRV patrolling routes v. PRV associated to districts vi. PRV patrol monitoring vii. Yearly Monthly, weekly, daily MIS viii. Assigned patrol routes covered ix. Seizure or alert during patrolling x. Deviations from assigned routes xi. Addition of new routes for patrolling xii. Addition of landmarks		

Patrol Management System				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		xiii. Map report which displays the route of patrol		
PMS.REQ.019	Browsing capabilities	The MDT user in field will be able to browse application on MDT in field		
		The Dy SP and above rank officers can view MIS over web link in UP-PICC and OMC		
		The District PRV manager, Circle Officer and SP Or SSP rank officers can view the patrolling in their respective districts over app and web link		
PMS.REQ.020	General Requirement	Feasibility to mention number of shifts should be available for any number of days.		
PMS.REQ.021	General Requirement	List of personnel available without patrol assignment should be visible at different police stations level and at aggregated level, for their better utilization at elsewhere		
PMS.REQ.022	General Requirement	A single view is required for no of PRVs assigned, Patrols and personnel, and remaining ones, with lists for any forthcoming shift- today evening, tomorrow morning etc.		

Patrol Management System				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
PMS.REQ.023	General Requirement	Proper integration of HRMS and PMS shall be possible to make assigners job easier i.e. The assigners shall have the details of available staff on the PRV so the communication of patrolling routes can be done with the respective staff		
PMS.REQ.025	General Requirement	Application shall have flexible date assignment functionality. Patrol routes are generally not repeated with same timings on consecutive days.		
PMS.REQ.026	General Requirement	UI should be simple with drag and drop functionality		

7. Fleet Management Solution

- Proposed features for the application

Fleet Management Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
FMS.REQ.001A	Overview of solution	MSI to provide with the tools that shall organize, manage, and coordinate work PRVs from a single platform.		
FMS.REQ.002A	Overview of solution	It helps to improve performance, provide compliance, and optimize costs		
FMS.REQ.003A	Overview of solution	It shall be integrated with HRMS in order to determine the staff of the PRVs for the given time period/slot.		
FMS.REQ.001	Maintenance planning	To receive routine information/ notifications for preventive maintenance		
FMS.REQ.002	Digital Vehicle Inspection Reports	Digital Vehicle Inspection Reports (DVIR) to report vehicle and maintenance issues quickly and efficiently.		
FMS.REQ.003	Driver Behaviour	Application shall generate real-time PRV pilot behaviour data and driver risk profile to help fleet managers for identifying drivers who are at high risk.		
FMS.REQ.004	Driver safety league tables	Fleet management systems would also create driver safety league tables that can be used for safe driving incentive programs.		

Fleet Management Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
FMS.REQ.005	Integration with MDT	Application shall be installable to MDT for PRV management that shall be used by the field staff for supervision of PRV operations and maintenance e.g., refuelling of vehicles, submission of bills, logging the odometer readings at the time of PRV handover-takeover for patrol vehicle mileage validation, periodic inspection reports, and code violations if any etc. Thus, application shall be properly functional on MDTs, Tablets, computers, and mobiles		
FMS.REQ.006	Business Intelligence	The application shall provide insights in terms of BI reports for 1 glance view as well as in forms of detailed reports.		
FMS.REQ.007	General requirement	Fleet management application should be able to facilitate supervision, monitoring, and effective management of 4W and 2W PRVs		
FMS.REQ.008	Technology	The application should be able to be installed on MDT and should work seamlessly on the Desktops using a web link (for usage by UP112		

Fleet Management Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
		or its representative and by the District PRV Manager from its premises)		
FMS.REQ.009	MIS Generation Capabilities	The system should be able to generate all kinds of reports necessary for efficient management of PRVs and should include (but not limited to): a. PRV Fabrication design report b. PRV Pilot vehicle delivery report c. PRV received report d. PRVs Handover report e. PRV acceptance report f. PRV maintenance reports g. PRV inspection reports h. PRV fuel reports i. PRV personnel reports j. PRV personnel salary reports k. PRV accidental repair reports l. PRV code violation reports m. PRV personnel training reports System should allow the generation of these reports by MSI or UP112 or their authorized representatives in the minimum possible time		

Fleet Management Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
FMS.REQ.010	Online Odometer Logbook	The application shall have a provision of logging the odometer readings at the time of PRV handover-takeover so as to capture the details of patrol mileage by the outgoing PRV personnel. These readings as captured by the application shall be reported to the central system and shall act as an authentic source of validation. The system should be able to integrate with the AVLS and also the GPS in MDT with Odometer for automatic update of the Kilometers travelled		
FMS.REQ.011	Validation of odometer readings	System will enable other sources of validation of the odometer readings submitted by the PRV personnel through the in-built GPS in MDT that tracks the distance run by the PRV on its assigned Patrol route every day as part of the central solution that tracks each of the 4800 PRVs across the state		
FMS.REQ.012	Operational records maintenance	The system will facilitate maintenance of proper records of operations including (but not limited to): 1. PRV personnel logs (For Drivers, District PRV Managers including their personal details,		

Fleet Management Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
		attendance through the biometric module, leaves etc.) 2. PRV Maintenance Service Book 3. Repair or Maintenance History for each PRV 4. Breakdown or Maintenance or Out of Service schedule 5. Maintenance files for 2W and 4W PRVs (with maintenance status etc.) 6. Inventory of consumables required for uninterrupted PRV operations 7. PRV periodic inspection reports 8. Fuel records, Fuel Card-Driver Id Card transaction summary reports 9. Vehicle maintenance records		
FMS.REQ.013	PRV Response Time recording and reporting	System shall also be able to provide PRV Response time records to UP112 through the application online. The data should be suitable for Statistical Analysis for all PRV responses. These records should include the following data		

Fleet Management Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
		elements: PRV-identifier, Time-PRV en-route, Time-PRV clear and Time-PRV-available for the next call.		
FMS.REQ.014	PRV Periodic Inspection Report	The application should have provision to monitor and enlist periodic Inspections (at least one every Calendar Month) to determine the PRV condition including compliance or otherwise with the maintenance manual, the maintenance program me, specifications (through MDTs) and standards and the maintenance required and shall submit online reports of such Inspections to the Department through the MDT application.		
FMS.REQ.015	Manual	The application will store PRV manuals, general PRV handling guides etc. in electronic format		
FMS.REQ.016	Maintenance of other Police records	System should be able to maintain all the other relevant Police records in electronic format and should be readily available for Department's use at any point of time		
FMS.REQ.017	Authorized Service Centers	The system should be updated with the List of Authorized Service Centers and should allow		

Fleet Management Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or no)	Deviation
		the update of this list by the user whenever required		

8. Mobile Device Management (MDM)

Mobile Data Management				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
MDM.REQ.001	Mobile Data Management	The solution must support mainstream versions of Android, Windows Phone,		
MDM.REQ.002	Mobile Data Management	Chrome OS, Windows Rugged and Windows desktop Operating Systems.		
MDM.REQ.003	Mobile Data Management	The solution should provide Zero-day support for mainstream versions of Android, Windows		
MDM.REQ.004	Mobile Data Management	Phone, Chrome OS, Windows Rugged and Windows desktop Operating Systems.		
MDM.REQ.005	Mobile Data Management	The solution should use a common MDM agent for all the devices and platform.		
MDM.REQ.006	Mobile Data Management	The solution should provide remote management and automatic updates and upgrades for the provisioned devices from a centralized Web console.		

Mobile Data Management				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
MDM.REQ.007	Mobile Data Management	The MDM solution should provide granular & detailed MDM capabilities like Password management, device restriction, remote wipe & lock.		
MDM.REQ.008	Mobile Data Management	The MDM solution should provide the real- time device inventory status like Battery, network, passcode present on device or not, Location Information.		
MDM.REQ.009	Mobile Data Management	The solution must have capability to generate automated, scheduled reports and real-time dashboards.		
MDM.REQ.010	Mobile Data Management	The MDM solution should Detects jailbreak or rooting before allowing enterprise resource access.		
MDM.REQ.011	Mobile Data Management	The MDM solution should Checks device policy compliance before allowing enterprise resource access.		
MDM.REQ.012	Mobile Data Management	The Solution should be part of mobile security alliance and provides threat security for business mobility against cyber-attacks by integrating the industry's leading security solutions.		
MDM.REQ.013	Mobile Data Management	The MDM solution should have an automatic policy control that deletes all enterprise policies, profiles, apps and data if the management agent is removed.		
MDM.REQ.014	Mobile Data Management	The MDM Solution should support Kiosk mode to restrict device to run approved applications.		

Mobile Data Management				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
MDM.REQ.015	Mobile Data Management	The Solution should provide user self-service portal to manage their own devices and corporate access (GPS, Policy and Security Management, Compliance visibility).		
MDM.REQ.016	Mobile Data Management	The Solution should be able to enforce conditional access policies based on identity, authentication strength, data sensitivity, user location, device compliance.		
MDM.REQ.017	Mobile Data Management	The Solution should have the capability to support both on-prem and on cloud deployment model with same set of features and functionality.		

9. HRMS

- Proposed features of the application

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.001A	Overview of Solution	HRMS shall be a native application that will be available on Web and Mobile Application		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.002A	Overview of Solution	HRMS Solution will facilitate in enabling effective monitoring and supervision of UP POLICE 112 staff at HQRS, OMCs, DCRs and PRV staff.		
HRMS.REQ.003A	Overview of Solution	HRMS shall be available even for other non-Gov. employees such as Communication officers, Communication Supervisory staff, Technical Manpower of MSI, Building Management Staff		
HRMS.REQ.004A	Overview of Solution	HRMS to be developed for Facial based attendance solution installed on MDT for attendance of PRV staff and Integrate with Biometric Systems available at UP112 HQRS, OMCs and DCR for attendance management		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.005A	Overview of Solution	HRMS software would be designed for UP112 operations. This would cover the electronic supervision and measurement of the following indicative personnel processes and transactions related to: • Time and attendance • Payment to agency • Leave management • Travel management of staff • Transportation • Transfer or promotion of outsourced staff • Rewards and recognition received • Training conducted • Code violations if any • Complete life cycle of personnel from selection, evaluation to exit grievance redressal		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.001	General Requirement	The solution must be fully integrated system and automate all related processes for State-wide UP112 staff		
HRMS.REQ.002	General Requirement	The solution must be real-time update and access of detail data		
HRMS.REQ.003	General Requirement	The solution must support facility to provide centralized key services		
HRMS.REQ.004	General Requirement	System should enable accurate and flexible mapping of organizational roles		
HRMS.REQ.005	General Requirement	It should have accurate and easy availability of information with drill downs, drill ups with supporting data		
HRMS.REQ.006	General Requirement	It should provide Authentic, reliable, accurate and timely data		
HRMS.REQ.007	General Requirement	It should have Business intelligence, MIS from the system (reports daily or weekly or monthly or yearly or till date) comparison of data (Past or Current)		
HRMS.REQ.008	General Requirement	System should be web based		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.009	General Requirement	All forms and reports should be downloadable and printable in pdf format		
HRMS.REQ.010	General Requirement	Should be able to integrate with user directory		
HRMS.REQ.011	General Requirement	Should have the ability to integrate with Patrol Management System		
HRMS.REQ.012	General Requirement	Should be able to integrate with single sign based on different user roles		
HRMS.REQ.013	Attendance & Leave Management	HRMS will be integrated with biometric system for attendance		
HRMS.REQ.014	Attendance & Leave Management	System should have ability to view list of weekly offs, holidays in a year of ITECCS, field and OMCs staff		
HRMS.REQ.015	Attendance & Leave Management	System should have ability to define types of leaves: sick leave, privilege or earned leave, casual leave etc.		
HRMS.REQ.016	Attendance & Leave Management	System should have ability to apply for leave under the appropriate category and state the reasons for it		
HRMS.REQ.017	Attendance & Leave Management	System should have ability to Check the status of leave request		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.018	Attendance & Leave Management	System should have ability to approve or cancel or modify leave requests by staff		
HRMS.REQ.019	Attendance & Leave Management	System should have ability to view accrued leave balances		
HRMS.REQ.020	Attendance & Leave Management	System should have ability to intimate the officer concerned when a staff member goes on unauthorized leave (unmarked attendance) or returns back from unauthorized leave or extends leave or reports in the middle of the sanctioned leave period (along with appropriate reduction in sanction)		
HRMS.REQ.021	Attendance & Leave Management	System should have ability to provide the following reports to authorised persons on attendance and leave details:		
HRMS.REQ.022		1) consolidated status of present or absent staff members working under him or her		
HRMS.REQ.023		2) number of staff members for whom leave has not been approved or declined or modified		
HRMS.REQ.024		3) number of staff members attending office late		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.025		4) total number of leave quota (category-wise) and actual leaves taken in a period by a staff member		
HRMS.REQ.026	Attendance & Leave Management	System should have ability to manage on-line application, tracking and approval of various kinds of leave through workflow logic and self-service		
HRMS.REQ.027	Attendance & Leave Management	System should have ability to update work schedule or shift pattern of staff		
HRMS.REQ.028	Attendance & Leave Management	System should have ability to maintain working hours, weekly offs and national or local holidays		
HRMS.REQ.029	Attendance & Leave Management	System should have ability to define overtime facility		
HRMS.REQ.030	Attendance & Leave Management	System should have ability to define leave quota for staff		
HRMS.REQ.031	Attendance & Leave Management	System should have ability to manually update attendance & leave details of staff in case for a staff member to whom access card is not applicable		
HRMS.REQ.032	Attendance & Leave Management	System should have ability to correct attendance & leave details of staff		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.033	Attendance & Leave Management	System should have ability to update half day attendances or leaves in the system		
HRMS.REQ.034	Attendance & Leave Management	It should facilitate leave balances to be merged or transferred or credited through an accrual process in the system automatically based on user defined criteria		
HRMS.REQ.035	Attendance & Leave Management	System should have ability of record keeping and maintenance of historical data		
HRMS.REQ.036	Travel and Transport	It should have ability to automate Travel process		
HRMS.REQ.037	Travel and Transport	It should have ability to record Travel Policy & Procedure		
HRMS.REQ.038	Travel and Transport	It should have ability to generate itinerary details		
HRMS.REQ.039	Travel and Transport	It should have ability to record the travel with unique number and update about cancelled, approved, or deferred		
HRMS.REQ.040	Travel and Transport	It should have ability to request travel by staff and approve or reject transfer requests of staff (Integrate with SSS Module)		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.041	Travel and Transport	It should have ability to generate lists of travel requests or recommendations received to be reviewed by the Competent Authority for deciding on travels		
HRMS.REQ.042	Travel and Transport	It should have ability to produce itinerary, travel request, routes details		
HRMS.REQ.043	Rewards	HRMS will have all details of rewards and recognition received by staff would be available online		
HRMS.REQ.044	Rewards	Rewards and recognition will be provided based on recommendation and will be recorded online		
HRMS.REQ.045	Rewards	Reward list, nominees will be part of HRMS		
HRMS.REQ.046	Rewards	It should provide and generate rewards policy		
HRMS.REQ.047	Rewards	It should provide recognition rules, terms and conditions, applicability		
HRMS.REQ.048	Rewards	It should have all rewards cycle, emoluments involved if any enlisted		
HRMS.REQ.049	Appraisal	This appraisal will be for outsourced staff members. It should have ability to fill appraisal documents in the system during		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		each stage of appraisal and integrate with SSS		
HRMS.REQ.050	Appraisal	It should have ability to view appraisal documents, provide rating and feedback		
HRMS.REQ.051	Appraisal	It should provide the functionality to review to request changes within a specified time after submission of appraisal document post approval from competent authority		
HRMS.REQ.052	Appraisal	It should have the ability to capture agreement on final rating of both the reviewed and reviewer.		
HRMS.REQ.053	Appraisal	Ability to maintain Audit trial of all changes made to this process		
HRMS.REQ.054	Training	It should have ability to capture Training needs of various classes of staff		
HRMS.REQ.055	Training	It should have ability to capture Training needs of staff met or not met during the quarter or year		
HRMS.REQ.056	Training	It should have ability to formulate and update Annual Training Calendar with list of Training Programmes, Batch size, target group etc.		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.057	Training	It should have ability to provide input for payment to Trainers or Institutes		
HRMS.REQ.058	Training	It should have ability to update list of Trainers or Institutes for various training programmes		
HRMS.REQ.059	Training	It should have ability to record participant's attendance in training programmes and staff members nominated but did not attend a training programme		
HRMS.REQ.060	Training	It should have ability to notify supervisors of staff members about the nomination for training programme		
HRMS.REQ.061	Training	It should have ability to define and print training nomination letters to be sent to staff for invitation		
HRMS.REQ.062	Training	It should have ability to customize training feedback form and training nomination letters		
HRMS.REQ.063	Training	It should have ability to define training feedback & effectiveness form		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.064	Training	It should have ability to manually update training feedback provided by participants in the online feedback form		
HRMS.REQ.065	Training	It should have ability to analyse training feedback		
HRMS.REQ.066	Training	It should have ability to capture Training facilities available within the organization		
HRMS.REQ.067	Training	It should have ability to book training rooms by departments for specific training programmes		
HRMS.REQ.068	Training	It should have ability to capture course content of all training programmes along with list of Target group, batch size		
HRMS.REQ.069	Training	It must have functionality for online registration, cancellation, rescheduling, reminder, and confirmation of training classes		
HRMS.REQ.070	Training	For any request raised with regards to registration, cancellation, rescheduling, it should provide the functionality to approve or reject the request by competent authority		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.071	Training	It should have ability to maintain training database with full training history of entire staff		
HRMS.REQ.072	Violation	HRMS will have ITECCS violation policies and guidelines for Police department and outsourced staff members		
HRMS.REQ.073	Violation	HRMS should enable appropriate authorised persons to log in and register any act of violation against a staff member as per the agreed rules and policy		
HRMS.REQ.074	Violation	It should have the ability to approve or reject the above by competent authority		
HRMS.REQ.075	Violation	Module should include details of number of violations allowed as per role		
HRMS.REQ.076	Violation	Type of violations should be listed		
HRMS.REQ.077	Violation	It should have the ability to auto send email to respective role's supervisor, if he or she crosses the threshold limit		
HRMS.REQ.078	Violation	If the number of violations allowed are exceeded, it should have the ability to mention next steps to be taken both by the defaulter and immediate supervisor		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.079	Violation	It should have the ability to cancel, change number of violations captured after due approval from competent authority		
HRMS.REQ.080	Violation	It should have the ability to grant access to this information to only a select few		
HRMS.REQ.081	Staff Master	Ability to store and maintain staff's personal data such as staff members no., name, addresses, phone numbers, emergency contact information and email addresses, Salary Bank Account Details, passport details		
HRMS.REQ.082	Staff Master	Ability to maintain staff's gender, date of birth, blood group, citizenship, marital status, religion, caste etc.		
HRMS.REQ.083	Staff Master	Ability to maintain a staff's education, certifications, degrees, and any endorsements		
HRMS.REQ.084	Staff Master	Ability to maintain previous (multiple) employment details like name of the organization, department, position held (designation), start or end dates, reason for leaving, last salary drawn, references etc.		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.085	Staff Master	Ability to maintain names, date of birth and contact details of spouse, children, dependents, parents, dependants, nominees under different schemes, etc.		
HRMS.REQ.086	Staff Master	Ability to maintain staff's recruitment category like physically handicapped or sportsperson or ex-servicemen or specialist or SC or ST or OBC or compassionate grounds or Others		
HRMS.REQ.087	Staff Master	Ability to update staff member's recent photograph		
HRMS.REQ.088	Staff Master	Ability to maintain the dialect and languages known with details of speak, read and write separately. Clear indication for the mother tongue		
HRMS.REQ.089	Staff Master	Ability to maintain history of trainings attended (prior to joining & after joining) like name of the course, name of the Institution, month & year of training, duration of the course in days or weeks etc.		
HRMS.REQ.090	Staff Master	Ability to maintain the awards for which nominated or received by a staff including the name of the award, year of award, in		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		which discipline or field and date of receipt of award and special status or privilege, if any, to be given to him for the award		
HRMS.REQ.091	Staff Master	Ability to maintain date of joining, probation period, date of confirmation in each grade or post		
HRMS.REQ.092	Staff Master	Ability to date and time stamp all changes in the database enabling data availability on 'as on date or time' basis		
HRMS.REQ.093	Staff Master	Flexibility of additionally capturing any information relating to staff member at a later date		
HRMS.REQ.094	Staff Master	Ability to maintain concurrent jobs for staff with additional responsibilities or special duties in addition to regular responsibilities		
HRMS.REQ.095	Staff Master	Ability to update only authenticated data reflected in the staff's master		
HRMS.REQ.096	Staff Master	Ability to maintain staff's data with regards to claims, etc.		
HRMS.REQ.097	Staff Master	Ability to maintain and view staff leave details		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.098	Staff Master	Ability to maintain staff's data with respect to PF, Gratuity, etc. and the nominations for the same		
HRMS.REQ.099	Staff Master	Ability to create organizational chart of all positions and reporting relationships		
HRMS.REQ.100	Staff Master	Ability to provide restricted access to different classes of staff master data		
HRMS.REQ.101	Staff Master	Ability to maintain the insurance related details for each staff member, like insurance number, nominee details, amount etc.		
HRMS.REQ.102	Staff Master	Ability to maintain Audit trial of all changes made to sensitive information		
HRMS.REQ.103	Staff Master	Ability to maintain service files documents in scanned form including Proof of Date of Birth, domicile, Bonds, if any, executed, disciplinary cases details, photograph etc.		
HRMS.REQ.104	Staff Master	Ability to send alerts to appropriate authorised persons when driving license expires or violation is logged in against a staff member or on any other related issue		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.105	Staff Master	Ability to track the physical location of the service file by recording the unique file number and place where it is kept (After HRMS no physical file movement may be required)		
HRMS.REQ.106	Staff Self Service (SSS)	It will facilitate staff to apply for changes in permanent & correspondence addresses, details of family members, emergency contact details, contact details, office location, nomination for various schemes like PF or Gratuity, etc.		
HRMS.REQ.107	Staff Self Service (SSS)	HRMS should be able to add or update bank information for expense reimbursement, PAN no, passport details, driving license no. or any other relevant information		
HRMS.REQ.108	Staff Self Service (SSS)	HRMS should be able to provide address proof letter to UP112 for various purposes		
HRMS.REQ.109	Staff Self Service (SSS)	HRMS should be able to integrate SSS with Employee Master		
HRMS.REQ.110	Staff Self Service (SSS)	HRMS should be able to remind the staff through self-service or e-mail regarding		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		modification or requirement of additional data		
HRMS.REQ.111	Staff Self Service (SSS)	HRMS should be able to send the staff confirmations after changes are made online		
HRMS.REQ.112	Grievance Redressal and Suggestion System	HRMS will have ITECCS grievance related policies and guidelines for Police department and outsourced staff members		
HRMS.REQ.113	Grievance Redressal and Suggestion System	HRMS will facilitate to list various techniques to facilitate communication		
HRMS.REQ.114	Grievance Redressal and Suggestion System	HRMS will facilitate to issue docket number for different classes of staff members separately		
HRMS.REQ.115	Grievance Redressal and Suggestion System	It should have the ability to define type of grievance or suggestion		
HRMS.REQ.116	Grievance Redressal and Suggestion System	The users should the ability to log in complaints or suggestions		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.117	Grievance Redressal and Suggestion System	Ability to check status of the grievance or suggestion logged		
HRMS.REQ.118	Grievance Redressal and Suggestion System	It should have the functionality to restrict access to a select few and maintain confidentiality of information		
HRMS.REQ.119	Grievance Redressal and Suggestion System	It should have the ability to withdraw or change complaint or suggestion within a specified time		
HRMS.REQ.120	Grievance Redressal and Suggestion System	If the grievance or suggestion is not responded to within a specified time, it should have the ability to auto send email to higher authority for escalation		
HRMS.REQ.121	Grievance Redressal and Suggestion System	Ability to maintain Audit trial of all changes made to this information		
HRMS.REQ.122	Policy Rules and automation	The proposed solution should have an intuitive business rules definition framework that would enable business users to manage business policies easily with less or no intervention from technical staff.		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.123	Policy Rules and automation	The business rules framework should be able to model the complex business logic in a natural language format		
HRMS.REQ.124	Policy Rules and automation	Business users should be able to test the logic integrated with the underlying architecture as well independently.		
HRMS.REQ.125	Policy Rules and automation	Solution shall be linked to SMS gateway as per requirement for Payroll mechanism, grievance etc.		
HRMS.REQ.126	Transfer, Promotion and Suspension	HRMS will have all transfer, promotion or suspension related policies and respective guidelines of outsourced staff present in this module		
HRMS.REQ.127	Transfer, Promotion and Suspension	It should have the ability to raise request for outsourced staff member's transfer, promotion or suspension using a detailed form or defined framework only for specified persons		
HRMS.REQ.128	Transfer, Promotion and Suspension	Any request raised for transfer, promotion, or suspension to be reviewed and approved or rejected by competent authority		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.129	Transfer, Promotion and Suspension	Should provide an escalation or appeal mechanism for the requestor in case request is rejected		
HRMS.REQ.130	Transfer, Promotion and Suspension	It should have the functionality to restrict access to a select few and maintain confidentiality of information		
HRMS.REQ.131	PRV attendance	HRMS shall be accessible to PRV Staff and attendance system PRV shall be integrated with HRMS. Registration of Field/PRV Staff shall be available at DCR level		
HRMS.REQ.132	e-learning	HRMS shall be integrated with e-learning to keep track of learning, training attended, training required by UP112 officials		
HRMS.REQ.133	CAD Solution	HRMS shall be integrated with CAD Solution to keep track of staff accessing the CAD application		
HRMS.REQ.134	MDT Integration	Integration with MDT's application shall be available. HRMS facility to be available on MDT platform for PRV staff attendance		

HRMS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
HRMS.REQ.135	CAD mobile solution integration	HRMS facility to be integrated available on CAD mobile application		
HRMS.REQ.136	Geo coordinates	HRMS shall be able to capture location/ coordinates at the time of capturing attendance		
HRMS.REQ.137	General Requirement	For leave approval notifications, SMS facility shall be available		
HRMS.REQ.138	Biometric attendance system integration	Centralized monitoring of the DCR staff through integration with biometric attendance system		
HRMS.REQ.139	Facial attendance system integration	HRMS to be developed for Facial based attendance solution installed on MDT for attendance of PRV staff		

D. Maps and Location Identification

1. Geographical Information System (GIS)

Geographical Information System (GIS)				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
GIS.REQ.001 A	Solution Overview	MSI shall design Geographic Information System (GIS Software) to store, retrieve, manage, display, and analyse all types of geographic and spatial data.		
GIS.REQ.002 A	Solution Overview	MSI has to provide online and offline maps of the required area at contact center, OMC, DCRs and PRVs.		
GIS.REQ.003 A	Solution Overview	Provided maps shall be integrated with CAD system to give unified picture.		
GIS.REQ.001	General Requirement	The GIS application will render the distress citizen location or Vehicle location and identify the GIS location with GIS map and GIS map data and will send to the RMO/ ES desktop and to MDT device		
GIS.REQ.002	General Requirement	MSI shall provide the key components which would be involved to implement GIS functionality such as GIS map, GIS map data and GIS Server, Geo fencing tools etc		

Geographical Information System (GIS)				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
GIS.REQ.003	General Requirement	GIS map is a base layer on which GIS map data should be rendered at CAD application and MDT devices in Hindi and English languages.		
GIS.REQ.004	General Requirement	MSI shall provide the GIS Engine which will be centrally located and fetch data from GIS data based on latitude and – longitude received and renders on base map for viewing		
GIS.REQ.005	General Requirement	The use of GIS should strictly adhere to the End User License. Specifically, the Intellectual Property Rights (IPR) for the Map Image should be as per End User License		
GIS.REQ.006	General Requirement	The GIS POI which is collated through MDT devices and GIS Data collection mobile application shall be added on incremental basis at centralized GIS data. An application that enables incorporation of GIS Point of interest (POI) captured through an MDT device in field and passed on to NOC into centralized GIS. This feature should enable capture and		

Geographical Information System (GIS)				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		incorporation of ground features resulting in real-time updation of GIS data, thereby making it current at all times.		
GIS.REQ.007	General Requirement	MSI to consider 6000 sq. km as city area for 1:1000 mapping and rest can be considered as rural area. The positional accuracy of + or- 10 m for 1:1000 maps and accuracy of + or- 50m for 1:5000 maps.		
GIS.REQ.008	General Requirement	The GIS map required should be compatible and must support ELS/AVLS and Vehicle Navigation System with routing and driving directions calculation. GIS Map Shall also have AI/ML feature that improves the route suggestion based on the shortest time taken by analysing shortest past and current traffic situation. Recommendation of routes shall not be based on arial distance between PRV and event location rather it shall be based on motorable routes		

Geographical Information System (GIS)				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
GIS.REQ.009	General Requirement	GIS map for CAD and Navigation on MDT and handheld should support for visual and, voice (preferably) based turn by turn direction and visual should support English and Hindi.		
GIS.REQ.010	General Requirement	Navigation on MDT should display current locations, target place, feature to save routes, time to go, expected time of arrival and distance to go		
GIS.REQ.011	General Requirement	GIS map should be locally hosted at police premises and should have features to update the attribute and police level information		
GIS.REQ.012	General Requirement	GIS map should work for Security planning and Traffic management		
GIS.REQ.013	General Requirement	Application should work on mobile platform (iOS/Windows/Android) in the		

Geographical Information System (GIS)				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		similar functionality as that of the web platform		
GIS.REQ.014	General Requirement	**In order to support routing, the GIS map should be provided in navigation format with specifications as follows:** a) Road network should be segmented in a manner that it has unique junction nodes and can supports routing algorithm to navigate and calculate distance to each individual location. b) Solution has to ensure that the GIS maps have the following essential map features: • Drag and Pan • Zoom • Find and zoom to position • Cartographic attributes • Search a specific vehicle on the map		

Geographical Information System (GIS)				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		• Dynamically Turn on or Off map layers c) It should be integrated with Location based system (LBS) to render the location of the citizen on the GIS maps d) It should have all interest points of internal security scheme of districts on the GIS Maps e) Roads should be classified properly on the basis of usage, average speed, road conditions, connectivity etc. so that priority of each road segment is properly set f) MSI shall provide census information and shall map up to the village level and above as published by the registrar general and census department of India. It should be mapped up to the geo entities for village, tehsil and higher up to the state level. g) Road network should be		

Geographical Information System (GIS)				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		segmented at - • Every intersection of two or more roads • Every Administrative boundary levels • Where Rail Track intersects with any road objects • Every road segment having a corresponding start and end junction longitude and latitude to create the whole routable road network. Further every segment shall be attributed with a unique identifier; name, if it exists and its length h) Road network continuity shall be maintained to enable navigation or routing. i) Administrative layers shall represent parent-child relationship. For example, each record in locality layer shall have a parent defined as city name. This shall		

Geographical Information System (GIS)				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		apply to all administrative layer GIS map should support application to find Nearby Points of Interest		
GIS.REQ.015	General Requirement	All locations should be available as Point data/ point layer Below is the list of Layers A. Administrative • City boundaries • District layers • Locality boundaries • Village boundaries • Important Buildings(Gov. or Private)/Monuments/Crossings /Roads/Streets etc. would be part of NexGen UP112 • Boundary or Area of Police Station and Commissionerate (Zoning – area of responsibility of hierarchical police		

Geographical Information System (GIS)				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		formations/headquarters with geographical boundaries). • Boundaries or Area of Fire Stations • Jurisdiction limits • Police Zonal and police range, district range, area, circle, Police station and village level classification • Ward boundaries B. Transportation • Road network with specifications • Rail network • Highway Network C. Landmarks • Police Head Quarters, Police stations, Police Chowkis and other Police installations • All Govt. offices or Institution etc. • All major landmarks of the city D. Land Use		

Geographical Information System (GIS)				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		• Water bodies • Green areas		
GIS.REQ.016	Layers	Details of layer with name and symbol shall be provided by MSI as per section 9 annexure 27 and 28		
GIS.REQ.017	General Requirement	MSI shall provide the minimum number of POI for each district of UP state as described as per as per section 9 annexure 27 and 28, current POI is around 18 lac and MSI need to upgrade to approx. 50 lac and cost should be added in GIS map and Map data component under costing format.		

2. GIS Data Capturing Mobile Application

GIS data capturing Mobile Application				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
GISMA.REQ.001	General Requirement	MSI has to provide the GIS Data collection mobile application which shall be used to collect the field location data of different areas in the UP state. These data would be used as a point of interest (POI) in the GIS solution		
GISMA.REQ.002	General Requirement	There will be an incremental POI growth in the system which should be added in the central GIS data in DC and DRC		
GISMA.REQ.003	General Requirement	This application will be installed in the mobile devices and shall be provided to the field officer where officer will capture the data at field level like location address, near landmark detail etc. and store the data in the application		

GIS data capturing Mobile Application				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
GISMA.REQ.004	General Requirement	Once the data is stored, the officer will then push the data to the DC and DRC GIS database through the mobile application.		

3. GIS Map Geo-Fencing Application

GIS Map Geo- Fencing Application				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
GISGFA.REQ.001	General Requirement	MSI shall provide the Geo-fencing application which will be used to create the boundary of the UP-state areas including Police boundaries up to Police stations level, cities, districts, village level etc.		
GISGFA.REQ.002	General Requirement	MSI shall create the geo fencing for police station on GIS vector maps of police stations which will comprise the villages, jurisdictions, and other areas		
GISGFA.REQ.003	General Requirement	This will be enriched for more than 50 layers. This will help the user to understand the current area and location of the vehicle and distress caller in the system		
GISGFA.REQ.004	General Requirement	Creating the Geo fencing shall be user friendly, and this should have draw or drag and drop feature for drawing geo fence		

GISGFA.REQ.005	UI based	Drag and drop feature shall be available for drawing the Geo Fence and deciding patrol charts.		
GISGFA.REQ.006	UI based	In case PRV travels beyond the area defined, alert shall get generated on CAD system and PRV staff shall provide proper justification for this violation to RoIP or Event Supervisor		
GISGFA.REQ.007	Recommendation	Geo fencing based suggestions of nearest PRV should be available in CAD		

4. Location Based Service (LBS)

Location Based Service (LBS)				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
LBS.REQ.001	Call Location Detection	System should be capable to detect the location of the caller through subscriber detail record (SDR) database and call detail record (CDR).MSI shall create the database for SDR and CDR details also.		
LBS.REQ.002	IOT location	User will register on UP112 portal with their IoT device information. If any case comes into CAD through registered devices. System should be capable to		

Location Based Service (LBS)				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		capture the latitude & longitude coordinates from registered devices (which are connected to the internet) and detect the location of the user.		
LBS.REQ.003	Mobile Apps	System should be capable to receive the latitude & longitude coordinates and detect the location of the user and should be able to integrate with CAD to send the location.		
LBS.REQ.004	SMS	System should be capable to receive the SMS with mobile number and text message. It should detect the location of the sender based on SDR and CDR database		
LBS.REQ.005	General Requirement	MSI has to provide the location-based service solution to the NexGen UP112. This solution shall be implemented for all cities of UP		
LBS.REQ.006	General Requirement	Location of the distressed caller should be made available to the Control Room for distressed callers who are using landline as well as mobile phones, irrespective of whether the distressed caller is carrying a		

Location Based Service (LBS)				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		basic or feature phone or a smartphone. Data connectivity and mobile based applications should not be required for this purpose		
LBS.REQ.007	General Requirement	The distressed caller may call or send a SMS, in either case, location of the caller needs to be tracked and made available to the Control Room		
LBS.REQ.008	General Requirement	The location of the distressed caller should be tracked and made available to the Control Room during the course of the emergency (i.e., not just the location when call was initiated, but the location at any point during the entire emergency period). The detection of the caller location should be identified with in 10-15 sec in the system. Refresh time interval of location should be within 10-15 sec.		
LBS.REQ.009	General Requirement	A centralized Location Gateway should be set up for this purpose		

Location Based Service (LBS)				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
LBS.REQ.010	General Requirement	Location Gateway should be hosted at a State-owned DC or cloud DRC		
LBS.REQ.011	General Requirement	Location information should be made available to UP 112 and OMC over industry standard APIs using a secured network connection		
LBS.REQ.012	General Requirement	Location Gateway should have necessary authentication, authorization, and accounting (AAA) controls to avoid unauthorized access or misuse of location information		
LBS.REQ.013	General Requirement	Location Gateway should be able to integrate with Telecom Operator’s GMLC or HLR database for Emergency Response Services		

Location Based Service (LBS)				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
LBS.REQ.014	General Requirement	In case the Telecom Operator does not have LBS infrastructure or does not have the requisite capacity in its LBS infrastructure, then the Location Gateway should act as a hosted GMLC and should be able to directly talk to Telecom Operator's HLR or MSC to obtain caller location information. This would reduce Government's dependency on Telecom Operators having LBS infrastructure or exposing the same for emergency purpose		
LBS.REQ.015	General Requirement	Location Gateway should integrate with all the Telecom Operators operating in State of Uttar Pradesh		
LBS.REQ.016	General Requirement	Location Gateway must integrate with Mobile Network Portability (MNP) service provider to identify the caller's Telecom Operator		

Location Based Service (LBS)				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
LBS.REQ.017	General Requirement	On one end, the Location Gateway should be able to integrate with network elements of multiple telecom operators, while on the other end it should be able to on board or service or provide location information to UP 112 and OMC		
LBS.REQ.018	General Requirement	Location Gateway should identify the type of subscriber (mobile or fixed line or SMS) and use this information to query the Mobile Telecom Operator or Fixed line subscriber database accordingly		
LBS.REQ.019	General Requirement	The Location Gateway should also possess a fixed-line caller information service or database at the backend, so that when the caller number is identified as a fixed-line caller, then its location can be derived from the said service or database		

Location Based Service (LBS)				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
LBS.REQ.020	General Requirement	To ensure privacy of citizens, location information should only be shared for emergency calls. Control Room staff should not be able to view location of any mobile number entered through CAD or other application		
LBS.REQ.021	General Requirement	The detection of the caller location should be identified with in 10-15 sec in the system.		

5. Emergency/Advanced Location Services (ELS/ALS)

Emergency/Advanced Location Services (ELS/ALS)				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**

ELS.REQ.001	General Requirement	Advanced Mobile Location (AML) shall be leveraged to identify location of callers calling through smart phones (Android/iOS). The location shall derive from the location data of the phone (GNSS, Wi-Fi)		
ELS.REQ.002	General Requirement	For Google, AML (ELS) shall be supported for all android/iOS devices		
ELS.REQ.003	General Requirement	This system shall be used to identify location of victims who have communicated over WhatsApp or SMS. It will help increase the reach without over-burdening the system		
ELS.REQ.004	General Requirement	MSI shall provide satellite-based location tracking of PRVs which are in those areas where telecom network connectivity is either very poor or no connectivity. Satellite based tracking shall be done using GPS device that will be placed on the PRVs which will continuously provide the location of the vehicle without depending on the telecom operators		

6. Vehicle Tracking System

Vehicle Tracking System				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
VTS.REQ.001A	Solution Overview	A vehicle tracking system combines the use of automatic vehicle location in individual vehicles with software that collects these fleet data for a comprehensive picture of PRVs locations and movements.		
VTS.REQ.002A	Solution Overview	VTS shall be integrated part of CAD system and GPS devices fitted inside the PRVs		
VTS.REQ.003A	Solution Overview	VTS shall have a refresh rate of 5 seconds in order to display movement of a PRV		
VTS.REQ.001	General Requirement	GPS based tracking system shall provide tracking your vehicle and location anywhere and at anytime		
VTS.REQ.002	General Requirement	It shall provide real-time status updates of the fleets. Timely alerts and notifications to the UP112 to make informed decisions. Intuitive Dashboard		

VTS.REQ.003	General Requirement	Some of features required by Vehicle tracking system- • End-to-End platform for fleet tracking, trip/schedule planning, health monitoring, maintenance, and management. • GPS enable real-time tracking on all the fleets. • Alerts and Monitoring on metrics such as speed, location, trip history, driver behaviour analysis, idling time etc. • Maintenance activity logs like service scheduling, issue status and billing model with payment details. • Reports and Analytics that assist in taking better business decisions. • Capturing real-time health diagnostics through OBD devices. • Digital logging for all the transactional data for error-free data entry.		

7. PRV Location Tracking by Citizen

Sr. No.		Minimum Requirement Description		Deviation

	Nature of Requirement		Compliance (Yes or No)	
LTC.REQ.001A	Solution Overview	Citizen shall be able to track movement of PRV assigned to cater event reported by them.		
LTC.REQ.002A	Solution Overview	PRV location tracking facility shall be available to citizens of UP state of respective event.		
LTC.REQ.003A	Solution Overview	It shall be like the cab aggregator application available in the market like Ola, Uber etc. on web platform		
LTC.REQ.001	General Requirement	CAD system shall send the SMS as soon as PRV dispatch to the Event location		
LTC.REQ.002	General Requirement	SMS content should include the link for PRV tracking which is heading to the distress caller		
LTC.REQ.003	General Requirement	After redirecting to the PRV tracking page user should be able to see the live location of the PRV heading to the distress caller along with the location of the incident on map		
LTC.REQ.004	General Requirement	User should be able to see Expected time of Arrival (ETA) along with the following route by PRV on map		
LTC.REQ.005	General Requirement	After click on PRV icon map, user should get the PRV details like as PRV contact		

		Number, Vehicle Registration Number, PRV id, etc.		
LTC.REQ.006	General Requirement	User can make call to the PRV by click on PRV contact Number and there should be a provision to send a text message to the PRV as well		
LTC.REQ.007	General Requirement	After click on Event icon on map user should get the Event info like as Event type, event subtype, etc.		
LTC.REQ.008	General Requirement	This shall also have feature of activation or deactivation the tracking on need basis e.g., if UP112 wants this feature only of Women or old people then MSI shall have option of activating it for required user and disabling for other Citizens		

E. Others

1. Document Management System

Document Management System				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
DMS.REQ.001A	Solution Overview	DMS should have functionality to manage all the relevant documents with updated version and categorization of the documents		
DMS.REQ.002A	Solution Overview	DMS should have a provision to detect the user roles and permission and show the relevant functionality to the user as per requirement		
DMS.REQ.003A	Solution Overview	DMS should have an administrator console to manage all the documents, user, and other features of the portal		
DMS.REQ.001	General Requirements	The solution should support enterprise class RDBMS such as MS SQL Server, Oracle, DB2, etc.		
DMS.REQ.002	General Requirements	The Solution should be multi-tier, web-based solution (having web-based front-end for users and as well as for system administrative functions) having centralized database, web, and application server with support for clustering.		
DMS.REQ.003	General Requirements	The solution shall support versioning of documents with facility to write version comments		
DMS.REQ.004	General Requirements	The solution shall allow locking of documents for editing and importing it back into the system		
DMS.REQ.005	General Requirements	Repository should be format agnostic		

Document Management System				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
DMS.REQ.006	General Requirements	The solution should support configuration of approval processes. While processing a file, all the data and images for each transaction should be displayed to processing users and competent authority should be allowed to accept, reject, or send the files for review		
DMS.REQ.007	General Requirements	The solution should manage lifecycle of documents through record retention, storage, and retrieval policies.		
DMS.REQ.008	General Requirements	The Solution should support managing and tracking of physical location of documents		
DMS.REQ.009	General Requirements	The solution shall support page by page view for multi-page document.		
DMS.REQ.010	General Requirements	The solution shall facilitate zoom-in or zoom-out feature. The user shall be able to customize the zoom and pan feature along with other image operations like Invert, rotate etc.		
DMS.REQ.011	General Requirements	The solution should support archival & view of PDF or A format documents (open ISO standard for long term archival of documents)		
DMS.REQ.012	General Requirements	The solution shall support for viewing documents in native application.		

Document Management System				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
DMS.REQ.013	General Requirements	The solution shall provide facility of putting text, graphic and image annotations on scanned document pages.		
DMS.REQ.014	General Requirements	The solution shall support comprehensive annotation features on images like highlighting, marking text, underlining putting sticky notes on documents, and support for text and image stamps etc.		
DMS.REQ.015	General Requirements	The solution shall support automatic stamping of annotations with username, date, and time of putting annotations.		
DMS.REQ.016	General Requirements	The solution shall store annotations as separate file and at no time, the original image shall be changed. The system shall provide facility of taking print outs with or without annotations		
DMS.REQ.017	General Requirements	The solution shall provide facility to index folders, files, and documents on user-defined indexes like department, ministry, file number, year etc.		
DMS.REQ.018	General Requirements	The solution shall facilitate manual and automatic indexing using OCR functionality or from other applications		

Document Management System				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
DMS.REQ.019	General Requirements	The solution should support automatic full text indexing for textual search		
DMS.REQ.020	General Requirements	The solution shall support saving of search queries and search results		
DMS.REQ.021	General Requirements	The solution shall support search for documents or folders on document or folder on profile information such as name, created, modified, or accessed times, keywords, owner etc.		
DMS.REQ.022	General Requirements	The solution shall support definition of Users, Groups and Roles relation in the system along with multiple levels of access rights (Delete or Edit or View or Print or Copy or Download).		
DMS.REQ.023	General Requirements	The solution shall provide LDAP support for integrating with directory services and shall support single sign on		
DMS.REQ.024	General Requirements	The solution shall support audit-trails with username and date and time stamp for every activity		
DMS.REQ.025	General Requirements	The solution shall support integration with database-based authentication.		
DMS.REQ.026	General Requirements	The solution shall support integration with PKI infrastructure for enhanced security.		

Document Management System				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
DMS.REQ.027	General Requirements	The solution shall support web-based administration module for the complete management of system.		
DMS.REQ.028	General Requirements	It should be based on open standards and have API support for data import & export.		
DMS.REQ.029	General Requirements	The System shall support integration with Email Servers.		
DMS.REQ.030	General Requirements	The System shall provide fully functional APIs for Integration with external application		

2. Directory Services

Directory Services				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
DS.REQ.001A	System Overview	Directory services should have a provision to create, update and modify the LDAP directory		

Directory Services				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
DS.REQ.002A	System Overview	It should have a provision to integrate with the Identity and access management		
DS.REQ.003A	System Overview	It should be used to define the roles and permission of different kind of users in the system		
DS.REQ.004A	System Overview	Directory services should have proper integrations with DNS, DHCP. Email and other infrastructure components and service		
DS.REQ.001	General Requirement	Support for LDAP-based mechanism for storing and accessing identity data and should be provided in high availability to avoid any single point of failure		
DS.REQ.002	General Requirement	Console or Web Based interface to navigate or update LDAP identity data		
DS.REQ.003	General Requirement	Support for addition of custom logics into LDAP operation processing		
DS.REQ.004	General Requirement	Support to integrate with identity and access management as per proposed solution		
DS.REQ.005	General Requirement	Should support directory virtualization		
DS.REQ.006	General Requirement	Support for configuration changes using GUI		

Directory Services				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
DS.REQ.007	Synchronization	Support for data synchronization with third party identity stores (Active directory etc.)		
DS.REQ.008	Standards	Adherence to LDAP Standards like RFC 2696, RFC 3671 etc.		
DS.REQ.009	Failover mechanism	Support for server failover and failback		
DS.REQ.010	Security	Support for protection against any kind so external threat		
DS.REQ.011	Security	Support for SSL digital certificate for secure encrypted communication between LDAP client and server		
DS.REQ.012	Scalability	Support for high scalability into the largest environment		

3. E-Learning

E-Learning				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**

EL.REQ.001A	System Overview	MSI is required to manage the eLearning module for administration, tracking, reporting and delivery of learning courses or training programs. UP112 may use the module to manage any other training program beyond what MSI is providing. The objective is to upgrade e-learning module and audio-visual learnings.		
EL.REQ.002A	System Overview	The module shall be available to be used by UP112 resources to access learning content and to create, deliver, monitor participation, and assess attendees/ trainees' performance.		
EL.REQ.003A	System Overview	For the police personnel on the field, the MSI shall design an e-Learning module that can be accessed through the MDT devices installed in their vehicles.		
EL.REQ.004A	System Overview	MSI should ensure that the e-Learning modules are not limited to Technical aspects of the solution but should also include the SOPs as defined by UP112.		
EL.REQ.005A	System Overview	In order to track the effectiveness of training programmers, MSI should also provide an online catalogue of e-Learning modules and allow for Training and Competency Assessment through online tests.		
EL.REQ.006A	System Overview	Some of the key features envisaged have been listed below: 1. Ease of use 2. Integration 3. Content management 4. Testing and assessment capabilities 5. Reporting and tracking		

EL.REQ.007A	System Overview	The module shall ensure that for each of the learner groups identified, the system shall enable the user to define the learning path and allow for mandatory trainings along with schedules to complete these trainings.		
EL.REQ.008A	System Overview	Also, the system should allow to track the performance of the trainee before and after training, helping in analysing the impact analysis of the training.		
EL.REQ.001	General Requirement	The officer should be able to access their assigned eLearning courses in the browser-based interface that they use to manage schedules and request time off from their systems. They have to log in and open a new application window for training session.		
EL.REQ.002	General Requirement	Quality monitoring evaluation data shall be used to assign targeted learning.		
EL.REQ.003	General Requirement	E-learning software should be able to schedule the training based on skill assessment of the Officers		
EL.REQ.004	General Requirement	E-Learning software should allow access for scheduled training assignments while listening to a recorded interaction.		
EL.REQ.005	General Requirement	Integrated Scorecard should be able to aid in automatic lesson assignments when a KPI falls below an excepted goal		

EL.REQ.006	General Requirement	The software should provide a provision where training clips can be developed based on best practice calls. The recorded interactions should be used to rapidly build learning content with assessment information.		
EL.REQ.007	General Requirement	The E-Learning software should support remote access.		
EL.REQ.008	General Requirement	The E-Learning content development software should allow adding and or recording narration directly into the application without additional software requirement		
EL.REQ.009	General Requirement	The E-Learning content should be in English and Hindi language for the user		
EL.REQ.010	General Requirement	The officer should be able to access their assigned eLearning courses in the browser-based interface that they use to manage schedules and request time off from their systems. They have to log in and open a new application window for training session.		
EL.REQ.011	General Requirement	Quality monitoring evaluation data shall be used to assign targeted learning.		
EL.REQ.012	General Requirement	E-learning software should be able to schedule the training based on skill assessment of the Officers		
EL.REQ.013	General Requirement	E-Learning software should allow access for scheduled training assignments while listening to a recorded interaction.		
EL.REQ.014	General Requirement	Integrated Scorecard should be able to aid in automatic lesson assignments when a KPI falls below an excepted goal		

EL.REQ.015	General Requirement	The software should provide a provision where training clips can be developed based on best practice calls. The recorded interactions should be used to rapidly build learning content with assessment information.		
EL.REQ.016	General Requirement	The E-Learning software should support remote access.		
EL.REQ.017	General Requirement	The E-Learning content development software should allow adding and or recording narration directly into the application without additional software requirement		
EL.REQ.018	General Requirement	The E-Learning content should be in English and Hindi language for the user		
EL.REQ.019	General Requirement	The MSI shall design and provide content for training, in case the content is being provided by UP112, the MSI shall upload the content on the module.		
EL.REQ.020	General Requirement	The content shall be tailor-made, easy, and convenient to use and shall be categorized based on the proficiency level of the user. Should ensure active and effective learning by participants.		
EL.REQ.021	General Requirement	The e-learning levels may be defined (Beginner, Intermediate, Advanced) and identified by the MSI in consultation with UP112.		
EL.REQ.022	General Requirement	The content shall include text, documents, audio, video, simulations etc.		
EL.REQ.023	General Requirement	The system shall record the feedback of trainees for all trainings conducted online or offline and shall provide analysis as per requirements of UP112.		

EL.REQ.024	General Requirement	The system shall mandate users to under-go any trainings without skipping any content as per the requirements and shall also provide soft copy of certificates generated from the system.		
EL.REQ.025	General Requirement	The MSI shall regularly update the content of the courses as per the defined periodicity in consultation with UP112.		
EL.REQ.026	General Requirement	MSI shall create a detailed Dashboard with insights of learning records for each trainee including details like date of completion, assessment score, progress of training course etc. and option to download intelligence reports from the admin account in different formats like .xlsx, pdf, csv etc. The module shall generate regular notifications and alerts to the users reminding them of any trainings which are due or the trainings for which deadlines have already been crossed.		
EL.REQ.027	General Requirement	Auto search functionality for video lectures/training modules.		
EL.REQ.028	General Requirement	Content should have subtitles wherever possible		
EL.REQ.029	General Requirement	Intelligent suggestions based on user history and course content Customisation as per skills and course recommendations		
EL.REQ.030	General Requirement	Recommendations based on the trainings undertaken/signed up for		

EL.REQ.031	General Requirement	Small videos/quick learnings can be built and shared to respective PRVs as a part of training		
EL.REQ.032	General Requirement	Pop up with training summary while hovering over recommended trainings		

4. Chatbot

Chatbot				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
CB.REQ.001	Deployment	Solution should provide conversational chat solution wherein citizens can interact with chat bot for simple enquires to complex form submission services as well.		
CB.REQ.002	General	It should allow citizens to just type their question into the chat window and get an instant response from a virtual digital assistant and even fill up some online forms.		
CB.REQ.003	Enquiry	When citizens enquire cannot be handled by bot application, the same chat can be escalated to Contact/Helpdesk Centre with previous chat history so that citizen enquiry can be handled by live agent		

Chatbot				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		without losing the context of the previously happened conversation.		
CB.REQ.004	Agent Transfer	Citizen can ask for transfer to an agent anytime in the conversation.		
CB.REQ.005	General	In order to start conversation, chatbot shall send an interactive list of options related to different operational areas of application utility like welcome message, how to get started etc.		
CB.REQ.006	Knowledge	Chatbot response shall be based on organizational knowledge base or information retrieved from various Software Solutions, Contact Center etc.		
CB.REQ.007	Integration	Chatbot should be able to Integrate with CAD/ICCC Platform for Automatic Case Creation , Status etc		
CB.REQ.008	Social Media	Chatbot should be able to handle social media channels like Whatsapp , Facebook Messenger etc		
CB.REQ.009	SoS	Emergency/ SoS from Citizen can be captured with the help of chatbot		
CB.REQ.010	Feedback	Feedback from citizens of state shall be automated via use of chatbot		

Chatbot				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
CB.REQ.010	Integration	MSI has to ensure the Chatbot shall be integrated with UPCOP application		

5. SMS Gateway

Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
SMSG.REQ.001	General Requirement	Used for sending SMS of the event to all responders		
SMSG.REQ.002	General Requirement	Need to be integrated with CAD application for sending the messages to defined officials		

6. Video Conferencing

Video Conferencing				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
VC.REQ.001A	Solution Overview	• Video conferencing shall be more comprehending in the next phase of project enabling 78 districts Control room, SP/SSP offices, OMCs, headquarters in Lucknow and PRVs connect via Mobile or MDT on VC through a single software using the existing infrastructure upgrade preferably		
VC.REQ.002A	Solution Overview	• Video conferencing will strengthen district SP/SSPs and commiserates to videoconference with PRVs and with the other units connected on same MPLS network		
VC.REQ.003A	Solution Overview	• New feature like Logged in user in conference can also share the private text message through the software as well		
VC.REQ.004A	Solution Overview	• Additional feature like meeting via other Video Conference service provider such as Google Meet and Teams shall be available		
VC.REQ.005A	Solution Overview	• Auto camera focus feature during VC shall be available		

Video Conferencing				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
VC.REQ.006A	Solution Overview	• Feasibility to have video call with PRV staff either on MDT or on Mobile shall be available		
VC.REQ.001	Video standards	Should support H.263 / H.263+ / H.263++, H.264		
VC.REQ.002	Video Frame Rate	Should be 30 fps and 60fps with 1080p resolution from day one		
VC.REQ.003	Video Features	Ability to send and receive two live simultaneous video sources in a single call, so that the image from the main camera and PC or document camera can be seen simultaneously.		
VC.REQ.004	Video Features	Should support H.239 and BFCP protocols with 1080p resolution		
VC.REQ.005	Video Output	Should have at least 2 no.'s of HDMI / DVI (High-Definition Multimedia Interface) output to connect 2 Nos. Full High-Definition display devices such as plasma / LCD / LED /projectors for both Video and Content.		
VC.REQ.006	Video Input	Should have minimum 2x HDMI Video Inputs to connect at least HD Cameras of 1080p@60fps resolution directly on the codec. The system		

Video Conferencing				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		should be supplied with 1 x 1080p60fps cameras day one.		
VC.REQ.007	Video Input	Should have at least 1 x DVI/HDMI to connect a PC / Laptop with audio input. DVI to VGA converter should be supplied with the unit. The content resolution should be 1080p@30fps		
VC.REQ.008	Audio standards supported	G.711, G.722, G.722.1, 64 kbps MPEG-4 AAC-LD /equivalent standard must be supported.		
VC.REQ.009	Other Desirable features	Noise Reduction, Automatic Gain control, Acoustic Echo Canceller, Active Lip synchronization		
VC.REQ.010	Audio Inputs	Should support minimum 2 Microphone should be supplied day one so that audio from all the participants can be adequately captured.		
VC.REQ.011	Audio Inputs	The system should have required line level inputs or digital line in jack for additional audio source		
VC.REQ.012	Audio Outputs	The system should have required line level outputs or digital line in jack for line out		

Video Conferencing				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
VC.REQ.013	External devices	Should have USB port to connect external devices.		
VC.REQ.014	Network Interfaces	LAN Or Ethernet--10 / 100 /1000Mbps full duplex		
VC.REQ.015	Network Interfaces	Should have support for IPV4 and IPV6		
VC.REQ.016	Bandwidth	IP--at least 6 Mbps		
VC.REQ.017	Inbuilt Multisite Capability	The Video endpoint should have inbuilt minimum 1+8 multisite capability with each site connecting at 1080p resolution.		
VC.REQ.018	Camera Specifications	Minimum 10x optical zoom cameras with 1920x1080p 60 frames per second.		
VC.REQ.020	Camera Specifications	Minimum Pan range: +/-90 degrees ● Minimum Tilt range: +/-15 degrees		
VC.REQ.021	Directory services	The Video endpoint should support Local Recording		
VC.REQ.022	Directory services	Should support LDAP and H.350 protocols for directory transfer.		

Video Conferencing				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
VC.REQ.023	General requirement	Should support minimum HD720p Video resolution.		
VC.REQ.024	General requirement	The desktop client should have capabilities such as Instant messaging, chat, participants view etc.		
VC.REQ.025	General requirement	It should be possible to share the content from the desktop client		
VC.REQ.026	General requirement	The desktop client should be available for desktop or laptop (windows or mac), smartphone (android & iPhone) and iPad users		
VC.REQ.027	General requirement	It should be possible for a user to login into soft client using the single credential from any device.		
VC.REQ.028	General requirement	The solution should have the flexibility to accept the call on any device such as desktop or laptop or iPad or iPhone etc.		
VC.REQ.029	General requirement	The desktop clients should be IPV4 and IPV6 day one		

Video Conferencing				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
VC.REQ.030	General requirement	The desktop clients should be interoperable with Video conference endpoints for both audio & video.		
VC.REQ.031	General requirement	The desktop should have capabilities such as full screen view, mute audio, self-view as PIP, onscreen keypad for DTMF dialling etc.		
VC.REQ.032	General requirement	The MCU must be a hardware/SW based MCU providing minimum 30 ports and above of 1080p 30fps		
VC.REQ.033	General requirement	The MCU should be scalable in future		
VC.REQ.034	General requirement	All the 30 Ports must be able to connect different sites at different bandwidths and protocols. H.264 AVC standard must be supported at the minimum to connect all the 10 sites.		
VC.REQ.035	General requirement	The bridge should support room-based video end points, users joining from browsers' supporting WebRTC and HTML5 and its own clients. In case additional components are required for this functionality, all additional components required to have this functionality has to be included in the solution		

Video Conferencing				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
VC.REQ.036	General requirement	The bridge should have the capability to host meetings with internal and external participants in a secure way such that it should co-exist with the enterprise security policies		
VC.REQ.037	General requirement	The bridge should have components such as the Web Server for Web RTC, Scheduler as part of the offering from day one.		
VC.REQ.038	General requirement	Should support H.263, H.263+, H.264, WebRTC video algorithms		
VC.REQ.039	General requirement	Should support video resolution from SD to Full HD to join into a conference		
VC.REQ.040	General requirement	Must support the ability to allow Video conferencing devices, Clients on Mobile phones, Smart phones and Laptops to join into conference. These clients can be inside the WAN network or even on the Internet without a VPN.		
VC.REQ.041	General requirement	The bridge should support transcoding of different Audio/video Protocols.		
VC.REQ.042	General requirement	The bridge should have H.239/BFCP protocol for sending and receiving dual video streams (Presenter + Presentation).		
VC.REQ.043	General requirement	The bridge should support 128 Bit strong AES encryption for calls and H.235/SHA1 for authentication		

Video Conferencing				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
VC.REQ.044	General requirement	It should support for H.323 SIP Interworking Encryption and H.323 SIP Interworking Duo Video		
VC.REQ.045	General requirement	The MCU should support viewing of minimum 28 parties in continuous presence mode.		
VC.REQ.046	General requirement	MSI to ensure no lag or buffering in the video conferencing solution		
VC.REQ.047	General requirement	Video conferencing shall have the feature of making groups and call simultaneously. Groups shall be predefined on the level of Thana, Circle, DCR etc.		
VC.REQ.048	Seamless	There shall be no lag or buffering in provided solution		

7. Identity and Access Management Software (IAMS)

Identity and Access Management System				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
IAMS.REQ.001	Identity and Access Management	Solution should provide the ability to make real-time course-grained authorization decisions such as a whether to grant access to an application		

Identity and Access Management System				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
IAMS.REQ.002	Identity and Access Management	Solution should allow access and authorization permission criteria to be linked to role definitions rather than to individual user accounts so that these decisions are driven by a user's membership of a role		
IAMS.REQ.003	Identity and Access Management	Solution should respond to requests from applications for authorization decisions, based on user role membership and other user properties		
IAMS.REQ.004	Identity and Access Management	Solution should respond to requests from applications for authorization decisions, based on user role membership and other user properties		
IAMS.REQ.005	Identity and Access Management	Solution should be sized for 65000 Users		
IAMS.REQ.006	Identity and Access Management	Solution should support the implementation of Role Based Access Controls (RBAC) for controlling access to functions within an application		
IAMS.REQ.007	Identity and Access Management	Solution should support separation of duties		
IAMS.REQ.008	Identity and Access Management	Solution should detect orphaned accounts (accounts that have no associated record in a specified authoritative data source) and perform an action such as "suspend" or "notify"		
IAMS.REQ.009	Identity and Access Management	Solution should detect unauthorized changes to a user account and send a notification and roll back the changes		

Identity and Access Management System				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
IAMS.REQ.010	Identity and Access Management	Solution should provide the ability to a user who has forgotten his/her login ID to trigger an automated resending of it to the email address associated with their user account		
IAMS.REQ.011	Identity and Access Management	Solution should provide the ability for a user to self-reset their password		
IAMS.REQ.012	Identity and Access Management	Solution should enforce password policies during user self-service password resets		
IAMS.REQ.013	Identity and Access Management	Solution should be triggered to synchronize data in the solution identity data repository by an event in another authoritative data source.		
IAMS.REQ.014	Identity and Access Management	Solution should automatically discover data in the other identity data sources, (e.g. detect new user accounts in back-end applications and retrieve their associated attributes)		
IAMS.REQ.015	Identity and Access Management	Solution should generate a unique user ID – a unique and permanent identifier to unambiguously identify every user in the solution identity data repository		
IAMS.REQ.016	Identity and Access Management	Solution should be capable of identifying individuals who have more than one user account in the solution identity data repository, and merging these accounts into one		
IAMS.REQ.017	Identity and Access Management	Solution should perform audit and logging capabilities		

Identity and Access Management System				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
IAMS.REQ.018	Identity and Access Management	Solution should provide operational and user activity reports provided out of the box		
IAMS.REQ.019	Identity and Access Management	Solution should allow for the automatic archival of audit logs after a given period of time		
IAMS.REQ.020	Identity and Access Management	Solution should provide a workflow system to accept change requests from users directly, request and track authorization, and provision access once requests are submitted and approved.		
IAMS.REQ.021	Identity and Access Management	Solution should allow users can reset or change forgotten passwords and access or unlock locked accounts		
IAMS.REQ.022	Identity and Access Management	Solution should enforce password strength using password policy		
IAMS.REQ.023	Identity and Access Management	Solution should support SMS support which allows one-time tokens via text message for user verification, activation and new passwords.		
IAMS.REQ.024	Identity and Access Management	The system shall provide comprehensive reporting such as —who has access to what, —who approved what, —orphaned accounts found and these reports should be available online or can be exported for distribution.		

Identity and Access Management System				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
IAMS.REQ.025	Identity and Access Management	Proposed solution should be on-premise and should be capable of supporting 100% user capacity at any given point of time.		
IAMS.REQ.026	Identity and Access Management	Proposed solution is required for internal Consumption and not to provide any services to citizens / Civilians. OEM License should be inline		
IAMS.REQ.027	Identity and Access Management	Solution should include Single Sign-on Functionality		
IAMS.REQ.028	Identity and Access Management	Solution should be built on a federation standards-based architecture.		
IAMS.REQ.029	Identity and Access Management	Solution should have federation support.		
IAMS.REQ.030	Identity and Access Management	Solution should support federation protocols: SAML, ADFS, Oauth, OpenID Connect		
IAMS.REQ.031	Identity and Access Management	Solution should provide risk-based access control, authentication and authorization of users based on different attributes		
IAMS.REQ.032	Identity and Access Management	Solution should have its own user store or should leverage existing directories such as Active Directory or LDAP directories.		
IAMS.REQ.033	Identity and Access Management	Solution should provide strong authentication and multi-factor authentication to web and federated applications		

Identity and Access Management System				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
IAMS.REQ.034	Identity and Access Management	Solution should maintain logs for user access without exposing passwords		
IAMS.REQ.035	Identity and Access Management	Solution should also provide thick client SSO capability for client server-based application architecture		
IAMS.REQ.036	Identity and Access Management	Solution should enable a "stepped" approach to authentication, where advanced credential requests can be added within applications as users attempt to access more sensitive areas of the application.		
IAMS.REQ.037	Identity and Access Management	Solution should have multiple configurable methods, like biometric, SMS OTP, etc. that can be used for different applications based on the risk evaluation of those access.		
IAMS.REQ.038	Identity and Access Management	The solution shall provide out-of-the-box integration to the following directories for authentication. a. Active Directory, b. LDAP Directory c. RADIUS Server		
IAMS.REQ.039	Identity and Access Management	The solution shall support strong (two-factor) authentication technologies at least with the following: a. Smart Card b. Dynamic/One Time Password c. Biometric devices d. Two-Factor Token e. Digital Certificates		

Identity and Access Management System				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
IAMS.REQ.040	Identity and Access Management	The solution shall support integration to various security repositories (e.g. Active Directory, LDAP, Database, etc) to achieve Single Sign-On.		
IAMS.REQ.041	Identity and Access Management	The solution should protect home-grown and/or third-party applications.		
IAMS.REQ.042	Identity and Access Management	Proposed solution should be on-premise.		
IAMS.REQ.043	Identity and Access Management	The proposed PAM solution should offer various forms of deployment: Hardware appliance-based, virtual applbased, based or cloud based		
IAMS.REQ.044	Identity and Access Management	Proposed PAM solution should be sized for 300 Devices		
IAMS.REQ.045	Identity and Access Management	Solution should provide facility to monitor in real time and video recording of the privileged sessions for all the integrated devices, users and applications.		
IAMS.REQ.046	Identity and Access Management	The solution should be browser independent and there shouldn‘t be any browser dependency to manage and record the sessions.		
IAMS.REQ.047	Identity and Access Management	There should be no mechanism to export any password from the PAM vault under any circumstances.		
IAMS.REQ.048	Identity and Access Management	The proposed solution should support integration with enterprise infrastructure including strong		

Identity and Access Management System				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		authentication such as 2-factor & Radius		
IAMS.REQ.049	Identity and Access Management	The proposed solution should provide secure remote access to sensitive servers such as Windows servers, Unix/Linux, Web Applications without having to expose credentials to end-users		
IAMS.REQ.050	Identity and Access Management	The proposed solution should support logs forwarding to SIEM tool		
IAMS.REQ.051	Identity and Access Management	System should log activity in case of any PAM bypass or direct access event.		
IAMS.REQ.052	Identity and Access Management	All the solution components should be from single OEM only for tight integration.		
IAMS.REQ.053	Identity and Access Management	The solution should support high availability (load balancing and DC-DR) and should not have a single point of failure without any additional costs.		
IAMS.REQ.054	Identity and Access Management	Should be an on-premises solution only, so no data is sent to cloud infrastructure.		
IAMS.REQ.055	Identity and Access Management	The Proposed solution should have feature to map application clients with RDP applications and once admin access RDP application then can see only related applications.		

Identity and Access Management System				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
IAMS.REQ.056	Identity and Access Management	Solution should be able to invoke second level of authentication while accessing critical resources.		
IAMS.REQ.057	Identity and Access Management	The Multi Factor Authentication solution shall support authentication mechanism like Hardware USB Token, Hardware Token, Mobile Token, email Token & SMS Token.		
IAMS.REQ.058	Identity and Access Management	Mobile Token of Multi Factor Authentication solution shall have following features:		
IAMS.REQ.059	Identity and Access Management	Token shall generate password dynamically within every 60 seconds or less.		
IAMS.REQ.060	Identity and Access Management	Token Application that generates the password shall be PIN protected.		
IAMS.REQ.061	Identity and Access Management	Token shall have six-digit numerical passwords.		
IAMS.REQ.062	Identity and Access Management	Token shall be available as a software form factor. Mobile token can be installed on Windows mobiles, iOS, Android, Blackberry etc.		
IAMS.REQ.063	Identity and Access Management	Every token shall have unique identity & shall be unique to user.		
IAMS.REQ.064	Identity and Access Management	Token shall be time synced with authentication server.		
IAMS.REQ.065	Identity and Access Management	Support Android, IOS, Windows mobile, windows 10 for soft token implementation		

Identity and Access Management System				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
IAMS.REQ.066	Identity and Access Management	Solution should support duress authentication		
IAMS.REQ.067	Identity and Access Management	The Multi Factor Authentication solution shall support following authentication mechanisms: Time based one-time password (TOTP) soft token, SMS, Email, Fingerprint, FaceID, PKI, voice OTP		
IAMS.REQ.068	Identity and Access Management	Solution should be able to enroll all ten fingers for biometric authentication.		
IAMS.REQ.069	Identity and Access Management	The Multi Factor Authentication solution shall support authentication mechanisms OAUTH, SAML & OpenID Connect		
IAMS.REQ.070	Identity and Access Management	Solution should not have any restriction on number of users accessing PAM portal.		

8. Datawarehouse, Data Analysis and Business Intelligence Tool

- As detailed under section number 4.27.5 of 'Data architecture and requirements', Analytics and research center (ARC) is envisaged in NexGen UP112 to generate insights on issues of UP112 operations and to identify bottle necks of current system. But for ARC to function well data shall be available in a form that insights, rich visualization, or useful reports can be generated. Thus, MSI is expected to take all relevant steps as detailed in section number 4.27.5 to ensure availability of refined, integrated, and redefied data.
- The envisaged analytics and BI solution will help the department to streamline its operations and plan resource deployment better. It shall act as a force multiplier and support day to day policing to cope up with traditional challenges of Law & Order. It shall be an end-to-end enterprise grade solution to meet the data quality and data analytics challenges faced by the organization. Some of the key components of the data analytics and BI solution are following:

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
General Requirements				
DDB.REQ.001 A	Overview of Solution	The proposed solution is envisaged as a single integrated solution with all components (end-to-end Data Management, Data Quality, Advanced Analytics, Alerting and Investigation, Monitoring and Visualization capabilities) from a single vendor and no bolt-on applications to ensure seamless flow of information and quick insight generation. Some of the key components of the solution is described below: • **Data Sources Layer:** This is the source layer where operational data is recorded. Data source are integration points which feeds data into application data repository layer. These integrations can be APIs (Application program interfaces) or offline loading of data sets. • **Data Ingestion Layer:** Data ingestion comprises of ETL (extract,		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		transform, load) operations which are key database functions that are combined into one tool and have automatic flow of pulling out the data from data sources and place it into Central Data repository in required format. This ensures that clean and standardized data flow into a central repository in the form of defined data structure to support data analysis. • **Data Repository Layer:** Data repository play key role in project. This layer will be responsible in storing and maintaining data in desired data structure for easy retrieval and quick analysis. Data storage layer should maintain different types of databases (ex: RDBMS, NoSQL, JSON, Logs etc.) • **Application Access Layer:** This will enable authorized business users and admin to connect through the envisaged solution using desired		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		protocol. It is front end to application and will handle all user experience. Authentication, authorization, security, and monitoring will be key responsibilities of this layer. • **Data Query Layer:** Data query layer extracts information from data processed by the ingestion layer and formats it into a human-readable form. • **Data Science (AI-ML) Layer:** Analytics Engine layer is the process of examining data sets to draw conclusions about the information they contain. This will help department to make data backed efficient operational decisions. Some of the key sub-layers of the envisaged analytics engine are – • BI Reporting • Statistical Analysis • Text Analytics		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		• Artificial Intelligence and Machine Learning (AI-ML) Its main goal will be to distil large datasets into visual graphics to allow for easy understanding of complex relationships within the data. Speed is key, and data visualization should aid in the understanding of vast quantities of data by not only applying visual representations to the data but also complex algorithms to automate extraction of key insights. • **Management Layer:** Management layer of the envisaged solution will help in implementing department specific SOPs, easy navigation across the solution, storing of insights in a structured manner and provide collaborative environment to the multi-disciplinary team to work efficiently. This will also ensure quick adoptability of the solution by the end users.		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		• **Data Governance Layer:** The solution should have ability to apply and implement data security and information security practices consistent with the organization's data security standards and policies. The security features of the solution should offer the following benefits: • Secure access to data and metadata • Role-based access to application features • Logging and auditing of security events • Access control reporting • Encryption of data in-flight and at-rest • The Solution should maintain a complete and comprehensive audit trail of all user activity from the moment they log on to the moment they log out, including any failed log-in attempts. Full details of searches,		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		views of data, export or printing of data, record creation, modification or deletion, user and system administrative tasks should be recorded. This includes the name of the user carrying out the action with date and time information. Proposed features of the application		
DDB.REQ.001	Analytics and BI tool	The Proposed Advanced Analytics Solution should be a pre-integrated, on-premises solution containing Data Management, Data Quality, Analytics, Alerting, Investigation, Monitoring and Visualization capabilities.		
DDB.REQ.002	Analytics and BI tool	The proposed solutions should have a single point of control over administrative tasks in the intelligence platform from Data Integration, Statistical Analysis, Analytical Models, Data Mining Models and Business Intelligence Reports.		
DDB.REQ.003	Analytics and BI tool	The proposed solution should provide interactive graphical user interface (GUI) / no-coding environment to add or modify data sources, relationships amongst entities, workflows, user screens across the		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		application, contents of drop downs, report templates etc. without vendor involvement.		
DDB.REQ.004	Analytics and BI tool	The solution should be deployable on-premises as well as on Cloud. It should be cloud ready, have microservices enabled architecture, support NLG generated insights and at the same time provide Model governance and Audit controls		
DDB.REQ.005	Analytics and BI tool	The solution should offer Single Integrated open platform for Analytics lifecycle, capabilities like Auto ML, Auto Feature Engineering, Open-Source Integration (R/ Python), Pre-Built Model templates, Machine Learning Model interpretation, AI Generated Data Preparations suggestions, AI Generated predictions, AI Generated explanations which ease the usage of technology and generate quick insights.		
DDB.REQ.006	Analytics and BI tool	The solution must be built on a loosely coupled microservices-based platform to enable features such as autoscaling, separation of configuration data from services layer, application data as backing services, services availability by standard protocol, etc.		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.007	Analytics and BI tool	The solution must support multi-tenancy and the flexibility of configuring single LDAP for all tenants or separate LDAP per tenant.		
DDB.REQ.008	Analytics and BI tool	The platform must provide in-built reverse proxy and forward proxy capabilities.		
DDB.REQ.009	Analytics and BI tool	The platform must have certificate manager capabilities and must support self-signed certificates for encryption of inter-process communication.		
DDB.REQ.010	Analytics and BI tool	The platform must be easy-to-deploy and must allow deployment automation using infrastructure-as-code techniques.		
DDB.REQ.011	Analytics and BI tool	The solution should contain data quality dictionary as a collection of files that store data and logic that define data management operations, such as data cleansing. This should be available as out-of-box.		
DDB.REQ.012	Analytics and BI tool	The tool should control access to applications, modules and functions based on user roles and privileges.		
DDB.REQ.013	Analytics and BI tool	The tool should provide a Central Metadata Repository to manage the flow and traceability of data and structures.		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.014	Analytics and BI tool	The solution should allow users to access procedures containing data management / data quality / analytical services through easy-to-use front-end interfaces		
DDB.REQ.015	Analytics and BI tool	The Tool should support client requests via standard SOAP interfaces.		
DDB.REQ.016	Analytics and BI tool	The solution shall have the capability to export data in open standards (such as XML/Json formats).		
DDB.REQ.017	Analytics and BI tool	The Proposed Advanced Analytics Solution should contain data quality dictionary as a collection of files that can store data and logic to aid data management operations, such as data cleansing and standardization.		
DDB.REQ.018	Analytics and BI tool	The Proposed Advanced Analytics Solution should enable Python, R, Java, Lua, and Scala programmers experience the power of solution through the use of APIs. It should support programming from popular open-source languages.		
DDB.REQ.019	Analytics and BI tool	System should be able to ingest data from multiple disparate data sources and bring it under one integrated platform for search, analysis, investigation, alerting, and correlation analysis.		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.020	Analytics and BI tool	The system shall be using capabilities from such architectures to create one holistic solution. The system should be able to perform in-depth analytics on the ingested unstructured data.		
DDB.REQ.021	Analytics and BI tool	Solution should be a thin client web-based application accessible only through HTTPS.		
DDB.REQ.022	Analytics and BI tool	Solution should support major browsers like Chrome and Firefox.		
DDB.REQ.023	Analytics and BI tool	The solution should be COTS with the requirements of the department to reduce implementation efforts, time, and cost		
DDB.REQ.024	Analytics and BI tool	The suite should offer single management console for metadata administration of the software from ETL, Data Quality, Statistical Analysis, Data Mining and Optimization to Business Intelligence Reports		
DDB.REQ.025	Analytics and BI tool	The Solution should provide a visual console to perform administrative tasks		
DDB.REQ.026	Analytics and BI tool	The Solution should provide the ability to View Users Data and Metadata Queries		
DDB.REQ.027	Analytics and BI tool	From administrative console, user should be able to start/stop service(s) pertaining to the solution		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
Security				
DDB.REQ.028	Analytics and BI tool	The tool should control access to applications, modules and functions based on user authentication and authorization		
DDB.REQ.029	Analytics and BI tool	The data access should be controlled based on individual profiles		
DDB.REQ.030	Analytics and BI tool	The security should be based on roles		
DDB.REQ.031	Analytics and BI tool	The Tool should provide for privileges to be set at a user level		
DDB.REQ.032	Analytics and BI tool	The product should support personalization and should provide zero-coding environment to customize screens.		
DDB.REQ.033	Analytics and BI tool	The Suite should support SSL		
DDB.REQ.034	Analytics and BI tool	The Solution should support for digital certificates		
DDB.REQ.035	Analytics and BI tool	The Solution should support for encryption. The suite should provide for data, metadata, data transmission between systems in encrypted format		
DDB.REQ.036	Analytics and BI tool	The platform must provide capabilities for data encryption, anonymization and masking using as AES-256-bit technologies.		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.037	Analytics and BI tool	The platform must support TLS based encryption for data-on-the-wire.		
Data Ingestion/Data Management				
DDB.REQ.038	Analytics and BI tool	The tool should provide native access to Industry leading RDBMS like ORACLE, SQL Server, DB2 etc.		
DDB.REQ.039	Analytics and BI tool	The tool should be rich in the set of in-built transformations and functions that should include predefined table and column-level transformations.		
DDB.REQ.040	Analytics and BI tool	The tool should provide for reuse of individual transformations.		
DDB.REQ.041	Analytics and BI tool	The tool should support for surrogate key generation.		
DDB.REQ.042	Analytics and BI tool	The tool should provide for creation of user-defined external transformation functions.		
DDB.REQ.043	Analytics and BI tool	The tool should provide pre-build functionalities for the following: · Financial Transformations · Mathematical Transformations · Statistical Computations · Should provide intuitive Graphic		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.044	Analytics and BI tool	The solution should provide user interfaces for Data Profiling, Data Standardization, Clustering and Data Augmentation capabilities. In Data Profiling, it should be able to conduct the following analysis: • structure discoveries, • frequency distribution • Pattern distribution • Various Statistical Analysis • Outliers Detection and Percentile reporting • Relationship Discoveries • Drill through analysis from graphical reports to transactional data		
DDB.REQ.045	Analytics and BI tool	Support data quality measurement on an on-going basis embedded into batch and near-time process		
DDB.REQ.046	Analytics and BI tool	Should be customizable and allow enhancement of its knowledge repository by constantly updating it.		
DDB.REQ.047	Analytics and BI tool	Should support data cleansing and de-duplication, duplicate suspect processing, house holding, with array of out-of-the- box standardization rules conform data to corporate standards – or can build customized rules for special situations.		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.048	Analytics and BI tool	Should have business rules and GUIs for automatic merging and manual merging.		
DDB.REQ.049	Analytics and BI tool	The Tool should provide for a rule's library to clean, standardize, match, and enhance data as it moves into the master reference file and is reused for downstream processes.		
DDB.REQ.050	Analytics and BI tool	The Tool Should provide fuzzy logic to induce tolerance during matching		
DDB.REQ.051	Analytics and BI tool	The Tool Should use the parsed data to provide flexible matching criteria		
DDB.REQ.052	Analytics and BI tool	The Tool Should have options for manual/automatic merging of clustered records		
DDB.REQ.053	Analytics and BI tool	The Tool Should enable to define rules for record and/or field selections during the merging process		
DDB.REQ.054	Analytics and BI tool	The Tool Should have the capability to enrich data from internal data sources		
DDB.REQ.055	Analytics and BI tool	The Tool Should have the capability to enrich data from external/third party data sources		
DDB.REQ.056	Analytics and BI tool	The tool should have the ability to disable and enable nodes and submit flows in any state.		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.057	Analytics and BI tool	The tool should have enhanced mapping features that includes intelligent handling of data type conversions, easy and selectable customizes mappings, and controlled propagation of changes to mappings.		
DDB.REQ.058	Analytics and BI tool	The tool should have the ability to start job runs from the source, the target, or the middle of the job.		
DDB.REQ.059	Analytics and BI tool	The tool should have the ability to easily capture and display performance information such as real time, CPU time, memory use, input/output, and record count data, with the ability to display this information as a table or as a graph.		
DDB.REQ.060	Analytics and BI tool	The tool should have transformations to perform analytical operations like Correlations, Distribution Analysis, Frequency and Summarization.		
DDB.REQ.061	Analytics and BI tool	System shall contain the data, software, and processes needed to cleanse, consolidate, and transform the data from their source system format to the data warehouse format.		
DDB.REQ.062	Analytics and BI tool	System shall be able to facilitate bulk data movement		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.063	Analytics and BI tool	System shall be able to join data from multiple sources and support for concurrent processing of multiple source data streams, without writing procedural code		
DDB.REQ.064	Analytics and BI tool	System shall be able to extract and transform information from multiple sources without any intermediate files		
DDB.REQ.065	Analytics and BI tool	System shall be able to check incoming data for quality, reliability, consistency, and validity, and then transform as required.		
DDB.REQ.066	Analytics and BI tool	System shall facilitate data profiling based on dynamic, user defined validation rules and support identification of user defined 'events' to trigger alerts (through email reports) to authorities		
DDB.REQ.067	Analytics and BI tool	System shall support In-memory data handling		
DDB.REQ.068	Analytics and BI tool	System shall allow high-performance movement and transformation of data between disparate systems in batch mode.		
DDB.REQ.069	Analytics and BI tool	System shall support batch mode data quality implementation		
DDB.REQ.070	Analytics and BI tool	System shall be able to generate notification alerts based on the occurrences of relevant knowledge items and as per pre-defined priority		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.071	Analytics and BI tool	System shall have the capability to correct mistakes in spellings, inconsistencies, casings, and abbreviations		
DDB.REQ.072	Analytics and BI tool	System shall support correction logic for Indian names, addresses, phone numbers, pan numbers, passport number and other identification proof documents and demographic details		
DDB.REQ.073	Analytics and BI tool	System shall support profile matching through multi-field text matching functionality on entity-profile information (comparison could be on combination of name, PAN, address, telephone number etc.)		
DDB.REQ.074	Analytics and BI tool	System shall provide facility to create ad hoc queries through use of simple business terms for querying the data sources		
DDB.REQ.075	Analytics and BI tool	System shall provide facility to save the queries and edit the same in future to derive newer queries		
DDB.REQ.076	Analytics and BI tool	System shall provide facility to save and export the generated reports in file formats like RTF, HTML, PDF		
DDB.REQ.077	Analytics and BI tool	The solution should be able to create networks based on both transaction as well as relationship-based data, and create a		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		nodes and links among the entities specified		
DDB.REQ.078	Analytics and BI tool	It should be possible to identify common entity types which are super hubs –i.e., appear commonly in majority of transactions and treat them separately as per need		
DDB.REQ.079	Analytics and BI tool	The solution should support various types of matches such as exact / fuzzy match etc. with the watch list		
DDB.REQ.080	Analytics and BI tool	The application should have functionality to "flag / unflag" entities as and when they are added to / removed from a watch list		
DDB.REQ.081				
Data Science (AI-ML) & Business Intelligence	Analytics and BI tool	The solution should provide one integrated user interface and workbench for data wrangling, data exploration, business intelligence and visualization, feature engineering, and modern statistical, data mining and machine learning techniques all in a single, integrated in-memory processing environment for faster insights, flexible deployment, and reliable and secure governance		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.082	Analytics and BI tool	The solution should provide interactive entity resolution capabilities that help analysts get the most accurate picture of complex relationships. The solution should provide out-of-box entity analytics and direct intelligence analysts by showing measures of centrality in entity networks - such as closeness, betweenness and influence to highlight areas of potential interest		
DDB.REQ.083	Analytics and BI tool	The solution should enable identification of suspicious behaviour profiles through a hybrid-analytics approach combining anomaly detection, business rules, advance predictive modelling, and network analytics		
DDB.REQ.084	Analytics and BI tool	The solution should help analysts to visualize complex network of relationships between entities - such as people, places, things, and events over time and across multiple dimensions		
DDB.REQ.085	Analytics and BI tool	The solution should help analysts identify entity relationships that aren't obvious, traverse and query complex relationships, and uncover patterns and communities interactively		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.086	Analytics and BI tool	The solution should support both web-based interfaces for programming and interactive point-and-click workflows and a collaborative environment that enables easy sharing of data, code snippets and best practices across analysts		
DDB.REQ.087	Analytics and BI tool	The solution should enable analytical tasks to be linked together as a single in-memory job without having to reload the data or write out intermediate results to disks - for faster execution and insight		
DDB.REQ.088	Analytics and BI tool	The solution should provide in-built features and advanced techniques for the analyst to detect rare events, anomalies, and outliers and/or influence points to help determine, capture, or remove them from downstream analysis such as predictive models.		
DDB.REQ.089	Analytics and BI tool	The solution should have model building & lifecycle management capabilities including data preparation, model development and model assessment as an interactive graphical user interface (GUI) to enable less tech savvy analysts create and test their own models as and when required.		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.090	Analytics and BI tool	The solution should have in-built modules for analysis of variance, multivariate analysis, and statistical algorithms to build prediction models such as Linear, Logistic, Non-Linear and Quantile regression models, Generalized Linear models, Predictive partial least squares, Neural Networks, Random Forest, Decision trees etc. using interactive user-interface with drag drop capability.		
DDB.REQ.091	Analytics and BI tool	The solution should have an inbuilt data transpose features such as variable binning, cardinality analysis, missing value imputation, sampling and partitioning etc. to save time and improve model input.		
DDB.REQ.092	Analytics and BI tool	The solution should be able to automatically calculate performance statistics such as ROC table, lift table, output statistics etc. and visualize it to the user on an interactive user interface.		
DDB.REQ.093	Analytics and BI tool	The solution should have automated model assessment capability to help the department choose the best fit model with higher predictability and lower false positive.		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.094	Analytics and BI tool	The solution should have in-built modules for Unsupervised learning with cluster analysis and mixed variable clustering		
DDB.REQ.095	Analytics and BI tool	The solution should in-built modules for modern machine learning algorithms to build predictive models - such as random forests, gradient boosting, artificial neural networks, support vector machines and factorization machines		
DDB.REQ.096	Analytics and BI tool	The solution, along with providing in-built modules for the modern machine learning algorithms, should also provide in-built feature for automated intelligent hyper-parameter tuning to identify optimal models through iterations, adopting the advanced methods such as Latin Hypercube.		
DDB.REQ.097	Analytics and BI tool	The Solution should provide a rich set of data mining algorithms that can be used for classification, regression, clustering, detection of outliers and anomalies, feature extraction, association analysis, and attribute ranking.		
DDB.REQ.098	Analytics and BI tool	The Solution should support Clustering of entities that are either user Defined or statistically chosen as best clusters, along		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		with strategies for encoding class variables into the analysis		
DDB.REQ.099	Analytics and BI tool	The Solution should support detection of patterns from the transaction data set over a defined time period for particular individuals / groups		
DDB.REQ.100	Analytics and BI tool	The Solution should have flexibility of high-performance imputation of missing values in features using different statistical options such as mean, pseudo-median and with user-specified values or with random value of non-missing values		
DDB.REQ.101	Analytics and BI tool	The Solution should support inbuilt data transformations and allow define custom transformations		
DDB.REQ.102	Analytics and BI tool	The Solution should support automated algorithms which will help the end-users to run multiple algorithms at a time and hence compare the results between them.		
DDB.REQ.103	Analytics and BI tool	The Solution should enable automated model assessment and scoring, and generate the associated model performance statistics and code for model scoring		
DDB.REQ.104	Analytics and BI tool	The solution should allow user to compare different predictive models on the basis of		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		different test statistics, and select the best model for deployment automatically		
DDB.REQ.105	Analytics and BI tool	The Solution should provide multiple methods to visualize data mining models and provide the user with sufficient levels of understanding and trust		
DDB.REQ.106	Analytics and BI tool	The Solution should be able to provide multiple reporting options to generate statistical and graphical summary of the transactions		
DDB.REQ.107	Analytics and BI tool	The Solution should be able to discover new patterns in the dataset (detect untrained patterns) and identify defined patterns in the dataset (trained patterns)		
DDB.REQ.108	Analytics and BI tool	The Solution should support processing, trend-analysis and modelling of data-points through exponential smoothing, missing data, and outlier data on all data sets before trend analysis / modelling		
DDB.REQ.109	Analytics and BI tool	The Solution should support trend analysis and modelling for identified parameters on entities, transaction-wise and commodity-wise data received from multiple sources		
DDB.REQ.110	Analytics and BI tool	The Solution should allow the analyst to view test statistic for each model built, and		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		hence select the model other than the auto select model		
DDB.REQ.111	Analytics and BI tool	The Solution should support optimized generic scriptable procedure for conducting advanced time series analysis and modelling		
DDB.REQ.112	Analytics and BI tool	The Solution should support profile matching through user-defined (configurable) business rules through ad-hoc querying across multiple fields of entity-wise information		
DDB.REQ.113	Analytics and BI tool	The solution should provide ability to provide interactive simulations and time series modelling		
DDB.REQ.114	Analytics and BI tool	The Solution should support Time Series and scenario (“What-If”) analysis for dependent variables.		
DDB.REQ.115	Analytics and BI tool	The solution should provide multiple methods of optimization (operations research) for optimizing decisions such as linear programming, integer programming etc.		
DDB.REQ.116	Analytics and BI tool	The Solution should enable rule based / cluster analysis for profile grouping and profile matching		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.117	Analytics and BI tool	The Department should be able to follow a champion challenger approach in model development through developing different model versions, compare results on different parameters, and select and deploy best performing model		
DDB.REQ.118	Analytics and BI tool	The Department should be able to model for risk using a variety of data mining, text mining, neural networks, machine learning, and simulation modelling techniques.		
DDB.REQ.119	Analytics and BI tool	The Analysts and Investigators should be able to make use of a fraud intelligence repository which gets populated containing information of performance of past models and scenarios, to improve accuracy of current predictive models. He/she should be able to define risk based on different levels such as relationships with entities, financial / non-financial transactions etc.		
DDB.REQ.120	Analytics and BI tool	The solution should be able to calculate the risk score of a network based on various metrics such as underlying entity risk, structure of the network, net flow of funds, and predictive models.		
DDB.REQ.121	Analytics and BI tool	Special types of network behaviour such as cyclical flow of transactions and funds,		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		shortest path to reach a suspect between two nodes etc. should be automatically identifiable and extractable from the networks.		
DDB.REQ.122	Analytics and BI tool	The Department should be able to carry out scenario analysis / what –if analysis on the model allowing for changes in future parameter values.		
DDB.REQ.123	Analytics and BI tool	The solution should allow alerts to be generated whenever flagged entities or entities with high-risk rating and having financial/ non-financial transactions or some level of activity		
DDB.REQ.124	Analytics and BI tool	The solution should support detection of patterns so that criteria for various thresholds can be reviewed and modified.		
DDB.REQ.125	Analytics and BI tool	The solution should support selection of criteria for Identification of cases for special vigilance		
DDB.REQ.126	Analytics and BI tool	The solution should be scalable to incorporate any additional functional requirements and application of additional niche analysis capabilities (such as text analytics etc.) of the Data Mining tool.		
DDB.REQ.127	Analytics and BI tool	The Solution should have ability to assign risk / fraud scores at various levels of aggregation such as at a transaction level,		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		entity level (aggregate of transactions and demographic / relationship information) or at a network level		
DDB.REQ.128	Analytics and BI tool	The proposed software must be able to accept text and should accept commonly used text sources such as ASCII text, document files, spreadsheet files etc.		
DDB.REQ.129	Analytics and BI tool	Should support clustering (the automated discovery of categorical divisions of a document collection without a set of pre-defined labels) of text data such as transaction descriptions / entity details etc.		
DDB.REQ.130	Analytics and BI tool	The proposed solution should be compatible for handling data in Indian language Unicode format		
DDB.REQ.131	Analytics and BI tool	The solution should provide an in-built Single, point-and-click GUI interface for guided development and deployment of text models - through Natural Language Processing, Term's extraction, Topic discovery, Category definition, Concept specification, Document level sentiment identification		
DDB.REQ.132	Analytics and BI tool	The solution should provide an in-built ability to create, modify and enable (or disable) custom concepts and test linguistic rule definitions with validation		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		checks within the same interactive interface		
DDB.REQ.133	Analytics and BI tool	The solution should provide in-built project creation wizard for project definition and In-line help to guide analysts through the text model development process.		
DDB.REQ.134	Analytics and BI tool	The solution should provide in-built feature of detailing the status of each step of text model creation, processing status and message dialogue to help diagnose model development issues (such as an insufficient number of documents in the collection to generate topics).		
DDB.REQ.135	Analytics and BI tool	The solution should provide in-built project management options that permit multiple text models to be simultaneously developed and run, with associated descriptions indicating each model's development status		
DDB.REQ.136	Analytics and BI tool	The in-built Natural language processing feature provided by the solution should include automated parsing, tokenization, part-of-speech tagging, synonym detection, spell checking and stemming		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.137	Analytics and BI tool	The solution should include additional Text Mining features such as - Output lists of terms to drop/keep and term frequency counts, easy drag and drop between keep and drop terms, ability to apply customized start and stop lists (for terms to include/exclude from processing), ability to include custom-defined categories and custom concepts		
DDB.REQ.138	Analytics and BI tool	The solution should provide the analyst an option to develop a taxonomy without input documents, and later run the taxonomy against the corpus		
DDB.REQ.139	Analytics and BI tool	The solution should provide in-built feature of Automated machine discovery to identify the core themes in the input document collection with associated relevance score		
DDB.REQ.140	Analytics and BI tool	The solution should provide in-built feature to interrogate and explore Term relationships within topics with term clouds (with configurable thresholds), interactive term maps and by drilling into topics to evaluate relevancy and refine discovered topics		
DDB.REQ.141	Analytics and BI tool	The solution should provide in-built feature of visual depiction of Topic-level sentiment		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		for the documents associated with that theme		
DDB.REQ.142	Analytics and BI tool	The solution should provide in-built feature of being able to promote the desired topics into categories for classification rule definitions which could be further enhanced with concept definitions		
DDB.REQ.143	Analytics and BI tool	The solution should provide in-built feature of Automated initial category rule definition based on user-refined generated topics		
DDB.REQ.144	Analytics and BI tool	The solution should provide in-built feature of detailing rule robustness through measures of true positive, false positive and false negative as visual diagnostics		
DDB.REQ.145	Analytics and BI tool	The solution should provide in-built feature of editing, enhancing, removing, or defining the rules from scratch as custom categories		
DDB.REQ.146	Analytics and BI tool	The solution should provide an extensive list of prebuilt rule operators that would be available to the analyst for detailed rule-model specification		
DDB.REQ.147	Analytics and BI tool	The solution should provide in-built feature of using Concepts to provide contextual specificity to categories to refine models for more exact meaning extraction		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.148	Analytics and BI tool	The solution should include a Predefined list of concepts addressing common entity definitions for date, location, time, etc. - without a need to add rules from scratch for them		
DDB.REQ.149	Analytics and BI tool	The solution should enable the Analyst to write custom concepts using a suite of predefined operators, edit and refine predefined and pre-existing concept rules and validate the concept rules with diagnostic error messages detailing any identified syntax issues - all as built-in-features		
DDB.REQ.150	Analytics and BI tool	Analyst should be able to add different entities such as Bank Statements, CDR, HUMINT and create relationship on the fly to view a holistic picture.		
DDB.REQ.151	Analytics and BI tool	System should be able to identify entities from the text and aid analyst to connect them with existing entity to enrich the data.		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.152	Analytics and BI tool	User should be able to search data such as person, fir, vehicle, mobile numbers etc. using various features: - form based search, - free text search, - fuzzy search, - radial search - phonetic search - Boolean search - wildcard search - synonym search - parametric search - booster search		
DDB.REQ.153	Analytics and BI tool	System should be able to plot geo-coded data on a map		
DDB.REQ.154	Analytics and BI tool	The solution should be able to play animation on maps.		
DDB.REQ.155	Analytics and BI tool	Should intelligently animate the path on map travelled by the suspect		
DDB.REQ.156	Analytics and BI tool	Geo Fencing: Should be able to define a virtual boundary on geographical MAPs		
DDB.REQ.157	Analytics and BI tool	User should be able to map, visualize, and analyse crime incident patterns.		
DDB.REQ.158	Analytics and BI tool	Should be able to display the entities with specified properties on the MAP.		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.159	Analytics and BI tool	User should be able to search for information in a defined area		
DDB.REQ.160	Analytics and BI tool	User should be able to perform radial search i.e., by searching for data in a circle of user defined radius.		
DDB.REQ.161	Analytics and BI tool	The solution should take an open, hub and spoke, data-driven approach so that the investigator analyst can configure solution capabilities to respond to new trends and business problems, access new data sources, and expand the use of the solution across the organization as requirements keep changing.		
DDB.REQ.162	Analytics and BI tool	The solution should provide in-built features for Alert and Event Management with - Governance, audit and compliance, Prioritized queuing model, Enrichment, Scenario-fired event model, including scenario context, Manual alert creation and routing, Alert domains, and Custom disposition actions.		
DDB.REQ.163	Analytics and BI tool	The solution should provide a built-in functionality of alert-based investigation and alert exploration and triage - in which alerts are reviewed to determine the probability that they represent suspicious		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		behaviour and are evaluated for their importance		
DDB.REQ.164	Analytics and BI tool	After a decision is reached about how to handle the alert, the solution should provide built in features to apply an appropriate disposition of the alert - such as closing, suppressing, moving to another queue (such as high or low priority), linking to a different object (such as a police report or case), and relaying the alert information.		
DDB.REQ.165	Analytics and BI tool	The alerts and event management capabilities of the solution should enable the investigator to:		
DDB.REQ.166	Analytics and BI tool	Prioritize alerts, visualize alerts in different views to gain context., Enhance alerts by adding entities and integrating and connecting data., Escalate by routing alerts or changing their priorities, create manual alerts., Manage multiple alert domains., Designate an alert to prompt a deeper investigation.		
DDB.REQ.167	Analytics and BI tool	The solution should enable to not just identify the entity against whom the alert was created, but also related alerts, related entities, and their interlinkages.		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.168	Analytics and BI tool	The Solution should provide facility to define rules and set threshold-based alerts for the same on the data used for query and analysis supported by solution		
DDB.REQ.169	Analytics and BI tool	The solution should provide in-built feature of powerful search capabilities to explore the contents of the data repository, enabling the investigator to discover information relevant to a current investigation or information about which to base a new investigation. If the search returns something suspicious, the solution should enable the investigator to take the findings into an investigation workspace for analysis.		
DDB.REQ.170	Analytics and BI tool	The Solution should provide in-built features for search and discovery through Exploration and Visualization, Free-text search, Filters and Facets and Geospatial search		
DDB.REQ.171	Analytics and BI tool	The solution should provide in-built features of powerful search and surfacing results using Boolean operators for search, searching for exact phrases, proximity search, searching using wildcards, fuzzy search, specifying precedence, searching in specific fields, searching using numeric		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		operators (for e.g., search for objects where the age field is greater than 10), searching for all values within a range and searching for reserved characters		
DDB.REQ.172	Analytics and BI tool	The solution search feature should allow user to select/deselect entities of interest like Name, account number, UID, PAN etc. to narrow down the search results for enhanced understanding		
DDB.REQ.173	Analytics and BI tool	The Solution should come in with in-built feature of workspace for interactive intelligence analysis, which will provide an investigator work area that enables the investigator to gather objects of interest - such as entities and alerts, to the investigation from the data repository.		
DDB.REQ.174	Analytics and BI tool	In addition to standard, unbounded searches, the solution should come with in-built feature of geo-spatial search. The solution should provide a Map View that enables the investigator to search within specified areas. If a standard search indicates some areas of particular interest, the investigator should be able to draw shapes on the map to mark those areas, and then search again to return only locations within the bounds of the shapes.		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		Alternatively, the investigator should also be able to start from a map with Searching with no search results displayed, draw their search shapes, and then enter their search terms to search only in the selected areas.		
DDB.REQ.175	Analytics and BI tool	The solution should provide in-built feature of multiple visualizations to view relationships between the objects of interest and associated information - such as locations associated with the data plotted on a map, events associated with the data plotted on a timeline, network view of relationship within the data, tabular views, and detailed information views of the data.		
DDB.REQ.176	Analytics and BI tool	The solution come with an in-built feature to provide flexibility of adding different objects of interest to the investigation workspace as well as multiple investigation workspaces to a specific investigation.		
DDB.REQ.177	Analytics and BI tool	The Solution should come in with out of box feature of documenting key findings or insights for e.g., Network diagram from workspace captured as a finding - which will help analyst document the analysis. The insights could include information about an		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		alert, a snapshot of a network diagram, or other visualizations		
DDB.REQ.178	Analytics and BI tool	The Solution should provide in-built feature of documenting insights by adding text to insights, built-in rich-text editors to use font attributes to comply with regulations or to emphasize details and adding images or links to additional resources to the insights.		
DDB.REQ.179	Analytics and BI tool	The solution should have in-built features for Entity analytics through Entity resolution, Network analytics and visualization, Network link expansion, Network node decorator and enrichment		
DDB.REQ.180	Analytics and BI tool	Should have pre-configured features to identify and extract entities such as names, persons, organizations / companies, and locations from text data. It should also be able to use a customized list of entity pattern (such as PAN card, UID numbers etc.) based on rules		
DDB.REQ.181	Analytics and BI tool	Should make use of natural language processing (NLP) techniques to enable parsing and stemming of text data, identify of main topics of discussion and identify the correlated topics. It should also directly		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		support the use of regular expressions (REGEX) for matching purposes.		
DDB.REQ.182	Analytics and BI tool	The system should extract the following entities from unstructured data (indicatively) – · People · Organizations · Places · Events · Phone Numbers · IP Address · Dates		
DDB.REQ.183	Analytics and BI tool	The solution should have in-built feature for financial/ non-financial Transaction analysis using Transaction network visualization.		
DDB.REQ.184	Analytics and BI tool	Solution should provide capability for visualization and drilling down into networks		
DDB.REQ.185	Analytics and BI tool	Users of network visualization/ other appropriate visualization should be able to drill down further into networks and view additional links as required		
DDB.REQ.186	Analytics and BI tool	The solution should come with in-built features of multiple instances of network diagrams related to an investigation - that will be dynamically surfaced - by presenting		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		a selected object (such as an alert) as the central object and other relevant connected objects linked as appropriate.		
DDB.REQ.187	Analytics and BI tool	The solution should come with in-built features of making customizations to the network diagrams such as - incremental zooming for better viewing, moving the network diagram around the canvas, adding objects from the network diagram into existing or new investigation workspaces and adding the entire network into existing or new insight documentations		
DDB.REQ.188	Analytics and BI tool	The solution should come with in-built features of the network diagrams within investigation workspaces to be viewed as a table, as a detail list, within a map context, or on a timeline, all as appropriate		
DDB.REQ.189	Analytics and BI tool	The solution should come with in-built features of the network diagrams within investigation workspaces to apply modifications or change settings and properties to one or more selected nodes, add, delete, group, and ungroup nodes and links, expand relationships to perform in-depth investigations and hide or reveal nodes to better surface entities and relationships of interest		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.190	Analytics and BI tool	The solution should come with in-built features of the network diagrams within investigation workspaces to apply entity analytics through centrality measures such as closeness, betweenness, degree, Eigen, and influence - to understand significance of relationships within a social network		
DDB.REQ.191	Analytics and BI tool	Additional links and entities which are external to the network data, should also be allowed to be added to the network		
DDB.REQ.192	Analytics and BI tool	The entity analytics features in the solution should support and direct intelligence analysts by showing entity closeness, betweenness and influence to highlight areas of potential interest. Seeing the complex network of relationships between people, places, things, and events over time and across multiple dimensions helps analysts identify relationships that aren't obvious, traverse and query complex relationships, and uncover patterns and communities interactively.		
DDB.REQ.193	Analytics and BI tool	The solution should allow Analysts to interact through an in-built network viewer to see entire social networks and the flow of transactions. There should be features to		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		enable expand or trim the network as required, explore communities and individual relationships, and manipulate the network layout, as well as overlay transaction information to show exchanges between two parties.		
DDB.REQ.194	Analytics and BI tool	There should be features to take snapshots and clips of the insights that they develop, collaborate with other investigators, and document their findings.		
DDB.REQ.195	Analytics and BI tool	The network analysis should include in-built features such as Network viewer/Node link diagram, Visualize complete networks and relationships through multilevel expansion, Identifies areas of interest and centrality within the network by showing entity closeness, betweenness, influence and more, Node annotators to Help analysts identify entities at a glance and investigators understand network data by highlighting useful information on the node icon view (for example, to indicate customer accounts held at different banks).		
DDB.REQ.196	Analytics and BI tool	The Solution should provide facility to generate static or dynamic interactive visualization charts and graphs		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.197	Analytics and BI tool	The Solution should support analysis of cases to determine patterns that may help the department in optimizing existing resources and reducing pending cases		
DDB.REQ.198	Analytics and BI tool	The system shall have capability to generate scores for different entities based on the formulae and select cases with higher scores.		
DDB.REQ.199	Analytics and BI tool	The solution should have in-built features for Surveillance and alert creation so that Analysts can author scenarios to uncover anomalous events for triage.		
DDB.REQ.200	Analytics and BI tool	The solution should enable administrators quickly design and deploy new intelligence assets using interactive, drag-and-drop page builder features without having to develop elaborate custom interfaces		
DDB.REQ.201	Analytics and BI tool	The Solution should have built-in capabilities to assign Alerts to different strategies and queue for assignment from drop-down		
DDB.REQ.202	Analytics and BI tool	The Solution should come with Configurability features such as Open data model, Federated query, Easy addition of new data sources, Easy Page/Home page design with a drag-and-drop interface, Monitor and manage processes or jobs,		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		Defining of links/relationships, Application configuration import/export, Data import or query by reference from internal or external sources.		
DDB.REQ.203	Analytics and BI tool	The solution should have features to embed Graphs to understand profiles, Geo-maps to understand locations of persons, organizations and events and URLs to visualize web content on the same investigation interface.		
DDB.REQ.204	Analytics and BI tool	System shall provide facility to summarize and present data using a variety of highly customizable charts, including vertical and horizontal bar, pie, donut, sub-grouped pie, star and block charts, plots like scatter, line, area bubble, multiple axis and overlay plots		
DDB.REQ.205	Analytics and BI tool	System shall provide dashboard facility with visual features like Metric Dials, Graphs, etc. for display and track of metrics		
DDB.REQ.206	Analytics and BI tool	System shall be scalable to incorporate any additional functional requirements and application of analysis capabilities of the BI tools		
DDB.REQ.207	Analytics and BI tool	The solution should provide flexibility of displaying the dashboards on third-party tools such as MS-Office applications		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.208	Analytics and BI tool	The solution should allow generation of dashboard using ad-hoc queries by the user		
DDB.REQ.209	Analytics and BI tool	The reporting solution should be web-enabled.		
DDB.REQ.210	Analytics and BI tool	The reporting Solution should enable different types of users to conduct fast, thorough explorations on all available data without the need to Subset / sample / create multiple views of data with minimal training for users		
DDB.REQ.211	Analytics and BI tool	Capability to import and integrate local text/csv/xls files with the data warehouse/ODS and be able to generate reports with no intervention from IT		
DDB.REQ.212	Analytics and BI tool	The reporting Solution should have the ability to be configured on open standard hardware		
DDB.REQ.213	Analytics and BI tool	The reporting Solution should provide a user friendly; web based, drag, and drop interface for data preparation for data tables available in-memory		
DDB.REQ.214	Analytics and BI tool	The reporting Solution should provide Auto charting. Based on data items selected for analysis, the reporting Solution should automatically choose the chart best suited		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		to display the type of data selected: E.g., one measure yields a frequency chart, two measures yield a scatter plot, three measures yield a bubble chart, etc.		
DDB.REQ.215	Analytics and BI tool	The reporting Solution should provide Geographical map views to provide a quick understanding of geospatial data.		
DDB.REQ.216	Analytics and BI tool	The reporting Solution should provide capabilities to subset data without intervention of IT or requirement for any specific skills / technology		
DDB.REQ.217	Analytics and BI tool	The reporting Solution should allow 'On-the-fly' hierarchy creation for being able to traverse to lowest information to undertake root cause analysis		
DDB.REQ.218	Analytics and BI tool	The reporting Solution should provide the capability to export data to Excel and CSV/TSV document formats		
DDB.REQ.219	Analytics and BI tool	The reporting Solution should have the ability for Interactive report viewing for information consumers using iPad and Android devices using a native application most popular gestures and capabilities, including zoom, swipe, etc., to optimize ease of use and user engagement.		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.220	Analytics and BI tool	The reporting Solution should provide users the capability to save and share their analysis as exploration, report, or PDF		
DDB.REQ.221	Analytics and BI tool	The reporting Solution should not be dependent on data warehouse or data marts. The reporting Solution should be able to surface information directly from transactional systems		
DDB.REQ.222	Analytics and BI tool	The reporting Solution should visually prepare data for analysis, including joining tables, defining custom calculated columns, and creating custom expressions for data tables available in-memory		
DDB.REQ.223	Analytics and BI tool	The reporting solution should provide capabilities to schedule jobs for data updates and report refresh		
DDB.REQ.224	Analytics and BI tool	The reporting solution should provide integrated analytics to identify Relationships in the data using Data Mining Techniques		
DDB.REQ.225	Analytics and BI tool	The reporting solution should be capable of scaling up to distributed computing environments if needed in order to leverage the parallel processing capabilities of multiple machines		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.226	Analytics and BI tool	The reporting solution should allow users to securely view reports on mobile devices while online or offline.		
DDB.REQ.227	Analytics and BI tool	'The reporting solution should be able to maintain Mobile device logging history and also be able to backlist/whitelist devices		
DDB.REQ.228	Analytics and BI tool	System should support exploration of relationships (either transactional or demographic / profile based) of entities through appropriate visualization. Adequate emphasis on core measures such as transaction amount, size of entity etc. should be depicted as node size / link width etc.		
DDB.REQ.229	Analytics and BI tool	System shall have capability to generate analytical reports on the basis of defaulter history (across non-filers, defective, zero and short filers)		
DDB.REQ.230	Analytics and BI tool	System shall enable tracking an entity post flagging, it is required to earmark such entity profiles in the system and to generate reports for that entity and his associated entities.		
DDB.REQ.231	Analytics and BI tool	The system shall have capability to generate MIS reports using GUI		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.232	Analytics and BI tool	Department should be able to design reports and dashboards in a GUI based environment with automatic refresh based on changes in underlying data sources		
DDB.REQ.233	Analytics and BI tool	The solution should have feature wherein Reports can be designed without the need for an underlying cube / summarized data structure		
DDB.REQ.234	Analytics and BI tool	The solution should have feature wherein Report can be drill down to most granular level of detail as their access controls / profiles allows		
DDB.REQ.235	Analytics and BI tool	The solution should have feature wherein Reports can be populated / filtered based on sub-queries and interactive filters from previous selections.		
DDB.REQ.236	Analytics and BI tool	The solution should have feature wherein Parameters can be passed among reports to retrieve details and investigate specific entity.		
DDB.REQ.237	Analytics and BI tool	The solution should have feature wherein Based on need, users of the reporting portal can execute stored procedures through the reporting interface and visualize the reports		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.238	Analytics and BI tool	The solution should have feature wherein Upon identification of actionable items (such as non-filers, address mismatches), report consumers can access procedures to carry out processes for customer contact / communication through the reporting interface		
DDB.REQ.239	Analytics and BI tool	System shall support generation of reports through user-defined (configurable) ad-hoc querying across multiple fields of entity-wise information (across registration, passport, CDR data, etc.)		
DDB.REQ.240	Analytics and BI tool	The user interface should have the capability to integrate with Web-Services i.e. Should support sending and receiving web services		
DDB.REQ.241	Analytics and BI tool	The solution should provide flexibility of displaying the dashboards on third-party portals including MS-Office applications		
DDB.REQ.242	Analytics and BI tool	The solution should allow generation of dashboard using ad-hoc queries by the user		
Management Layer				
DDB.REQ.243	Analytics and BI tool	The Solution should have in-built Case management features including case id generation, Workflow implementation,		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		team assignment, tasking, evidence chain management, auditing, report generation etc.		
DDB.REQ.244	Analytics and BI tool	The admin should be able to assign users/groups to each case.		
DDB.REQ.245	Analytics and BI tool	User should be able to create and modify case details		
DDB.REQ.246	Analytics and BI tool	The solution should be able to add case specific details		
DDB.REQ.247	Analytics and BI tool	The solution should enable user to add case specific entities (people, organization, mobile, bank accounts, bank statement, CDR etc.)		
DDB.REQ.248	Analytics and BI tool	User should be able to store case specific investigative insights for future references.		
DDB.REQ.249	Analytics and BI tool	User should be able to create tasks and assign tasks from the case screen		
DDB.REQ.250	Analytics and BI tool	User should be able to attach files to the case		
DDB.REQ.251	Analytics and BI tool	The solution should be able to automatically identify similar cases		
DDB.REQ.252	Analytics and BI tool	User should be able to adopt institution wide best practices to improve efficiency and reduce investigation time.		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.253	Analytics and BI tool	Users should be able to add comments to a case.		
DDB.REQ.254	Analytics and BI tool	The solution should enable printing of case specific reports for dissemination through a configurable report template.		
DDB.REQ.255	Analytics and BI tool	The Solution should have the ability to create SOPs or workflows for additional review(s) and rework(s) before case disposition based on several factors (role, tier, delegated authority, etc.…).		
DDB.REQ.256	Analytics and BI tool	Users should be able to create task and update the status of the task		
DDB.REQ.257	Analytics and BI tool	User specific task should be displayed on the user's home page		
DDB.REQ.258	Analytics and BI tool	User should be able to view all his task at one place and change the status as applicable.		
DDB.REQ.259	Analytics and BI tool	The tool should have ability to configure organization specific workflows to bring structure, control and automate processes.		
DDB.REQ.260	Analytics and BI tool	The solution should provide intuitive user interface to develop and implement organization defined custom workflows during case lifecycle to support organizational processes, without the need of coding.		

Data warehousing and BI Tools				
Sr. No.	Nature of requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
DDB.REQ.261	Analytics and BI tool	The solution should support audit management		
DDB.REQ.262	Analytics and BI tool	The solution should save HTTP status code returned by the server		
DDB.REQ.263	Analytics and BI tool	The solution should have full audit trail / logging of all changes in the database (who, when, which table, which field, old value, new value)		
DDB.REQ.264	Analytics and BI tool	The solution should be able to track user actions including but not limited to Sign In, Sign Out, Download File, Download Attachment, Create, Delete, Export, Print, Remove, Search, Link and Unlink etc.		
DDB.REQ.265	Analytics and BI tool	The solution should save IP addresses of the device used to perform audited action		
DDB.REQ.266	Analytics and BI tool	User should be able to export outcome of the audit queries to excel		
DDB.REQ.267	Analytics and BI tool	The solution should provide no coding environment to add new data sources, make or update relationships amongst entities, add/modify workflows, user screens, report templates, dashboard etc. though an interactive GUI without the need of coding.		

9. Video Management Software

Video Management Software				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
VMS.REQ.001A	Overview of solution	Video management software shall be used for viewing the feed of camera mounted on PRVs deployed in critical areas		
VMS.REQ.001	General requirement	The proposed video management system software should be able to support minimum 120 CCTV Cameras per Server or better for management and recording. Proposed VMS should be scalable and unlimited client and Server without any restriction		
VMS.REQ.002	General requirement	The proposed solution should be supplied with required hardware, software / Appliance, and local storage in high availability mode to keep archival for minimum 30 days. The solution should have recording, database, and management servers in HA Mode (auto failover) with adequate configuration for best performance. The VMS solution shall support failover architecture		
VMS.REQ.003	General requirement	VMS should support video streams up to 60 Frames per second for all cameras in different resolutions		

Video Management Software				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
VMS.REQ.004	General requirement	The VMS should have user interface that provides one-click access, drag-drop, context menu, shortcut keys, customizable GUI etc.		
VMS.REQ.005	General requirement	Simple, clear documentation including User Guides (how to use the product) and Technical Reference Manuals (quick reference on function and procedures) shall be submitted		
VMS.REQ.006	General requirement	Roles based user management: User, roles, rules, and privileges should be stored on the central VMS server.		
VMS.REQ.007	General requirement	The System should not restrict the number of recording servers. Should support dual streaming. Should allow each stream to be viewed independently by client viewer. Recording from connected cameras should be stored in database. Should support multiple storage format		
VMS.REQ.008	General requirement	Update of hardware drivers & firmware free of cost VMS version upgrade at no extra cost		
VMS.REQ.009	General requirement	The VMS should have ability to easily install, configure, modify, search, and remove		

Video Management Software				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		surveillance devices with automatic discovery of IP devices		
VMS.REQ.010	General requirement	Provision for primary and backup storage settings for individual camera feeds		
VMS.REQ.011	General requirement	The VMS should have ability to configure multiple streams with different quality parameters e.g. Codec (H.264, H.265, MPEG, JPEG) resolution, frame & bit rate etc. The VMS shall support end to end encrypted streams with cameras supporting SRTP both in Unicast and Multicast.		
VMS.REQ.012	General requirement	Basic recording options (Full, Scheduled recording, Motion detection recording, external/internal hardware or software events / trigger based)		
VMS.REQ.013	General requirement	Advanced recordings options (Video only, Audio only, Video plus Audio, Retention rules, Archive/backup rules, and storage limits etc.)		
VMS.REQ.014	General requirement	PTZ configuration including presents, patterns, patrolling, masking, priority, and permissions.		

Video Management Software				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
VMS.REQ.015	General requirement	PTZ controls: When PTZ is deployed and enabled, system should offer a separate control panel for control.		
VMS.REQ.016	General requirement	Multiple Monitor Support: The system should allow connecting multiple monitors on single client workstation (loaded with suitable graphics card) and display different contents on each of the connected		

10. SDWAN Controller Software

SDWAN Software Controller				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
SDWAN.REQ.001	SD-WAN Architecture	SD-WAN Solution should be based on the SDN principal and so there should be clear separation of the control, management, and the data-plane. Each component should be independently scalable and manageable.		

SDWAN Software Controller				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
SDWAN.REQ.002		Control Plane: Control plane is responsible to maintain centralized routing table, controls route advertisement as per policy, creates end to end segments on network, instruct data plane to change traffic flow as per policy.		
SDWAN.REQ.003		Data Plane: Data plane is responsible to forward traffic in encrypted tunnels, apply local policy like QoS, ACL etc. The network should be implemented as true software defined network architecture with a centralized control plane residing in the Central Controller.		
SDWAN.REQ.004		SD-WAN System should be able to support Zero Touch Deployment of CPE device with predefined parameters irrespective of any location and without involvement of central team during activity at remote site. Also, solution should support the Two Factor Authentication on the device activation.		
SDWAN.REQ.005		SD-WAN Operational Solution should not be impacted, Control & Management nodes goes down. Solution should support head-		

SDWAN Software Controller				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		less mode for minimum of 7 days data plane reachability.		
SDWAN.REQ.006		SDWAN Management solution should provide single platform to monitor, troubleshoot and maintain the SDWAN Features and other security features including (Firewall, IPS, Antivirus, URL-filtering, DDOS, UTM, SD-WAN Traffic policy, QOS)		
SDWAN.REQ.007	Simplified, Scalable and Secure Network Architecture	The solution must be capable to do quick rollout of SD-WAN and branch deployments without complexity via multiple zero-touch provisioning (ZTP) approaches. New branch/Site deployments should be automated and completed in minutes.		
SDWAN.REQ.008		The Controller should be designed for scale to support up to 200 numbers of sites and the applicable required SDWAN licenses for controllers should be provided from day 1		
SDWAN.REQ.009	Solution Components and Deployment Options	The SD-WAN solution control components (Orchestrator/ Controller and Reporting System) should have options to deploy the system onsite using VMs, BareMetal/Whitebox, standard x86		

SDWAN Software Controller				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		appliances, it should not run-on proprietary hardware.		
SDWAN.REQ.010		The solution should support Enterprise deployment model that requires all SD-WAN components to be deployed in a closed network.		
SDWAN.REQ.011		SD-WAN Gateway, to Integrate SD-WAN and non-SD-WAN network.		
SDWAN.REQ.012	Multi-tenancy Support	All solution components should support have a native multi-tenancy framework so that the Management, Control and Data Planes are segmented.		
SDWAN.REQ.013		The solution should support multi-tenancy i.e., the customer's configuration, monitoring, reporting, routing, and traffic should be kept isolated while customer can control and manage the Infrastructure by themself.		
SDWAN.REQ.014	API Support	The solution components [Orchestrator / Reporting System] should support standard API on northbound interfaces to allow for any programmatic control and automation of		

SDWAN Software Controller				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		all SD-WAN configuration and monitoring processes.		
SDWAN.REQ.015	HA and Resiliency	The solution must have high availability (HA) in the management plane [Orchestrator/Management System] and Control Plane with redundant and geo-redundant options. In Forwarding-plane and Edge devices should support Active/Standby or Active/Active option. Link Aggregation support etc.		
SDWAN.REQ.016	Multiple Uplinks Circuits and Switchover	Solution should support any multiple types of WAN uplink, including T1/E1, DSL, Broadband Internet, MPLS, LTE, Radio and 5G in future. WAN links must be used independently of any other WAN link connected to the SD-WAN CPE by utilizing the dynamic path selection, steering and SLA functionality.		
SDWAN.REQ.017		Traffic link switchovers are handled by the monitoring feature allowing seamless transitions between WAN network without dropping existing sessions.		

SDWAN Software Controller				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
SDWAN.REQ.018	Service Topologies	The solution should support flexible topologies on a per-VPN basis, such as:		
SDWAN.REQ.019		Full mesh		
SDWAN.REQ.020		Partial mesh		
SDWAN.REQ.021		Spoke to Hub only (spokes connect to Hub only)		
SDWAN.REQ.022		Spoke to Spoke via Hub (any communication between spokes is done via Hub)		
SDWAN.REQ.023		Spoke to Spoke direct (direct route to spokes, and a backup route to Hub)		
SDWAN.REQ.024		The control plane should have the flexibility to define topologies at the VPN and the tenant levels.		
SDWAN.REQ.025	Connecting non-SD-WAN Sites and Disjoint Underlay Networks	For cases when some branch sites connect to a provider network with SD-WAN CPE and other branch sites connect to another provider network with a traditional PE-CE model, these SD-WAN to a non-SD-WAN environment should be able to communicate. If SD-WAN gateway is used		

SDWAN Software Controller				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		it should be able to communicate with the PE routers using standard routing protocols like OSPF and/or BGP, to exchange routes between the two islands.		
SDWAN.REQ.026		SD-WAN Gateways must address following main use cases:		
SDWAN.REQ.027		Disparate/Disjoint underlay-transport networks		
SDWAN.REQ.028		MPLS L3VPN Interworking		
SDWAN.REQ.029		Datacentre Interconnect for Inter-DC connectivity		
SDWAN.REQ.030		The solution should have options to connect SD-WAN CPEs located in one underlay to remote SD-WAN CPEs located in other disjoint underlay networks from any SD-WAN CPE in the whole SD-WAN domain.		
SDWAN.REQ.031	Interop and integration with external systems	The solution should be able to integrate with third-party management systems, Automations tools using standard protocols like SNMP, SYSLOG, Restful API etc., Integration with AAA, NTP etc.		

SDWAN Software Controller				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
SDWAN.REQ.032	Reporting	Generating statistics for reporting to retrieve on REST API, GUI, external syslog server or directly on the CPE. Reporting capabilities to visualize in real-time or regularly generate customized graphs and reports. Those customized reports can be scheduled, stored, and shared to email directly from the Management portal.		
SDWAN.REQ.033		Solution must provide historical and real-time data reporting for:		
SDWAN.REQ.034		Availability		
SDWAN.REQ.035		WAN link utilization		
SDWAN.REQ.036		Application usage based on total volume, and bandwidth		
SDWAN.REQ.037		Application performance based on latency, jitter, and packet loss		
SDWAN.REQ.038		Performance of various paths between any two branches		
SDWAN.REQ.039		SLA violation events		

SDWAN Software Controller				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
SDWAN.REQ.040		Alarms		
SDWAN.REQ.041		QoS statistics		
SDWAN.REQ.042		System load (such as CPU, Memory utilization)		
SDWAN.REQ.043		Utilization of the different access link of various branches		
SDWAN.REQ.044	Diagnostics Tools	Troubleshooting capabilities. Users who have the proper RBAC access can access logs, alarms, debugging capabilities, and various tools (TCPdump, speed tests, ping, traceroutes, etc.) from the SD-WAN Orchestrator/Controller.		
SDWAN.REQ.045	Routing Protocols	The solution must interact on the WAN or LAN side with standard protocols when there is a requirement of routing exchange between the SD-WAN and the existing infrastructure. The solution should support protocols such as static routing, VRRP, OSPF, BGP for IPV4 and IPV6 MP-BGP. BFD for faster convergence times as well as IP-SLA probes based on ICMP or		

SDWAN Software Controller				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		tracking to next hops or beyond to ensure IP connectivity.		
SDWAN.REQ.046	VPN	The solution must be compatible with Layer 2 VPN, Layer 3 VPN and Network Segmentations like VRF based segmentation to differentiate amongst Customer and business units/departments.		
SDWAN.REQ.047	Enhancing Voice and Video	The solution must support monitoring the link performance like loss, jitter, delay, link utilization along with FEC and packet replication to ensure real-time traffic always uses the best performing paths.		
SDWAN.REQ.048	TCP Optimization	SD-WAN solution must support TCP optimizations to mitigate the effects of high latency and packet loss on the performance of TCP-based applications		
SDWAN.REQ.049	Advance Security Features	SD-WAN solution must have advance security capabilities, like Zone protection, Denial-of-Service Detection and Mitigation, Stateful Firewall, Next-Generation Firewall, and Unified Threat Management like		

SDWAN Software Controller				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		Antivirus/malware protection, IPS/IDS, URL Filtering etc.		
SDWAN.REQ.050	Secure Overlay Network	SD-WAN solution must enforce encryption and authentication of all control, management, and data plane traffic among all SD-WAN components.		
SDWAN.REQ.051	Hierarchical QoS	SD-WAN solution must support QoS, traffic must be classified based on L2/L3/L4 fields and application matching (L7) and DSCP marking for Application traffic management and to interoperate with existing Network Infrastructure.		
SDWAN.REQ.052		Improving the performance for Voice, Video, and Business critical traffic end-to-end.		
SDWAN.REQ.053	DHCP	SD-WAN solution must support DHCP Server and Relay function.		
SDWAN.REQ.054	Tunnelling Protocols	SD-WAN solution must support PPoE, GRE and IPsec VPN protocol with standard encryption and algorithm from all SD-WAN appliances.		
SDWAN.REQ.055	Multicast in the Overlay Network	SD-WAN solution must support Multicast features like IGMP, PIM-SM/SSM etc.		

SDWAN Software Controller				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
SDWAN.REQ.056	IPv6 Support	SD-WAN solution must support IPv6 protocols and features like		
SDWAN.REQ.057		IPv6 and dual-stack IPv4v6.		
SDWAN.REQ.058		IPv6 App Traffic Engineering, App Policy Based Forwarding.		
SDWAN.REQ.059		IPv6 rich topology support (hub-spoke, partial mesh, full mesh).		
SDWAN.REQ.060		IPv6 Underlay.		
SDWAN.REQ.061		OSPFv3, MP-BGPv6, static IPv6 routes.		
SDWAN.REQ.062		VRRPv6		
SDWAN.REQ.063		Transition mechanisms: NAT64		
SDWAN.REQ.064	Real-Time Network Monitoring	SD-WAN solution must have dashboards for real-time network monitoring.		
SDWAN.REQ.065		Monitoring Dashboard should contain wealth of information regarding system and network health. Presented data contains, but is not limited, to:		

SDWAN Software Controller				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
SDWAN.REQ.066		Multiple device health summary with drill down functionality to view the device list with their respective status		
SDWAN.REQ.067		SD-WAN Application Traffic. Real-time traffic monitoring of ingress/egress traffic via multiple ports		
SDWAN.REQ.068		Alarm summary and drill-down functionality to view the list of devices with their respective events		
SDWAN.REQ.069	User Authentication	Orchestrator portal must support RBAC to allow customization of the user's view in accordance with the user's privileges and roles. Strict RBAC policies to ensure that tenant-level users in an organization have no access to or knowledge of other tenants who are sharing the resource.		
SDWAN.REQ.070		Additionally, external authentication and authorization servers should be integrated to Orchestrator over RADIUS, LDAP, LDAP Secure, or TACACS protocols.		
SDWAN.REQ.071	End to End SLA Monitoring	SD-WAN solution must support end-to-end SLA monitoring. For example, branch to branch SLA monitoring like jitter, delay, loss etc. should happen end-to-end even the		

SDWAN Software Controller				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		branch-to-branch communication are through single or multiple SD-WAN HUB/Gateway.		
SDWAN.REQ.072	Centralized Network Topology Definition and Assurance	Solution must have Single touchpoint to define, monitor and maintain SD-WAN network.		
SDWAN.REQ.073	Support for CPE behind NAT	SD-WAN solution must support automatic identification and tunnel creation when the SD-WAN CPE is connected behind a NAT device towards WAN.		
SDWAN.REQ.074	Link load balancing and Failover	SDWAN solution must have the support to use all the links as Active-Active with WRR based load balancing.		
SDWAN.REQ.075		SDWAN should be able to detect failover condition in sub-seconds and must switch to available path without disrupting applications like CRM, ERP, UCaaS, virtual desktop sessions, and more. It should be applicable for both brownout and blackout condition.		
SDWAN.REQ.076	User Level Control	There should also be a provision to provide user-level profiling, security posture check		

SDWAN Software Controller				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		and secured authentication using 802.1x and RADIUS/TACACS		
SDWAN.REQ.077		The authentication mechanism would be utilised for user and the edge devices, and the solution should support seamless integration.		
SDWAN.REQ.078	Warranty/Support	The entire solution should be on-prem solution and no solution component should be hosted on cloud/over the internet		
SDWAN.REQ.079		The solution should include five (5) years warranty from date of supply and extended AMC of three (3) years.		
SDWAN.REQ.080		The DC and DR components to be covered via a 24X7X4 OEM support and the edge locations to be covered via 8X5XNBD OEM support.		
SDWAN.REQ.081		The entire set of solutions should be from a COO as per the WTA guidelines.		
SDWAN.REQ.082		The entire set of solutions should be supported from the same OEM for at least 8 years from date of supply.		

11. Software Defined Network (SDN)

Software Defined Network				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
SDN.REQ.001	Software Defined Network	The proposed SDN solution should be a purely software-based solution and should not be dependent on any hardware make and model		
SDN.REQ.002	Software Defined Network	The SDN solution should offer to deploy virtualized network functions (like switching, routing, firewalling and load-balancing), administrators can build virtual networks for Virtual Machines or Virtual Desktop Infrastructure without the need for complex VLANs, ACLs or hardware configuration syntax on underlay physical network		
SDN.REQ.003	Software Defined Network	The SDN solution should support Stateful firewalling up to Layer 7 (including app identification and URL whitelisting/Filtering), embedded in the hypervisor kernel, distributed across entire environment with centralized policy and management without the need of any third -party agents		
SDN.REQ.004	Software Defined Network	The SDN solution should support security policies for virtual machines and can be defined based on grouping construct with dynamic or static membership criteria based on VM name, tags, logical switch,		

Software Defined Network				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		logical port, IPSets, computer OS Name, computer name, Active Directory		
SDN.REQ.005	Software Defined Network	The security policies in the virtualization layer must be tied to the application, which means whenever any application is moved from one virtualized server to another, even between different VLANs, the security policies should follow the application and there should be no need to redefine the security policies for the application at the new location. Also, when the application is deleted, all the security policies related to the application should also be remove		
SDN.REQ.006	Software Defined Network	The SDN solution should provide for automated delivery of virtual networking (micro segmentation), virtual Switching, virtual routing, virtual security services such as firewalling (EóW & NóS) and being software manageable.		
SDN.REQ.007	Software Defined Network	The SDN solution should support Layer-2 VPN allows you to extend your datacenter by allowing virtual machines to retain network connectivity across geographical boundaries		
SDN.REQ.008	Software Defined Network	Ability to provide micro-segmentation, security policies for a diverse workload environment containing on premises multi-hypervisor, containers, bare metal Server		

Software Defined Network				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		and multiple public clouds from a single console.		
SDN.REQ.009	Software Defined Network	The SDN solution should support distributed routing in-kernel with support of dynamic Routing and static Routing protocol including support for IPv6		
SDN.REQ.010	Software Defined Network	The SDN solution should have integrated distributed IDPS (Intrusion Detection & Prevention) functionality for East-West traffic.		
SDN.REQ.011	Software Defined Network	The bidder must propose East-West IDPS functionality with 2 Gbps throughput Per Nodes		

F. Cyber Security Applications

1. Anti-APT

Anti-APT				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
ANTIAPT.REQ.001	Anti APT	The solution should be able to communicate bi-directionally with the proposed NGFW, AntiSpam & End Point solution for automatic blocking/threat update		
ANTIAPT.REQ.002	Anti APT	The solution should support deep packet inspection of SSL encrypted traffic (including HTTPS) for both incoming and outgoing		
ANTIAPT.REQ.003	Anti APT	The quoted APT OEM must have NSS Lab's Recommended rating as per latest breach detection & prevention system report		
ANTIAPT.REQ.004	Anti APT	The solution should provide detection, analysis and remediation capability against APT & SSL based APT attacks.		

Anti-APT				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
ANTIAPT.REQ.005	Anti APT	The solution can be employed either on premise or on cloud, analysis engine using virtual execution to detect zero day and unknown threats and may or may not be signature based.		
ANTIAPT.REQ.006	Anti APT	The proposed solution should be able to detect and prevent advanced Malware, Zero-day attack, spear phishing attack, drive by download, watering hole and targeted Advanced Persistent Threat without relying on just Signature database.		
ANTIAPT.REQ.007	Anti APT	The proposed solution should perform dynamic real-time analysis of advanced malware to confirm true zero-day and targeted attacks. No file should be sent to third party systems or cloud infrastructure system for analysis and detection of Malware		

Anti-APT				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
ANTIAPT.REQ.008	Anti APT	The proposed solution should automatically detect and confirm multistage zeroday malware and targeted attacks without prior knowledge of the malware.		
ANTIAPT.REQ.009	Anti APT	The proposed solution should utilize a state-full attack analysis to detect the entire infection lifecycle and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration.		
ANTIAPT.REQ.010	Anti APT	The proposed solution should analyse advanced malware against a cross-matrix of different operating systems and various versions of pre-defined applications.		
ANTIAPT.REQ.011	Anti APT	The solution must support pre-populated Licensed copies of Operating systems and applications/softwares (like Microsoft Office). There should be no		

Anti-APT				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		requirement for the customer to buy additional license.		
ANTIAPT.REQ.012	Anti APT	The system should be able to support file sizes up to 100 mb or more		
ANTIAPT.REQ.013	Anti APT	The proposed solution should have the ability to analyse, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents, common multimedia contents not limited to such as JPEG/GIF/BMP/WMF and ZIP/RAR/7ZIP/TNEF archives to prevent advanced Malware and Zero day attacks.		
ANTIAPT.REQ.014	Anti APT	The proposed solution should capture, and store packet captures		

Anti-APT				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		of traffic relevant to the analysis of detected threats.		
ANTIAPT.REQ.015	Anti APT	The proposed solution should have the ability to display the geo-location of the remote command and control server(s) as an when possible considering the fact server hosting threat vectors use proxy servers/ VPN/ jump servers to camflouge their location, hence it is not always possible to get the correct geo location of the threst vector.		
ANTIAPT.REQ.016	Anti APT	The proposed solution should have the ability to report the Source IP, Destination IP, C&C Servers, URL, BOT name, Malware class, executable run, used protocols and infection severity of the attack.		
ANTIAPT.REQ.017	Anti APT	The proposed solution should be able to send both summary notifications and detailed per-event notifications utilizing the protocols (SMTP, or SNMP).		

Anti-APT				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
ANTIAPT.REQ.018	Anti APT	The proposed solution should have the ability to be deployed in out-of-band mode (also SPAN/TAP) & inline mode		
ANTIAPT.REQ.019	Anti APT	The proposed solution should be capable to block inbound malicious exploits delivered via a web channel and outbound call-back communications when deployed in inline, or out-of-band mode.		
ANTIAPT.REQ.020	Anti APT	The proposed solution should support SMB / CIFS / NFS protocol for sharing and transferring files		
ANTIAPT.REQ.021	Anti APT	The proposed solution should provide visibility into scan histories of each file scanned that are aborted, completed, or in progress.		
ANTIAPT.REQ.022	Anti APT	The solution should protect the endpoints against advanced threats including zero-day attacks, which target application vulnerabilities that have yet to be discovered or patched for minimum 500 users		

Anti-APT				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
ANTIAPT.REQ.023	Anti APT	The endpoint solution should be able to prevent attacks from known and unknown malwares		
ANTIAPT.REQ.024	Anti APT	The proposed solution should be able to analyse saved email (.eml) files for malicious attachments.		
ANTIAPT.REQ.025	Anti APT	The solution should provide reports in (but not limited to) PDF/CSV formats.		
ANTIAPT.REQ.026	Anti APT	The solution should have anti-evasion capabilities to prevent malwares detection of being run/executed in the virtualized environment.		
ANTIAPT.REQ.027	Anti APT	The solution should support for SIEM log integration.		
ANTIAPT.REQ.028	Anti APT	The solution should be able to schedule reports and also provide the flexibility to generate on-demand reports like daily/weekly/monthly/ yearly/specific range (day and time) etc.		

Anti-APT				
Sr.No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
ANTIAPT.REQ.029	Anti APT	Minimum number of Interfaces - 4x GE & 2 x 10G		
ANTIAPT.REQ.030	Anti APT	Number of VM's should be at least 24		
ANTIAPT.REQ.031	Anti APT	It should support Sandbox Analysis for multiple operating systems like Win7, Win8, Win10, Android, macOS etc		
ANTIAPT.REQ.032	Anti APT	High Availability & Maximum Scalability		
ANTIAPT.REQ.033	Anti APT	The solution should have dual AC power supply fully populated (within box) from day one		

2. SOAR Threat Intelligence Solution

Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
SOAR.REQ.001	General Requirement	SOAR Solution should have playbooks and workflow for automation and		

Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		orchestration with inbuilt Version control for Playbook's customization		
SOAR.REQ.002	General Requirement	SOAR Solution should have out of the box integration under following categories. Kindly provide detailed documentation of integrations and supported products as on date: Forensic tools like IT (e.g., AD, SAML), Communication tools (e.g., email, Slack), SIEM tools, Endpoint Security Solution, Network Security Solution, Web Proxy, Threat Intelligence, Dynamic malware analysis etc		
SOAR.REQ.003	General Requirement	SOAR Solution should support re-use playbooks in bigger playbooks (nested playbooks). Also. SOAR Solution Should allow creation of Manual Tasks and Automated Tasks in Playbooks. There should be		

Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		no restriction/licensing on the playbooks.		
SOAR.REQ.004	General Requirement	SOAR should have inbuilt features for security incident orchestration, Automation (SOA), case management, incident workflow (SIR), Threat intelligence platform and Threat Intelligence Process (TIP) to address the needs for a security operations centre.		
SOAR.REQ.005	General Requirement	SOAR Solution should support external users to contribute to an incident. It should provide free unlimited read only user licenses so that other departments such as helpdesk, Business team, IT, vendor etc. can comment/contribute to the investigation. Example - IT team can add comment whether an incident is true positive or remediation		

Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		updates without requiring any additional licenses.		
SOAR.REQ.006	General Requirement	SOAR should provide in-built threat intelligence (IOC) platform, feed unlimited structure, unstructured threat intelligence gathered from a combination of commercial, Open Source, user led, community, and industry driven and provide complete advisory of threats to plan countermeasures and proactive actions to reduce the risk. Solution should de-dupe, aggregate, normalize, enrich, and process threat intelligence in a holistic and actionable manner. the solution should be able to import threat intelligence in following formats - Structured / finished intelligence analysis reports (.txt, .pdf) - Automatically ingest email lists with threat information.		

Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		Automatically ingest email files (. mgs, .eml) with fully supported mailbox integration. ingest phishing emails using email forwarding to SOAR - Formatted CSV files, formatted MS office products - XML based structured intelligence - STIX, OPENIOC, Yara, TAXII - Provide a visual interface of threat data with a graphical map view of associated intelligence. - Automate indicator ingestion via application programming interface (API) - Ability to record time stamp on indicators, both creation and modification dates		
SOAR.REQ.007	General Requirement	MSI to provide documentary evidence for OOTB integrations.		

Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
SOAR.REQ.008	General Requirement	Proposed Solution should allow importing Indicators of Both structured and un-structured formats. Also, Solution should be able to do historical analysis and create relationships with existing incidents for the new IOC's.		
SOAR.REQ.009	General Requirement	Should support OOTB integration with 3rd party Vulnerability Management Tools (E.g., Tenable and Qualys) for a more proactive approach to security monitoring. SOAR should provide additional context by correlating vulnerability data with incident data gathered by other tools and threat intel within SOAR platform.		
SOAR.REQ.010	General Requirement	Should support all workflow and case management features. Below are minimum features - OOTB workflow templates for managing cases		

Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		- Full featured case management platform that can integrate with external systems - Automated tasks within cases such as executing playbooks - Ease to convert incident details into threat intelligence - Read/write workflow API for integrations or custom apps - Workflow playbook apps - Automated timeline generation for cases - Correlation of related cases		
SOAR.REQ.011	General Requirement	Solution should allow to create multiple dashboards for different purposes (SOC, IR, Threat Intel, etc.) Also, solution should have ability to provide complete audit trail.		
SOAR.REQ.012	General Requirement	Solution should allow creation and customization of playbooks. Below features are minimum requirement: -		

Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		-Integrated Playbook app development, test and simulation environment - Visually design, test, and deploy playbooks with drag and drop programmatic logic - clickable walkthroughs of playbook execution logs let you navigate through the process to assist debugging. - Support for dozens of 3rd party enrichment services and security defence products. - Orchestrate security tasks directly from your threat intelligence (automate upon change to intel or user action or external event) - Ingest and send threat intel and execute actions with any tool that has a supported API, even if not supported OOTB. - Automate data enrichment using playbooks and integrations with 3rd party apps.		

Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
SOAR.REQ.013	General Requirement	SOAR solution must provide out of the box at least 25 open-source threat intel feeds. SOAR Solution should support searching of Data/artifacts associated with historical incidents		
SOAR.REQ.014	General Requirement	Solution should have ability to prioritize playbook execution, so that in case of large incident queue critical events and associated actions are not delayed.		
SOAR.REQ.015	General Requirement	SOAR Solution should support adding of new product integrations from GUI without any interaction with command line. Also, Solution should support adding of new product integrations from GUI without any interaction with command line.		
SOAR.REQ.016	General Requirement	Store should collect and store evidence to ensure its applicability in the court of		

Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes or No)	Deviation
		law. Analyst should be able to attach artefacts like Log files, PCAP, exe files, to the incident.		
SOAR.REQ.017	General Requirement	SOAR should have Admin licenses for SOC staff at least 3 licenses		

3. Anti-DDOS

Anti-DDOS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
ADDOS.REQ.001	Appliance	The proposed dedicated Hardware device should support minimum 45 Gbps of throughput with up to 16 virtual instances. Should have internal redundant Power supply with 4 TB usable hard disk, 128 GB RAM.		
ADDOS.REQ.002	hardware Parameter	Appliance should support minimum 8 x 10G SFP+ ports all populated from day 1		
ADDOS.REQ.003	Performance	Should support minimum 20 MPPS & 500,000 Connections per second. It should support minimum 5 million L7 Requests per Sec. Device should support minimum 50K TPS on RSA 2K Key and 35K TPS on ECC		
		DDoS Protection		
ADDOS.REQ.004	DDoS features	Should protect TCP based attacks: TCP SYN Flood, TCP SYN-ACK Flood, TCP ACK Flood, TCP FIN/RST Flood , TCP Connection Flood ,TCP Slow Connection , TCP Abnormal Connection, TCP Fragments Flood, Défense WinNuke, TCP Error Flag		
ADDOS.REQ.005	DDoS features	Should protect UDP based attacks: UDP Flood, UDP Fragement Flood, UDP Fingerprint, Fraggle, UDP Large Packet		
ADDOS.REQ.006	DDoS features	Should protect HTTP & HTTPS based attacks: HTTP GET Flood, HTTP POST Flood, HTTP Slowloris, HTTP Slow POST, HTTP URL monitor, SSL Handshake, SSL Renegotiation		

Anti-DDOS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
ADDOS.REQ.007	DDoS features	Should protect DNS based attacks: DNS Cache Poisoning Defense, DNS Length Check Defense , DNS NxDomain Defense, DNS Query Flood Defense , DNS Reply Flood Defense, DNS TTL Check , DNS Source Authentication		
ADDOS.REQ.008	DDoS features	The solution should support Brute Force attack mitigation		
ADDOS.REQ.009	DDoS features	The solution should support the behaviour based DDOS mitigation.		
ADDOS.REQ.010	DDoS features	The solution should provide the traffic AUTO learning function for the DDOS traffic monitoring		
ADDOS.REQ.011	DDoS features	The traffic Auto learning threshold can be apply automatically after auto learning completed.		
ADDOS.REQ.012	DDoS features	The solution should provide the multi-level DDOS mitigation policy and different mitigation action based on DDOS traffic type.		
ADDOS.REQ.013	DDoS features	The solution should Access control list for IP, TCP, UDP, DNS, HTTP, URL, blacklist and whitelist,		
ADDOS.REQ.014	DDoS features	The solution should support Access control list based on inbuilt GeoIP with configurable duration.		
ADDOS.REQ.015	DDoS features	The solution should be able to import third party IP database through File or URL.		
ADDOS.REQ.016	IPv6 Dual Stack	The system should support IPv4 and IPv6 dual-stack without deteriorating performance		

Anti-DDOS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
ADDOS.REQ.017	High Availability	The solution shall have built-in high availability (HA) features in the following mode: Active-Passive, Active-Active using standard VRRP or equivalent		
ADDOS.REQ.018	Architecture	The solution shall be able to immediately support both IPv4 and IPv6, and implements dual stack architecture.		
ADDOS.REQ.019		The solution shall be able to support IPv4 & IPv6 routing protocols for traffic mitigation: Static Routing, OSPF Routing, BGPv4 Routing and Policy Based routing.		
ADDOS.REQ.020		The solution must be able to integrate with existing management system via SNMP version 3 and SNMP version 2		
ADDOS.REQ.021	Management	The solution must provide the latest Management Information Base (MIB) file for SNMP operation. Should support High Active/Active and Active/Passive High availability using open standard VRRP		
ADDOS.REQ.022		The solution log shall contain the following information: Attack logging like Source IP, Destination IP, Destination Port, Group Name, Service Name, Protocol Attack Type, Action , Anomaly Count, DDoS Attack and logging to Syslog		
ADDOS.REQ.023		The solution shall provide the flexibility of performing configuration via GUI and command base remotely.		
ADDOS.REQ.024		The solution shall be able to export syslog to existing syslog server and SIEM system.		

Anti-DDOS				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
ADDOS.REQ.025		The solution shall be able to support user authentication based on Local Password, RADIUS & TACACS+		
ADDOS.REQ.026		The solution shall support the provisioning of the reports - Attack reports -top sources, targets, attack type, Attack Severity Distribution, Attack Source Region		
ADDOS.REQ.027	Reporting	The solution must be able to generate summary attack report of daily/weekly/monthly		
ADDOS.REQ.028	Reporting	The solution must provide packet capture for debugging.		
ADDOS.REQ.029	Reporting	The solution must support the generation of pdf reports containing the detailed statistics and graphs		

4. Patch Management Solution

Patch Management Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
Patch Management				
PMS.REQ.001	Patch Management	The Solution should have ability to throttle bandwidth		
PMS.REQ.002	Patch Management	The solution should support local distribution points through preferred servers and endpoints and also peer downloading		

Patch Management Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
PMS.REQ.003	Patch Management	The Agents able to dynamically connect to the next nearest Distribution Point if the Distribution Point assigned to the agent is not available.		
PMS.REQ.004	Patch Management	The solution should prevent users with admin rights to uninstall the agent (The solution should be uninstalled only by the central administrator of the inventory management)		
PMS.REQ.005	Patch Management	The Solution should be able to hide the agent from the Desktops “Add/Remove Program” list from the central console.		
PMS.REQ.006	Patch Management	The Solution should have ability to track standalone executable based applications on each computer i.e. Applications that do not need to be installed but just needs to execute a standalone program. (Standalone applications/ executable/ portable programs needs to be tracked by the system)		
PMS.REQ.007	Patch Management	The solution should provide desktop admins capability to take remote control of endpoints for maintenance purposes. This feature should support copying files, removing files to/ from remote devices, should support HTML Remote capabilities		
PMS.REQ.008	Patch Management	The solution should have the ability to configure machines in all power saving		

Patch Management Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		modes (performance/ balanced/ power saving) for supported OS.		
PMS.REQ.009	Patch Management	The solution should be able to remove unauthorized, unlicensed software or any software installed in the endpoints and servers as required.		
PMS.REQ.010	Patch Management	The solution should have ability to execute a script before and/or after installation. It should also support custom script-based execution. Script should be provided by the bidder.		
PMS.REQ.011	Patch Management	The solution should support multi-task distribution of software/patches for wide scale distribution.		
PMS.REQ.012	Patch Management	The Solution must include agent software that is deployed on all managed devices having OS (All flavours of Windows Server and End points with supported OS. HP-UX Solaris, IBM, AIX, Linux Red Hat (Desktop, Enterprise) versions).		
PMS.REQ.013	Patch Management	The Solution must provide a remote agent deployment utility for installing agents remotely. The tool should be able to use Active Directory and Local Administrator Authentication for deploying agents to remote computers.		
PMS.REQ.014	Patch Management	The agent deployment strategy should also consider use of the following agent deployment methods:		

Patch Management Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
PMS.REQ.015	Patch Management	a. Active Directory Group Policies to deploy agents at domain login		
PMS.REQ.016	Patch Management	b. login scripts to deploy agents at domain login		
PMS.REQ.017	Patch Management	c. Use of existing 3rd party software distribution tools as available.		
PMS.REQ.018	Patch Management	d. Manually installing the agent where no other methods succeed.		
PMS.REQ.019	Patch Management	The agent should be configurable for quiet periods in which no work is done and with throttling features at client and Server sides (should above run at pre-defined times).		
PMS.REQ.020	Patch Management	The Agent should be able to coexist with other end point clients like antivirus, DLP , Application whitelisting Solutions etc.		
PMS.REQ.021	Patch Management	Solution should be able to do assessment for currently deployed patches and scope to deploy latest patches on all the endpoints/ Servers (All flavours of Windows Server and End points with supported OS. HP-UX, Solaris, IBM,AIX, Linux Red Hat (Desktop, Enterprise)		
PMS.REQ.022	Patch Management	Able to identify and report the machines (servers and endpoints) that have installed the patch that is to be rolled back. The offered solution should		

Patch Management Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		support rollback of patches and service packs applied.		
PMS.REQ.023	Patch Management	Able to determine if the patches on a machine (servers and endpoints) are correctly installed.		
PMS.REQ.024	Patch Management	Allow console user to deploy patches to all agents via a central console.		
PMS.REQ.025	Patch Management	Allow console user to set start and end date/time for each action deployed.		
PMS.REQ.026	Patch Management	Allow console user to define different patch deployment policies.		
PMS.REQ.027	Patch Management	The system must be intelligent to check the relevance of the computer before deploying a patch after download on the endpoints and servers.		
PMS.REQ.028	Patch Management	The solution should support integration with other security solutions such as SIEM and SOAR		
PMS.REQ.029	Patch Management	The solution should be able to provide audit reports to help in compliance with Patching requirements.		
PMS.REQ.030	Patch Management	The solution must be capable of using existing client computers as distribution points at remote sites without the need for allocating dedicated servers.		
PMS.REQ.031	Patch Management	The Patch management solution should support the range of applications other than Operating System Patches like Mozilla, Java, Chrome, and MS Office		

Patch Management Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		etc. to apply the appropriate patches released by the respective OEMs.		
PMS.REQ.032	Patch Management	The offered solution should support the event-driven remediation i.e. automatically initiate the process on receipt of a critical patch.		
PMS.REQ.033	Patch Management	The Patch Management solution should have the capability for Remediation i.e. Continuously deploy, monitor, detect and enforce patch management policies.		
PMS.REQ.034	Patch Management	The solution should support granular control over re-boot process after patch deployment like prompting user, allowing user to differ, rebooting immediately if no one has logged on, etc		
PMS.REQ.035	Patch Management	The solution must be able to provide real-time (within minutes) patch deployment status monitoring. It must allow console operators to deploy multiple patches at one time without the need to restart the computers.		
PMS.REQ.036	Patch Management	The solution should have capability to corelate cve to patch		
PMS.REQ.037	Patch Management	The solution should have capability to collect patch impact analysis from pilot group or broken application status after deployment of patches		

Patch Management Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
PMS.REQ.038	Patch Management	The solution should have automated workflow to do pilot group testing and then release to production		
PMS.REQ.039	Patch Management	The solution should have capability to download only selected os and third-party content		
PMS.REQ.040	Patch Management	The solution should have capability to create own content for patch management		
PMS.REQ.041	Patch Management	The solution should have capability to do Third party Software distributions for hybrid platforms		
PMS.REQ.042	Patch Management	The solution should have capability to do OS Provisioning on bare metal systems		
PMS.REQ.043	Patch Management	The solution should have capability to create customized queries based on the hardware and software inventory		
PMS.REQ.044	Patch Management	The solution should have capability to filter patches based on different parameters		
PMS.REQ.045	Patch Management	The solution should have capability to provide ability to distribute software through self-portals		
PMS.REQ.046	Patch Management	The solution should be able to customize notifications displayed on client systems		
PMS.REQ.047	Patch Management	The solution should integrate with Active directory		

Patch Management Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
PMS.REQ.048	Patch Management	The solution should haverole-basedd access control to manage the centralized console		
PMS.REQ.049	Patch Management	The solution should be able to do Software license metering		
PMS.REQ.050	Patch Management	The solution should be able to keep track of changed being done to hardware and software		
PMS.REQ.051	Patch Management	The solution should be able to manage remote users		
PMS.REQ.052	Patch Management	The solutions should able to import scap content		
PMS.REQ.053	Patch Management	The solutions must have ability to test patches before being deployed in production		
PMS.REQ.054	Patch Management	The solutions must validate the patches being downloaded in order to avoid MITM attack		
Software Distribution				
PMS.REQ.055	Software Distribution	The solution should support deployment on windows, Linux & Mac		
PMS.REQ.056	Software Distribution	The solution should spport deployment using powershell, batch, msi etc		
PMS.REQ.057	Software Distribution	The solution should be able to choose run as option while deploying software's silently		
PMS.REQ.058	Software Distribution	The solution should be able to uninstall applications automatically if reclaimed using software license metering		

Patch Management Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
OS Provisioning				
PMS.REQ.059	OS Provisioning	The solution support OS provisioning on Windows & Mac OS		
PMS.REQ.060	OS Provisioning	The solution should be capable of capturing image of existing OS		
PMS.REQ.061	OS Provisioning	The solution should include relevant drivers during deployment as per the hardware model		
PMS.REQ.062	OS Provisioning	The solution should support offline as well as online method		
PMS.REQ.063	OS Provisioning	The solution should support template-based provisioning		
Remote Control				
PMS.REQ.064	Remote Control	The solution should support seek permissions of the end user before taking remote		
PMS.REQ.065	Remote Control	The solution should support HTML as well as legacy remote control without depending on third party or without using windows rdp method		
PMS.REQ.066	Remote Control	The solution should support role-based access to take remote		
PMS.REQ.067	Remote Control	Help desk team should be allowed to connect even if does not have access to centralised server		
PMS.REQ.068	Remote Control	The solution should support copy, upload, remote execute & chat functionally out of box		

Patch Management Solution				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
PMS.REQ.069	Remote Control	The solution should support customization of remote-control settings to different groups		
PMS.REQ.070	Remote Control	The solution should keep audit trail for remote connections		
Reporting				
PMS.REQ.071	Reporting	The solution should support customization of reports		
PMS.REQ.072	Reporting	The solution should have Business intelligence tool to create customized reports and dashboards		
Inventory				
PMS.REQ.073	Inventory	The solution should support customized wmi & registry attributes if required to collect additional data in inventory		
PMS.REQ.074	Inventory	The solution be able to run & create multiple queries based on different attributes		
PMS.REQ.075	Inventory	The solution should keep track of inventory history		
PMS.REQ.076	Inventory	The solution should have ability to remotely troubleshoots the endpoints		
PMS.REQ.077	Inventory	The solution should be able to see running processes, services, events of remote systems		
PMS.REQ.078	Inventory	The solution should support alert mechanism		
PMS.REQ.079	Inventory	The solution should support customization of columns		

5. End Point Security

End Point Security				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EPS.REQ.001	End Point Security	Endpoint should have behavioural-based detection technology protects against zero-day file-less attacks that target applications with zero day or un-patched vulnerabilities		
EPS.REQ.002	End Point Security	The solution should Protects against zero-day attacks targeting undiscovered or un-patched application vulnerabilities		
EPS.REQ.003	End Point Security	The solution should Detects various memory techniques used in an exploit, such as ROP, HeapSpray, buffer overflow		
EPS.REQ.004	End Point Security	Endpoint should protect Shields web browsers, Java/Flash plug-ins, Microsoft Office applications, and PDF Reader		

End Point Security				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EPS.REQ.005	End Point Security	Simplified management and policy enforcement with Enterprise Management Server		
EPS.REQ.006	End Point Security	Endpoint features including compliance, protection, and secure access into a single, modular lightweight client		
EPS.REQ.007	End Point Security	The solution should Windows AD Integration helps sync organizations AD structure into EMS so same OUs can be used for endpoint management.		
EPS.REQ.008	End Point Security	The proposed system shall be able to queries a real time database of over 100 million + rated websites categorized into 70+ unique content categories.		
EPS.REQ.009	End Point Security	Real-time Endpoint Status always provides current information on endpoint activity & security events.		
EPS.REQ.010	End Point Security	Should support Endpoint Quarantine to quickly disconnect a compromised endpoint from the network and stop it from infecting other assets.		
EPS.REQ.011	End Point Security	Should support Automated Response to detect and isolate suspicious or compromised endpoints without manual intervention		

End Point Security				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
EPS.REQ.012	End Point Security	Vulnerability Dashboard to manage organizations attack surface. All vulnerable endpoints are easily identified for administrative action.		
EPS.REQ.013	End Point Security	Solution should have capability to submit unknown files to sandboxing for simulation on real time basis as per sandboxing analysis and revert back to Endpoint security solution to block and clean threats and sandboxing solution.		

6. Intrusion Prevention system (IPS)

Intrusion Prevention system				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
NIPS				
IPS.REQ.001	NIPS	The IPS should be a Dedicated purpose-built hardware, NOT a part of Firewall module or UTM solution with Real World Throughput of 10 Gbps and scalable up to 30 Gbps for future requirement on the same platform. Should		

Intrusion Prevention system				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		also support on-box SSL throughput of 10 Gbps scalable to 25 Gbps.		
IPS.REQ.002	NIPS	The NIPS solution should provide 4-port 10 GigE RJ-45 ports and 2-port 40 GigE SR & 2 Port 100-Gig Optical ports (modules as per design) with in-built fail-open from Day 1.		
IPS.REQ.003	NIPS	Deployment Modes supported: In-line; SPAN Port Monitoring		
IPS.REQ.004	NIPS	Should support 20,000 minimum signatures out of box & all the signatures update subscription should be provided from Day1		
IPS.REQ.005	NIPS	The NIPS solution should provide for resistance to IPS evasion and protection from anti-NIPS techniques using countermeasures like Packet reassembly, Stream reassembly, Fragment reassembly, Traffic normalization and Anti-spoofing		
IPS.REQ.006	NIPS	Block Actions: Drop packet, TCP Reset, Quarantine, Alert.		
IPS.REQ.007	NIPS	The proposed solution must support the following Network-wide protections:		

Intrusion Prevention system				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IPS.REQ.008	NIPS	DoS Protection—Protection against Volume-based Denial-of-Service attacks including SYN Floods, TCP Floods, UDP floods, ICMP and Application-level flood.		
IPS.REQ.009	NIPS	Vulnerability-based DoS attacks—Protection against any type of Teardrop attack, Ping of Death attack and Land attack.		
IPS.REQ.010	NIPS	DNS Protection—Protection against DNS query floods.		
IPS.REQ.011	NIPS	Signature-based Protection—Protection against known application vulnerabilities, and common malware, such as worms, trojans, spyware, and DoS.		
IPS.REQ.012	NIPS	Packet-Anomaly Protection		
IPS.REQ.013	NIPS	Self- learning capability — Should have capability to monitor the network traffic and develops a baseline profile. It should have the ability to constantly update this profile to keep an updated view of the network		

Intrusion Prevention system				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IPS.REQ.014	NIPS	Control traffic based on geographical locations -- For e.g., a policy can be created to block traffic coming or going to a particular country. Provision should be there to allow specific IPs for any blocked country		
IPS.REQ.015	NIPS	Blacklist rules and Whitelist rules-- Block or allow traffic to or from specified networks, based on protocols, applications, and other criteria.		
IPS.REQ.016	NIPS	The solution should support malware protection by performing file reputation analysis of malicious files.		
IPS.REQ.017	NIPS	The solution should have the ability to scan malware within files such as PDF using emulation techniques and block only if pdf files with java scripts are malicious.		
IPS.REQ.018	NIPS	The NIPS should support detection of malicious flash files using heuristic analysis rather than signatures. The NIPS should detect various flash exploitation techniques such as Vector Spraying, presence of shell code, and similar exploitation techniques.		

Intrusion Prevention system				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IPS.REQ.019	NIPS	Solution should integrate bi-directionally with proposed endpoint security suite to provide integrated reporting and host threat impact to include client forensics such as IP address, OS version, MAC address, logged in user, deployed security products, and current host threat detections		
IPS.REQ.020	NIPS	The NIPS solution should be application aware and should identify over 2000 Layer 2 through 7 applications and protocols and associate those applications with detected attacks		
IPS.REQ.021	NIPS	The NIPS solution should provide an advanced botnet detection framework that should use a probabilistic zero-day botnet detection approach. It should consist of multiple heuristics identified during the research and analysis of various bots. The NIPS solution should detect and cover anomalies in protocols being used for communication such as HTTP and SSL, response errors in protocols such as DNS and SMTP, suspicious behaviours such as port		

Intrusion Prevention system				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		scans and stealth scans, File Reputation, and IP Reputation		
IPS.REQ.022	NIPS	High Availability: The solution should provide failover among devices for all components and should be completely automatic without any sort of manual intervention. The solution must support Active-Failover and Active-Active architecture and high availability options for redundancy without using any third-party software		
IPS.REQ.023	Security Reporting and Management	The proposed solution must have historical security reporting solution, which provides the following:		
IPS.REQ.024	Security Reporting and Management	Customizable dashboards, reports, and notifications		
IPS.REQ.025	Security Reporting and Management	Centralized Management Solution should have capability of high availability at site level for enabling DR deployment		

Intrusion Prevention system				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IPS.REQ.026	Security Reporting and Management	Customized reports on HTML, CSV, and PDF format etc.		
IPS.REQ.027	Security Reporting and Management	Management system should provide detailed Event analysis for IPS and should provide Syslog output.		
IPS.REQ.028	Security Reporting and Management	Solution Audit Trail should contain at a minimum the name of the administrator making the change and the change made		
IPS.REQ.029	Security Reporting and Management	The management system should have no limit to the number of administrators that can be active in the management console concurrently		
IPS.REQ.030	Support Requirement	The solution should be proposed with Premium Support		
IPS.REQ.031	Support Requirement	The OEM Engineering and support should be based out of India		
IPS.REQ.032	Support Requirement	The OEM should provide a utility to collect product and system information to assist Support in diagnosing issues		

Intrusion Prevention system				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IPS.REQ.033	Support Requirement	Product upgrades should be easily be downloadable from the OEM Official Website		
IPS.REQ.034	Support Requirement	The OEM should provide a service which delivers the latest OEM product information by email — patch and upgrade notification; and critical alerts that require immediate attention.		
HIPS				
IPS.REQ.035	HIPS	The solution should offer next generation antivirus with machine learning and application containment, firewall, threat intelligence, Application Control, File Integrity monitoring and Change Control, HIPS/Threat Prevention, Network Visibility and Micro-Segmentation based firewall, Virtualisation Security, and cloud workload solutions in a single agent functionality to ensure optimal security and compliance for critical servers.		
IPS.REQ.036	HIPS	The solution should be managed from a single centralized console.		

Intrusion Prevention system				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IPS.REQ.037	HIPS	The solution should have a small overhead footprint such that it minimizes impact on system resource		
IPS.REQ.038	HIPS	The proposed solution should provide centralised management with key capabilities to manage physical, virtual, and cloud deployments for better security control, including policy management, deployment, visibility, and security management across all platforms.		
IPS.REQ.039	HIPS	The solution should offer True zero-day protection using a combination of signature based and behavioural malware detection powered by Machine Learning, along with application containment, Application and change control, File integrity monitoring for zero-day malware prevention.		
IPS.REQ.040	HIPS	Server security agent must support all mentioned platform Windows server (2008, 2008R2, 2012, 2012R2, 2016), RHEL (6.2,7.9, 7.4), Hyper V, VMWare, Open Stack to secure workloads regardless of where it		

Intrusion Prevention system				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		resides and can protect legacy systems that cannot be patched		
IPS.REQ.041	HIPS	The solution should be able to block unauthorized changes to critical system files, directories, and configurations		
IPS.REQ.042	HIPS	The solution should detect and imports virtual infrastructure details, security groups, and virtual networks along with control over public/private loud infrastructure and insight into the threat information across on-prim datacentres as well as public/private clouds		
IPS.REQ.043	HIPS	The solution should protect against system misconfigurations		
IPS.REQ.044	HIPS	Server Security solution should have HIPS/Threat Prevention controls to restrict application and operating system behaviour using policy-based least privilege access control.		
IPS.REQ.045	HIPS	Server agent must prevent malicious applications from inserting code into trusted applications. The HIPS, Threat Prevention, File Integrity monitoring, Host based firewall,		

Intrusion Prevention system				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		Application Control should be offered using a single agent.		
IPS.REQ.046	HIPS	The solution should provide the dynamic management of execution capability of applications on a server system, prevent unauthorized registry manipulation and in memory protection of application		
IPS.REQ.047	HIPS	The solution apart from allowing only authorised applications to run, should block any changes from being done to authorized applications, like DLL's, System files, registry etc., thus providing application treat protection		
IPS.REQ.048	HIPS	It should prevent execution of all unauthorized software, scripts, and dynamic-link libraries (DLLs) and further defends against memory exploits		
IPS.REQ.049	HIPS	The solution should provide for a real time capability to prevent execution of any authorized application to execute on the server system		
IPS.REQ.050	HIPS	The Solution should ensure that Only authorized software / applications / executable		

Intrusion Prevention system				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		codes are allowed to run and provides tamper protection to them.		
IPS.REQ.051	HIPS	Solution should be capable of creating whitelist for each system dynamically and no manual intervention in creating this list.		
IPS.REQ.052	HIPS	Each whitelist created should be unique to each system and should not be a common list		
IPS.REQ.053	HIPS	The solution should enable the user to self-approve any new application / software with business justification. So that new application can be run successfully with notification to administrator.		
IPS.REQ.054	HIPS	Solution should allow administrator to approve or revoke self-approved application status so that new application can be allowed to run or ban.		
IPS.REQ.055	HIPS	Solution should consider executables, ActiveX, Java, Perl scripts, bat files, VBS files, com files, dll files, sys files while creating the whitelist.		

Intrusion Prevention system				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IPS.REQ.056	HIPS	The proposed change control solution shall support Real-time Change Tracking of files and registry. Audit log should Include File, User information, Program name and contents that have changed		
IPS.REQ.057	HIPS	The proposed Change control solution should be capable of change monitoring as well as control / prevention.		
IPS.REQ.058	HIPS	In the Event of unauthorized file change, the proposed solution shall report WHAT changed, WHO made the change, HOW they made it and precisely WHEN they did so		
IPS.REQ.059	HIPS	The solution should offer intelligent filters which are pre-configured to track the relevant objects on the system, for each standard Operating System covering systems files including Windows, Solaris, HPUX, Linux and AIX. It should also include application filters for Apache, Tomcat, WebSphere and JBOSS, IIS, WebLogic, WebSphere, etc., and should be customizable.		

Intrusion Prevention system				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IPS.REQ.060	HIPS	Solution should provide options to authorise processes and users who can make changes to log files and pre identified files		
IPS.REQ.061	HIPS	Solution should offer granular read, read-write, or no access to identified process or users		
IPS.REQ.062	HIPS	The server security module should support Signature as well as behavioural based detection		
IPS.REQ.063	HIPS	Server security should support policies creation based on – User defined, Adaptive mode and Learn mode		
IPS.REQ.064	HIPS	Server Security should support firewall capabilities to directly block unwanted traffic		
IPS.REQ.065	HIPS	Server security solution should provide facility to create User defined signatures		
IPS.REQ.066	HIPS	Server security solution should provide protection from known attacks like – SQL injection, Cross Site scripting, Buffer Overflow without having signature updates		

Intrusion Prevention system				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IPS.REQ.067	HIPS	Server security solution should provide vulnerability shielding to the application not having patches installed		
IPS.REQ.068	HIPS	The Proposed Solution should offer virtualization security that offloads scanning, configuration, and .DAT update operations from individual guest images to an offload scan server within the premises		
IPS.REQ.069	HIPS	The solution should build and maintain a global cache of scanned files to ensure that once a file is scanned and confirmed to be clean, subsequent VMs accessing the file won't have to wait for a scan.		
IPS.REQ.070	HIPS	Should allow separate policies for on-access and on-demand scanning to enable fine-tuned security execution		
IPS.REQ.071	HIPS	Should provide Connector for VMware vSphere provides a complete view into virtual data centres and populates key properties such as servers, hypervisors, and VMs through the same management console.		

Intrusion Prevention system				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IPS.REQ.072	HIPS	The Solution should provide administrators gain visibility into the security status of all VMs and can monitor hypervisor-to-VM relationships in near real time.		
IPS.REQ.073	HIPS	The solution should provide for deep visibility, risk assessment, and remediation for hybrid cloud		
IPS.REQ.074	Management	The solution should be able to manage Endpoint Protection, server security and DLP including encryption from a single management console.		
IPS.REQ.075	Management	Solutions should support report customization and allow viewing directly using a web browser and also as a dashboard using the same management console for Endpoint Protection, server security and DLP including encryption		
IPS.REQ.076	Management	It should be able to deploy, manage, and update agents and policies from one management platform.		
IPS.REQ.077	Management	The centralized management solution should provide centralized Incident Management and		

Intrusion Prevention system				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		Reporting for Endpoint Protection, server security and DLP including encryption.		
IPS.REQ.078	Management	The management console should support hierarchical grouping of machines and policy deployment. The grouping could be based on IP Address of a subnet of machines or a particular site.		
IPS.REQ.079	Management	The management console should support use of Active Directory accounts and groups to manage roles		
IPS.REQ.080	Management	Solutions should provide near real-time event monitor allowing you to see events as they happen, view details (user, machine, rules triggered, etc), and even access evidence files as the events happen in your environment.		
IPS.REQ.081	Management	The management console should be able to automatically report about the new unprotected system connecting on the network		
IPS.REQ.082	Management	Solution should provide for custom reports and queries along with role-based access		

Intrusion Prevention system				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
		providing different levels of dash-boarding and relevant reports to users.		
IPS.REQ.083	Management	The management console should provide actionable reports		
IPS.REQ.084	Management	The management console should provide Reports in CSV, HTML,PDF and Excel Format		
IPS.REQ.085	Management	The solution should be able integrate with third party ticket management solution		
IPS.REQ.086	Management	Solution should provide the capability to log administrative activities in the Management console. Administrative activities that are logged in the Management console include, changes to policies, deployment of policies, agent override activities, agent termination, and agent uninstall key generation.		
IPS.REQ.087	Management	Solution should support ability to restrict access to company approved devices, but also if necessary, to permit exclusions to this requirement. Exception and/or exclusions can be designed to accommodate different devices or different groups of users		

Intrusion Prevention system				
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Compliance (Yes or No)**	**Deviation**
IPS.REQ.088	Management	Solution should provide the functionality of events being viewed, filtered, and sorted in the Management console, allowing security officers or administrators to view events and respond quickly. If applicable, suspicious content is attached as evidence to the event.		
IPS.REQ.089	Management	Solution should provide the functionality of logging and audit-trail capabilities.		

7. User Behaviour Analysis System

User Behaviour Analysis System				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
UBA.REQ.001	User Behaviour Analysis	Solution should be focused on supervised or unsupervised machine learning.		
UBA.REQ.002	User Behaviour Analysis	At a minimum, solution should support detection of anomalies for authentication, File Access, and Account Management (aka Active Directory) logs		

User Behaviour Analysis System				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
UBA.REQ.003	User Behaviour Analysis	Solution should have capability to reduce false positive reduction		
UBA.REQ.004	User Behaviour Analysis	Solution should support user-based behaviour analytics		
UBA.REQ.005	User Behaviour Analysis	Solution should be able to support behaviour profiling of at least 1000 users from day one		
UBA.REQ.006	User Behaviour Analysis	Solution should be focused on supervised or unsupervised machine learning.		
UBA.REQ.007	User Behaviour Analysis	The solution should support real-time monitoring of a. Abnormal Multiple privilege group membership changes b. Account Management Change Anomaly c. Multiple Account Management Changes Anomaly d. Abnormal Active Directory Change Time Anomaly e. Multiple Failed Active Directory Changes Anomaly f. Multiple Failed Privileged Group Membership Changes Anomaly g. Abnormal Admin Password Changes h. User Time, Access at Unusual Times i. Abnormal Multiple Failed Authentications j. User logged into multiple hosts k. User logged to abnormal hosts l. Abnormal Site/Domain Access m. Abnormal computer accessed remotely n. Mass File Renames o. Abnormal File Access		

User Behaviour Analysis System				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		p. Compromised account / system / host & device detection Mass q. Changes to groups r. Multiple logons anomaly s. Multiple files deleted t. Abnormal file access time u. Multiple file access times changed v. Multiple files moved to/from a shared drive w. Multiple folder permission changes		
UBA.REQ.008	User Behaviour Analysis	Solution should be able to track user's activities locally and remote network sites and should be able to report usage behaviour across the entire network.		
UBA.REQ.009	User Behaviour Analysis	Solution should have facility to assign risk and credibility rating to events.		
UBA.REQ.010	User Behaviour Analysis	Solution should support Machine Learning (ML) driven risk scores and risk profiles for user		
UBA.REQ.011	User Behaviour Analysis	Solution should not be app based or plugin based and should be dedicated machine learning engine running on appliance or Virtual machine.		
UBA.REQ.012	User Behaviour Analysis	Enabling UBA should have zero impact on EPS consumption		
UBA.REQ.013	User Behaviour Analysis	Solution must not be rule-dependent		

8. Zero Trust Network Access

Zero Trust Network Access				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
Security Service Edge (SSE) Technical Specifications				
SSE.REQ.001	Common SSE Platform Features	The proposed SSE Solution must have at least 3x Compute Edge DC's / POPs / Locations in India to cater DC, DR and NDR scenarios.		
SSE.REQ.002	Common SSE Platform Features	The SSE solution shall support minimum of 1000 users from day 1 with five-year subscription / license / support and should have flexibility to scale up to 5000 users in future with additional software / subscription license. In case of hardware-based solution, scalability needs to be provisioned from day 1 and should not require any additional hardware in future.		
SSE.REQ.003	Common SSE Platform Features	The SSE solution must not have a single point of failure at each Compute Edge DC's / POPs / Locations from day 1 and should have seamless failover transparently to DR/ NDR (running with same full scale & specified features) if primary site goes down. All features should be available with full scale for roaming user environment (when users are outside of the office).		

Zero Trust Network Access				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
SSE.REQ.004	Common SSE Platform Features	The SSE solution must be able to integrate with on-premise AD without any exposure to inbound rules in Firewall.		
SSE.REQ.005	Common SSE Platform Features	The SSE solution must be able to create users based on domains /emails and allow users to create their own passwords.		
SSE.REQ.006	Common SSE Platform Features	The SSE solution must be able to integrate with SAML 2.0 (Azure AD, OKTA and ADFS etc.).		
SSE.REQ.007	Common SSE Platform Features	All 3x Compute Edge DC's / POPs in India must be peered with Microsoft and Google to ensure better end user experience.		
SSE.REQ.008	Common SSE Platform Features	The SSE solution should have single user agent for all the features (SWG, CASB, ZTNA, FWaaS and RBI etc.) and must be of < 20 MB in size.		
SSE.REQ.009	Common SSE Platform Features	The SSE solution should have a single management / admin console for all the features (SWG, CASB, ZTNA, FWaaS and RBI etc.).		
SSE.REQ.010	Common SSE Platform Features	The SSE solution admin console access must be able to restrict from known customer IP locations only.		
SSE.REQ.011	Common SSE Platform Features	The SSE solution should have device posture validation across multiple parameters like Device Encryption, Registry Check, Process Check, AD Domain Check, OPSWAT and Certificates etc to provide specific URL or Internet Access based on granular policy controls.		

Zero Trust Network Access				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
SSE.REQ.012	Common SSE Platform Features	The SSE solution must have HTTP/2 support from day 1		
SSE.REQ.013	Common SSE Platform Features	The SSE solution must have 99.999% uptime SLA.		
SSE.REQ.014	Common SSE Platform Features	The SSE solution must have in-built data retention of at least 90 days from day 1.		
SSE.REQ.015	Common SSE Platform Features	The SSE solution should have in-built data lake for granular interactive customized reporting across all features (SWG, CASB, ZTNA, FWaaS and RBI etc.) from a single admin console.		
SSE.REQ.016	Common SSE Platform Features	The SSE Platform must also provide threat intel exchange platform to integrate with customer environment existing security stack such as EDR Solutions, Threat intel exchange solution, SIEM solutions, SSO solutions etc from day 1.		
SSE.REQ.017	Common SSE Platform Features	The SSE solution must have <10 ms of latency for 95th Percentile of Hourly Round-Trip Processing non-decrypted (HTTP) traffic.		
SSE.REQ.018	Common SSE Platform Features	The SSE solution must have <50 ms of latency for 95th Percentile of Hourly Round-Trip Processing encrypted (HTTPS) traffic.		
SSE.REQ.019	Common SSE Platform Features	The SSE solution should have direct OEM 24x7x365 Support with 30 Minutes response time for P1 tickets from day 1.		
SSE.REQ.020	Common SSE Platform Features	The proposed SSE solution should be from Leading OEM.		
Internet & SaaS Apps				

Zero Trust Network Access				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
SSE.REQ.021	Internet & SaaS Apps	The proposed solution must be able to inspect TLS 1.3 SSL inspection from day 1		
SSE.REQ.022	Internet & SaaS Apps	The proposed solution should be able to provide 125+ web categories and should have capability to enforce granular activity control (should not be limited to allow or block) on web categories as required.		
SSE.REQ.023	Internet & SaaS Apps	The proposed solution be able to cover Webmail Category should not be limited to only allow or block but should also support these activities: Browse, Create, Delete, Delete All, Download, Edit, Invite, Login Attempt, Login Failed, Login Successful, Logout, Mark, Move		
SSE.REQ.024	Internet & SaaS Apps	The proposed solution should be able to cover File Sharing / Cloud storage category should not be limited to only allow or block but should also support these activities: App to App, Browse, Create, Delete, Delete All, Download, Edit, Follow Invite, Join, Login Attempt, Login Failed, Login, Successful, Logout, Mark, Move, Post, Print, Search, Send, Share, Sign, Unshare, Upload, View, View All.		
SSE.REQ.025	Internet & SaaS Apps	The proposed solution should be able to cover Collaboration category should not be limited to only allow or block but should also support these activities: App to App, Browse, Create, Delete, Delete All, Download, Edit, Flag, Follow, Invite, Join, Login Attempt, Login Failed, Login Successful, Logout, Mark,		

Zero Trust Network Access				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		Move, Post, Receive, Search, Send, Share, Stop, Terminate, Unblock, Upload, View, View All		
SSE.REQ.026	Internet & SaaS Apps	The proposed solution should be able to cover IAAS Category for the AWS/Azure and GCP should not be limited to only allow or block but should also support these activities: Approve, Attach, Browse, Create, Delete, Detach, Download, Edit, Invite, Login, Attempt, Login Failed, Login Successful, Logout, Move, Post, Publish, Reboot, Share, Start, Stop, Upload, View, View All,		
SSE.REQ.027	Internet & SaaS Apps	The solution should also support real-time visibility for 40000+ sanctioned and unsanctioned applications with risk score based on CSA and CSS Standards.		
SSE.REQ.028	Internet & SaaS Apps	In addition to URL policies, the solution should have granular access policies based on applications risk scores.		
SSE.REQ.029	Internet & SaaS Apps	The solution has capability to provide User and Entity Behaviour Analysis (UBEA) profiling and risk score for users based on parameters like data exfiltration, locations awareness, bulk upload and download of files, bulk deletion of files, login-failures etc.		
SSE.REQ.030	Internet & SaaS Apps	The solution should have targeted user-agent protection and true file type analysis.		
SSE.REQ.031	Internet & SaaS Apps	The solution should have CSA STAR , ISO 27000 series and SOC certifications.		

Zero Trust Network Access				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
SSE.REQ.032	Internet & SaaS Apps	The proposed solution must be able to integrate with Organization IT Corporate Firewalls as well as any existing proxy solution for shadowIT visibility for Risk assessment of traffic from gateway devices in sniff mode.		
SSE.REQ.033	Internet & SaaS Apps	The proposed solution should have open threat intel exchange platform to integrate with customer environment existing security stack such as EDR Solutions, Threat intel exchange solution, SIEM solutions, SSO solutions etc.		
SSE.REQ.034	Internet & SaaS Apps	The proposed solution should have capability for bi-directional IOC exchange (MD5,SHA.urls etc) through custom rest API's and manually to offer best security for the enterprise environment using existing security investment.		
SSE.REQ.035	Internet & SaaS Apps	The proposed solution should have GRE, encrypted phase 1 and encrypted phase 2 IPSEC Tunnel from day 1 to support traffic forwarding from customer on-premises firewall and gateway router.		
SSE.REQ.036	Internet & SaaS Apps	The proposed solution should have capability to provide User and Entity Behaviour Analysis (UEBA) profiling and risk score for users based on parameters like data exfiltration, locations awareness , bulk upload and download of files, bulk deletion of files, login-failures etc.		
SSE.REQ.037	Internet & SaaS Apps	The proposed solution should have API/JSON calls for web traffic to dynamically identify		

Zero Trust Network Access				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		multiple instances of web application usage i.e., it should be able to identify personal, corporate, partner instances of apps like O365 / Gsuite / Box / GitHub etc. and enforce granular Threat and DLP policies on individual instances.		
SSE.REQ.038	Internet & SaaS Apps	The solution should support advance DLP capabilities like OCR and AI/ML classifiers for image scanning to detect India PII (Aadhar,PAN,Passport,Driving license etc.) Photo ID, Driving license, PII in Screenshots , Whiteboards and sensitive data leaks inside image files.		
SSE.REQ.039	Internet & SaaS Apps	The solution should be able inspect & block 8 times zipped / compressed files.		
SSE.REQ.040	Internet & SaaS Apps	The proposal solution should have access controls on any TCP and UDP ports. It must be able to define policies based on 5 tuple rules, fqdn destination and user, group-based access policies.		
SSE.REQ.041	Internet & SaaS Apps	The solution should have reverse proxy deployment to enforce granular context-specific access policies on unmanaged devices (BYOD) accessing corporate Google Drive, Gmail, Microsoft O365, Slack and AWS etc.		
Internal & Private Apps				
SSE.REQ.042	Internal & Private Apps	Applications accessed via from remote should not require network access (user should not		

Zero Trust Network Access				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		be able to find out the actual IP address of the application server)		
SSE.REQ.043	Internal & Private Apps	The solution should protect all Enterprise Internal applications from external attack. Even if there are some Vulnerability on the application it should not be exposed to external attacker.		
SSE.REQ.044	Internal & Private Apps	Any component installed in DC's (On-premises or IaaS) must not need any inbound ACL rule in customer DC/DR Firewall to provide access to Private Application.		
SSE.REQ.045	Internal & Private Apps	Solution should enable seamless access to Internal applications across multi-DC's (no need to connect any VPN/Remote Access Agent every time application access is required). The solution should be Always-On whenever Internet is reachable		
SSE.REQ.046	Internal & Private Apps	The solution should have dashboards providing information about Applications, Users, and System's Internal Components		
SSE.REQ.047	Internal & Private Apps	Connectivity between remote users' devices and private applications is secured by an end-to-end TLS (v1.3) encrypted tunnel and optimally routed through with a low latency, high-capacity, scalable network infrastructure.		
SSE.REQ.048	Internal & Private Apps	Granular policies for blocking or allowing access to private applications can be built on criteria including User, Group or Organizational Unit (OU); Device Classification; or Operating System.		

9. Application Security

Application Security				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
AS.REQ.001	Application Security	The solution must be able to analyse a wide array of programming languages including Java, .Net, C/C++, Objective-C, Android, PHP, COBOL, Ruby, Swift, HTML 5, Scala, APEX, TypeScript, Go, Kotlin and ABAP etc but not limited to these alone.		
AS.REQ.002	Application Security	The solution must detect over 1000+ unique categories of security vulnerabilities		
AS.REQ.003	Application Security	The solution must support a variety of operating systems: Windows, Linux, MacOSX		
AS.REQ.004	Application Security	Solution must have centralized console to reporting and automation		
AS.REQ.005	Application Security	The solution integrates with a defect-tracking system (e.g. HP ALM, QC Enterprise, Microsoft TFS, JIRA,		

Application Security				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		Bugzilla, VSTS) for easy creation of defects for vulnerabilities found from within the solution itself.		
AS.REQ.006	Application Security	The solution must support multiple common databases including Oracle, Microsoft SQL Server, MySQL		
AS.REQ.007	Application Security	The solution must support deployment on multiple common web application servers including Tomcat		
AS.REQ.008	Application Security	Solution must integrate with developers' machines supporting multiple methods of DevOps		
AS.REQ.009	Application Security	Solution must have multiple deployment options like on –prem, centralised, standalone, cloud or hybrid deployment		
AS.REQ.010	Application Security	It must be sized for 20 applications/ Codes		
AS.REQ.011	Application Security	The solution shall support simultaneous Crawl & Audit during scans.		
AS.REQ.012	Application Security	The solution shall allow for multiple concurrent scans.		
AS.REQ.013	Application Security	Solution must integrate with SAST tool for faster and better result		
AS.REQ.014	Application Security	It must share the results with SIEM solution as well		

Application Security				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
AS.REQ.015	Application Security	It must integrate with same centralized consoles of SAST tool		
AS.REQ.016	Application Security	The solution must support deployment on-premises, in the cloud and a combination of the two.		
AS.REQ.017	Application Security	Solution must be sized for 2 Named users		
AS.REQ.018	Application Security	Proposed Solution must have Supplied / deployed in at least 10 Govt. of India Departments.		
AS.REQ.019	Application Security	Proposed Solution of SAST and DAST should be from same OEM for having seamless Integration and single console		
AS.REQ.020	Application Security	The solution must provide Software Security Assurance Program governance capabilities including the ability to define multiple, customized, risk-based Secure Software Development Lifecycle procedures, assign tasks, track sign-off/approvals, act as a document repository, report progress, provide an on-boarding portal, etc.		
AS.REQ.021	Application Security	The solution shall have the ability to feed details of vulnerabilities found during a scan into an Intrusion Prevention System to block potential application exploits		

Threat Intelligence & dark Web Monitoring

Threat Intelligence & dark Web Monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
Scope				
THIDWB.REQ.001	Scope	The proposed Vendor solution shall provide cyber threat intelligence and attribution information in the area cyber-crime, cyber-espionage, hacktivism, and enterprise security		
THIDWB.REQ.002	Scope	The proposed Vendor solution shall provide strategic, operational / tactical and technical threat intelligence.		
THIDWB.REQ.003	Scope	The proposed Vendor solution shall provide cyber threat intelligence that is relevant to the Dial 112 entities based on their business sectors and geographical locations		
THIDWB.REQ.004	Scope	The proposed Vendor solution shall identify and track cyber threat actors that are relevant to Dial 112 . The proposed Vendor solution shall provide a brief summary of the cyber threat actors as part of the submission		
THIDWB.REQ.005	Scope	The proposed Vendor solution shall identify and track the tactics, techniques and procedures (“TTPs”) used by cyber threat actors that is relevant to Dial 112 . The proposed		

Threat Intelligence & dark Web Monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		Vendor solution shall provide a brief summary of the TTPs as part of the submission		
THIDWB.REQ.006	Scope	The proposed Vendor solution shall identify and track attack campaigns by the cyber threat actors that is relevant to Dial 112 . The proposed Vendor solution shall provide a brief summary for the campaigns, as part of the submission		
THIDWB.REQ.007	Scope	The proposed Vendor solution shall maintain a mapping of the cyber threat actors (alias) to those actors tracked by other reputable proposed Vendor solutions. The proposed Vendor solution shall provide the mapping of the cyber threat actors as part of the proposal submission.		
THIDWB.REQ.008	Scope	The proposed Vendor solution must have capabilities to generate a risk score or other quantitative risk assessments of the feeds at least in 2 categories - Reliability & Credibility		
THIDWB.REQ.009	Scope	The proposed Vendor solution must support monitoring of Dark Web forums for information related to Dial 112 and also provide searching of live raw feeds from these Forums.		

Threat Intelligence & dark Web Monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THIDWB.REQ.010	Scope	The proposed Vendor solution must support proactive monitoring of Threat Actor infrastructures such as C&C servers, Telegram/IRC channels, forums, OSINT, Card shops etc.		
THIDWB.REQ.011	Scope	The proposed Vendor solution must provide compromised information related to Dial 112 such as credentials, latest exposed credit cards (masked & unmasked both), Mule Accounts, Files, Mobile Devices etc by proactively monitoring Threat Actor infrastructures.		
THIDWB.REQ.012	Scope	The proposed Vendor solution must support monitoring of OSINT such as - Pastebin, Ideaone, Github, Virustotal, Anyrun etc for information related to Dial 112		
THIDWB.REQ.013	Scope	The proposed Vendor solution must provide list of all release vulnerabilities from different vendors both CVE and Non-CVE along with list of known exploits in the wild for the relevant vulnerabilities.		
THIDWB.REQ.014	Scope	The proposed Vendor solution must provide suspicious and malicious list of IPs in the categories of CnC server, DDoS, TOR nodes, BoT and Open Proxies etc		

Threat Intelligence & dark Web Monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THIDWB.REQ.015	Scope	The proposed Vendor solution must provide access to a central database of publicly leaked email credentials for easy search & alert if any of the Dial 112 accounts are leaked in public dumps.		
THIDWB.REQ.016	Scope	The proposed Vendor solution must have capability to detect defacement		
THIDWB.REQ.017	Scope	The proposed Vendor solution must provide detection of Phishing attempts, Domains, Phishing pages hidden inside and defacements by proactively monitoring Threat Actor infrastructures.		
THIDWB.REQ.018	Scope	The proposed Vendor solution should provide Cloud based sandbox for Dial 112 to submit files for detonation and inspection of unknown as well-known malware behaviour		
THIDWB.REQ.019	Scope	The proposed Vendor solution must provide Network Analytic Graph for Threat Hunting and attribution purposes for Dial 112 Threat Analysts. This linkage graph should act as a single lookup functionality for multiple types of IOCs		

Threat Intelligence & dark Web Monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THIDWB.REQ.020	Scope	The proposed Vendor solution must provide detailed analysis of latest Threats by Cybercriminal and Nation state Groups including but not limited to IOCs, MITREATT&CK mapping, tools used etc. These threat analysis reports should also include but not limited - - Malware - Campaign - Threat Actor profiles - TTP's - IOCs per threat - Monitoring of APT-related activity The Vendor must submit an example of such report as part of submission.		
Quality				
THIDWB.REQ.021	Quality	The proposed Vendor solution shall have a robust process in identifying, collecting, analysing, producing, reviewing and tracking cyber threat information to produce threat intelligence that are relevant to Dial 112 . The proposed Vendor solution shall provide the process stated above as part of the submission		
THIDWB.REQ.022	Quality	The proposed Vendor solution shall categorize the cyber threat intelligence for easy searching and reporting by category. The proposed		

Threat Intelligence & dark Web Monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		Vendor solution shall state its categorization supported in the submission		
THIDWB.REQ.023	Quality	The proposed Vendor solution shall enrich the cyber threat intelligence by adding context (Summary Report). The proposed Vendor solution shall state what enrichment is provided in the submission.		
Accuracy				
THIDWB.REQ.024	Accuracy	The proposed Vendor solution shall provide cyber threat intelligence that is accurate and relevant. The proposed Vendor solution shall provide information on accuracy and relevancy in the submission		
THIDWB.REQ.025	Accuracy	The proposed Vendor solution shall provide a confidence level for cyber threat information provided. The proposed Vendor solution shall provide information on the confidence level in the submission		
THIDWB.REQ.026	Accuracy	The proposed Vendor solution shall fine-tune the accuracy of the collection based on feedback from customer		
Timeline				

Threat Intelligence & dark Web Monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THIDWB.REQ.027	Timeline	The proposed Vendor solution shall provide cyber threat intelligence in a timely manner. The proposed Vendor solution shall provide the tailored intelligence within 24 hours of first exposure to the public		
THIDWB.REQ.028	Timeline	The proposed Vendor solution shall provide email alerts when new threat intelligence is available, based on rules configured		
THIDWB.REQ.029	Timeline	The proposed Vendor solution should provide multiple different attacks performed by a Cybercriminal or Nation-State group in single place for easy searching and IOCs consumption.		
Research Analyst Access				
THIDWB.REQ.030	Research Analyst Access	The proposed Vendor solution shall be supported by a research team with good track records with at least 5+ years of experience. The proposed Vendor solution shall demonstrate its track record as part of submission		
THIDWB.REQ.031	Research Analyst Access	The proposed Vendor solution shall be able to provide threat information (sanitized) from its incident response engagements (e.g. victim intelligence)		

Threat Intelligence & dark Web Monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THIDWB.REQ.032	Research Analyst Access	The proposed Vendor solution shall provide analyst access to Dial 112 , for the purpose of additional information request relating to cyber threats, such as threat actor, profiles, tactics, targets etc		
Machine Readable Technical Threat Intelligence (Feed)				
THIDWB.REQ.033	Machine Readable Technical Threat Intelligence (Feed)	The proposed Vendor solution shall provide Indicator of Compromise (IoC) information in machine readable format. IoCs shall include both network and host-based indicators. The proposed Vendor solution shall provide the types of IoCs provided in the submission		
THIDWB.REQ.034	Machine Readable Technical Threat Intelligence (Feed)	The proposed Vendor solution shall support STIX (Structured Threat Information Expression), TAXII (Trusted Automated Exchange of Indicator Information) and CSV format. The proposed Vendor solution shall state other formats supported in the submission		
THIDWB.REQ.035	Machine Readable Technical Threat Intelligence (Feed)	The proposed Vendor solution shall maintain and update the list of IoCs provided to Dial 112		

Threat Intelligence & dark Web Monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THIDWB.REQ.036	Machine Readable Technical Threat Intelligence (Feed)	The proposed Vendor solution shall provide IoC machine readable format that is supportable by the Bank's SIEM platform. The proposed Vendor solution shall support Dial 112 in configuring the Bank's SIEM platform to pull down IoC information automatically as part of the onboarding		
THIDWB.REQ.037	Machine Readable Technical Threat Intelligence (Feed)	The proposed Vendor solution shall provide option to access the cyber threat intelligence via REST API. The proposed Vendor solution shall state if the information provided via the REST API is structured or unstructured		
THIDWB.REQ.038	Machine Readable Technical Threat Intelligence (Feed)	The proposed Vendor solution shall state out-of-box support for Cyber Threat Intelligence Platform ("TIP") from reputable proposed Vendor solutions. The proposed Vendor solution shall state what TIP platform it supports out-of-box as part of the quotation submission		
Portal				
THIDWB.REQ.039	Portal	The proposed Vendor solution shall provide a portal for Dial 112 to view and access the threat information knowledge base.		

Threat Intelligence & dark Web Monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THIDWB.REQ.040	Portal	The proposed Vendor solution portal shall provide search features for Dial 112 to search based on keywords, IP addresses, file hashes, threat actors, malware names, CVE et cetera. The search should preferably support complex searches such as AND, OR search expressions. The proposed Vendor solution shall state the search capabilities as part of quotation submission		
THIDWB.REQ.041	Portal	The proposed Vendor solution portal shall provide capabilities to alert Dial 112 for any new relevant content made available. The proposed Vendor solution shall state the different customizations supported to configure the alerting feature		
THIDWB.REQ.042	Portal	The proposed Vendor solution portal shall provide periodic summary via email. The proposed Vendor solution shall state what are the regular finished threat intelligence products included as part of the proposal.		
Threat Briefing				
THIDWB.REQ.043	Threat Briefing	The proposed Vendor solution shall provide regular threat calls to brief its customers on strategic cyber threat outlook and round-up. The proposed Vendor solution shall state the format		

Threat Intelligence & dark Web Monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
		and structure of such threat calls in the submission on request		
THIDWB.REQ.044	Threat Briefing	The proposed Vendor solution shall provide periodic threat landscape briefing to its customers. The proposed Vendor solution shall state the format and structure of such threat landscape briefings in the quotation submission		
Post Implementation Support				
THIDWB.REQ.045	Post Implementation Support	The proposed Vendor solution shall provide First Level Support for post implementation		
THIDWB.REQ.046	Post Implementation Support	The proposed vendor must provide 24x7 access to analyst team via portal to provide support on various types of RFIs such as - Phishing Take down, Threat Actor Profiling, IOCs enrichment, Malware recerse engineering, email and APK analysis etc		
THIDWB.REQ.047	Post Implementation Support	The proposed Vendor solution must maintain history of all the requests or tickets on the portal for search and follow ups.		

Threat Intelligence & dark Web Monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THIDWB.REQ.048	Post Implementation Support	Provide Dial 112 with regular updates of its key innovations and capabilities, as well as market intelligence on related products and services that the proposed Vendor solution is providing Dial 112 , and providing business or technical consultancy service to Dial 112 as appropriate		
THIDWB.REQ.049	Post Implementation Support	proposed Vendor solution is to provide an individual who will be the primary contact for Dial 112 at the regional and local country level. This representative will:		
THIDWB.REQ.050	Post Implementation Support	Have overall responsibility for managing and coordinating the proposed Vendor solution's services		
THIDWB.REQ.051	Post Implementation Support	Meet regularly with Dial 112 representative and our appointed third-party proposed Vendor solutions if required		
THIDWB.REQ.052	Post Implementation Support	Have the authority to make decisions with respect to actions to be taken by proposed Vendor solution in the ordinary course of day-to-day management of Dial 112 's account		
THIDWB.REQ.053	Post Implementation Support	Ensuring internal compliance to Dial 112 's stated process and procedures		
Service Provider Credibility				

Threat Intelligence & dark Web Monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THIDWB.REQ.054	Service Provider Credibility	Service provider must have at least 10 years of experience in Cyber Threat Intelligence and forensic investigations related to cyber security across various countries (at least 5 countries)		
THIDWB.REQ.055	Service Provider Credibility	Service provider must have deep knowledge of attack methodologies, background, objectives, target countries/verticals categorised by specific APT groups.		
THIDWB.REQ.056	Service Provider Credibility	Service provider must release at least 5 reports publically in a year covering High-tech crimes by different Threat Actor groups providing technical details of attacks and TTPs.		
THIDWB.REQ.057	Service Provider Credibility	The service provider must have their own Computer Security Incident Response Teams (CSIRTs) accredited by an external agency.		
THIDWB.REQ.058	Service Provider Credibility	Service provider must be member of at least 2 of reputed industry institutions such as FIRST/TRUSTED INTRODUCER/APWG		
THIDWB.REQ.059	Service Provider Credibility	The service provider shall be in Market Guide		

Threat Intelligence & dark Web Monitoring				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THIDWB.REQ.060	Service Provider Credibility	The service provider must have been recognised by some industry experts/analysts for their Cyber Threat Intelligence services		
THIDWB.REQ.061	Service Provider Credibility	Service provider must have in-house capabilities to engage with law enforcement agencies and CERTs of different countries to provide assistance in investigations. Please provide public reference case studies of your engagement with law enforcement agencies.		

Threat Hunting Framework (Technology) with L3 CERT monitoring

Threat Hunting Framework (Technology) with L3 CERT monitoring (THF)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
	General			
THF.REQ.001	Detection of malware and infected devices	Identification of malicious communications carried out through the Customer's network between the infected device and the control server		

Threat Hunting Framework (Technology) with L3 CERT monitoring (THF)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THF.REQ.002		Identification of malicious files transmitted over the Customer's network and received via the e-mail system using the method of behavioural analysis in specially prepared virtual machines		
THF.REQ.003		Identification of threats on the Customer's host and timely blocking of abnormal behaviour		
THF.REQ.004		Revealing hidden malicious infrastructure aimed at the Customer's network		
THF.REQ.005		Visualization of malicious activity on the Customer's host, obtaining a complete list of additional indicators, their correlation with potential incidents detected in the Customer's infrastructure, and attribution according to the internal classifier		
THF.REQ.006	Malware blocking	The system should provide blocking of malware via next channels/integrations: Proxy server; Email system (on-premises/cloud solutions); Network file shares; On end-user devices (endpoints)		

Threat Hunting Framework (Technology) with L3 CERT monitoring (THF)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THF.REQ.007	Capability of on-premises installation	Analysis of incoming network traffic and behavioural analysis of files should be carried out by the system on the equipment installed in the Customer's data center and/or office		
THF.REQ.008	Logging within GUI	The system should record the activities of files, processes and users		
THF.REQ.009		Embedded module telemetry		
THF.REQ.010		Logs needed for threat hunting must be stored at least 2 weeks		
THF.REQ.011	Threat vectors	The system must prevent cyber threats for all attack vectors:		
THF.REQ.012		Email system (cloud and on-premises)		
THF.REQ.013		External storage systems		
THF.REQ.014		Network traffic		
THF.REQ.015		End-user devices		
THF.REQ.016	Management	All modules of the system must be connected to the Central node for control		
THF.REQ.017		Optionable 24/7 year-round monitoring and threat hunting provided by vendor or by third-party partners		
	Central node			
THF.REQ.018	Usability	Resource-intensive big data analysis must be performed at the Central Site.		

Threat Hunting Framework (Technology) with L3 CERT monitoring (THF)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THF.REQ.019		The detection logic can also be deployed both on the Central Node, which will not allow attackers to influence it, and on the Agent on the workstation.		
THF.REQ.020		Incidents management.		
THF.REQ.021		Threat hunting tools to research not only alerts but source logs as well (meta data, behavioural data, and so on).		
THF.REQ.022	Asset management	The system must collect data about the list of computers (hosts) and servers on which endpoint module is installed		
THF.REQ.023		The system must collect list of hosts, servers and network nodes passively detected in the analysed mirrored traffic		
THF.REQ.024		The system must make an inventory of the applications used on network hosts		
THF.REQ.025	Network separation	To communicate with the Central Node in order to receive updates and transfer the recorded information for centralized storage, sensors, a subsystem of behavioural analysis, must be connected to the network using a separate network interface.		
THF.REQ.026	Unified control system	The central node should implement four main functional blocks:		

Threat Hunting Framework (Technology) with L3 CERT monitoring (THF)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THF.REQ.027		a) update center		
THF.REQ.028		b) centralized data storage system		
THF.REQ.029		c) user interface		
THF.REQ.030		d) remote incident response		
THF.REQ.031		e) central management node for all product appliances		
THF.REQ.032	Correlation	The system should correlate the events of all detecting modules of the system to identify potential incidents, obtain additional indicators from the attacker's profile, and use them to test assumptions about the presence of an attack or infection.		
THF.REQ.033	Attribution	The system should attribute events, including different malware samples from different sources, with known malware families and cybercriminals' groups		
THF.REQ.034	Threat hunting	Based on network logs (metadata)		
THF.REQ.035		Based on email technical headers		
THF.REQ.036		Based on logs and processes information from end user devices		
	Network			

Threat Hunting Framework (Technology) with L3 CERT monitoring (THF)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THF.REQ.037	Network separation	The traffic analysis subsystem must connect to a copy of network traffic and ensure that there is no impact on the operability of the LAN and non-interference in the analysed network interaction.		
THF.REQ.038	Traffic analysis	The traffic analysis subsystem must capture network packets at the L2 level from the interface to capture network traffic, collect communication sessions and implement the following main functionality:		
THF.REQ.039		a) signature search in traffic based on decision rule base		
THF.REQ.040		b) registration of information about all connections occurring in network traffic (TCP, UDP, ICMP) with time stamp, number of packets and total amount of transmitted data within the framework of registered communication sessions		
THF.REQ.041		c) registration of information about DNS queries with time stamping, the source of the request, the recipient of the request, the content of the request, the received response, occurring in the network traffic		

Threat Hunting Framework (Technology) with L3 CERT monitoring (THF)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THF.REQ.042		d) registration of information about HTTP-requests taking place in network traffic with time stamp, request source, request recipient, method, URI and all request headers.		
THF.REQ.043		e) Anomalies/lateral movement detection based on ML algorithms		
THF.REQ.044	Peak load/throughput	The traffic analysis subsystem must support the processing of channels with a consolidated peak load of up to 1 Gbps. The traffic analysis subsystem must support the processing of tagged (VLAN) traffic.		
THF.REQ.045	Update decision/detection rules	The traffic analysis subsystem should interact with the central node and update the decision rule base and its own settings with a delay of no more than 5 minutes after the updated data is published in the update center. At the same time, the volume of transmitted information should not exceed 4000 MB per day.		

Threat Hunting Framework (Technology) with L3 CERT monitoring (THF)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THF.REQ.046	Interaction with the central node	The traffic analysis subsystem must transmit the registered information (IS events) to the central node in real time. At the same time, in case of unavailability of the central node for any reason, the traffic analysis subsystem must continue local accumulation of logs and files with a guaranteed storage depth of up to 14 days.		
THF.REQ.047		The traffic analysis subsystem must transmit the parameters of its own work (telemetry) to the central node to track emergency situations, overloads and operating parameters. Telemetry messages must include the following parameters:		
THF.REQ.048		a) the amount of allocated and free memory;		
THF.REQ.049		b) average CPU load across cores;		
THF.REQ.050		c) the number of packets received on the traffic receiving interfaces;		
THF.REQ.051		d) total volume of received data on the interfaces of traffic reception;		
THF.REQ.052		e) the amount of free space on your hard disk.		
THF.REQ.053		The central node must transmit to the traffic analysis subsystem:		

Threat Hunting Framework (Technology) with L3 CERT monitoring (THF)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THF.REQ.054		a) signature updates;		
THF.REQ.055		b) updating the decision rules;		
THF.REQ.056		c) indicators of known threats identified during the analysis of malicious files and network traffic at other points of the system installation;		
THF.REQ.057		d) updates of the software used.		
THF.REQ.058		The traffic analysis subsystem must have the functionality of transmitting telemetry and information about logged events through the Syslog mechanism for integration with other solutions of the Customer.		
THF.REQ.059	Proxy Integration via ICAP	Detection mode with file detonation		
THF.REQ.060		Inline mode with blocking		
	File analysis			
THF.REQ.061	General functionality and VM environment	Windows 7/10 Support		
THF.REQ.062		32-Bit and 64-Bit support		
THF.REQ.063		Emulating real environment (names, last updated user's software, browser history, etc.)		
THF.REQ.064		User activity emulation		
THF.REQ.065		Computer vision		
THF.REQ.066		Multilanguage support		
THF.REQ.067		Yara rules upload feature		

Threat Hunting Framework (Technology) with L3 CERT monitoring (THF)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THF.REQ.068		Manual files upload via web-interface		
THF.REQ.069		Upload via API		
THF.REQ.070		Possibility to download PDF report		
THF.REQ.071		Possibility to download PCAP file		
THF.REQ.072		Possibility to download extracted/created by sample files		
THF.REQ.073	Detection	Static analysis		
THF.REQ.074		Network analysis - C&C connections, signature detections, TLS/SSL MITM		
THF.REQ.075		Time-based attacks detection		
THF.REQ.076		Sandbox evasion techniques detection		
THF.REQ.077		Retrospective analysis based on new behavioural patterns / IoCs		
THF.REQ.078	Reporting	General information about sample (names, hashes, file size, etc.)		
THF.REQ.079		File structure		
THF.REQ.080		Risk scoring/assessment		
THF.REQ.081		Video or screenshots of execution		
THF.REQ.082		Sample behavioural markers (malicious, informal)		
THF.REQ.083		Known malware and cybercriminal groups attribution		
THF.REQ.084		MITRE ATT&CK Matrix mapping		
THF.REQ.085		Detailed network activity		

Threat Hunting Framework (Technology) with L3 CERT monitoring (THF)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THF.REQ.086		Detailed process tree		
	Endpoint security			
THF.REQ.087	Compatibility	The workstation analysis subsystem must be compatible with the installed Customer's antiviruses, EDR/XDR and DLP solutions.		
THF.REQ.088	Stability	The workstation analysis subsystem should not lead to performance degradation of the workstation		
THF.REQ.089	Logging	The workstation analysis subsystem should provide logging and transfer of files, processes, and user activities		
THF.REQ.090	Blocking and response	The workstation analysis subsystem should provide the ability to block malicious files		
THF.REQ.091		The workstation analysis subsystem should provide the ability to isolate infected computers from the local area network		
THF.REQ.092		The workstation analysis subsystem should send files that require scanning to the file behavioural analysis subsystem, and if the file is malicious, it should be blocked		

Threat Hunting Framework (Technology) with L3 CERT monitoring (THF)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THF.REQ.093		Solution should collect live forensic dumps like browser history, registry hives, windows event logs, memory dumps, etc.		
THF.REQ.094		Solution should be able to provide tools for remote access to end-user devices		
THF.REQ.095	Usability	Solution should be able to implement simple policies like blocking of unsigned executable files, DLLs, scripts, etc.		
THF.REQ.096		Solution should support custom policies, based on file hashes, SIDs, application names, extensions, etc.		
	Email security			
THF.REQ.097	Integration	The mail integration modules must provide fault tolerance for the mail system - cloud or on-premises		
THF.REQ.098		Mail integration modules must ensure that files are delivered to the behavioural analysis system for analysis.		
THF.REQ.099		Mail integration modules should block malicious objects		
THF.REQ.100		MTA (SMTP blocking) mode should be available		
THF.REQ.101		SMTP (BCC monitoring) integration should be available		

Threat Hunting Framework (Technology) with L3 CERT monitoring (THF)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THF.REQ.102		POP3 (BCC monitoring) integration should be available		
THF.REQ.103		IMAP (BCC monitoring) integration should be available		
THF.REQ.104		Inline integration with cloud email systems (Microsoft Office 365, Google Workspace)		
THF.REQ.105	Detection and response	Different URL analysis strategies feature to tune links analysis		
THF.REQ.106		Retrospective URL analysis		
THF.REQ.107		Password protected archive analysis		
THF.REQ.108		Custom policies based on senders, recipients, headers: SPF, DKIM and DMARC statuses, etc.		
THF.REQ.109		Different automatic actions for detected threats, at least: blocking; header adding; subject change		
THF.REQ.110		Automatic notification of a recipient about blocked emails		
	Integration with 3rd-party systems			

Threat Hunting Framework (Technology) with L3 CERT monitoring (THF)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THF.REQ.111	Common network equipment	The system must support integration with common network equipment (switches, routers, firewalls, etc.) for traffic analysis using different mirroring options: TAP, SPAN, RSPAN, SPAN-over-GRE		
THF.REQ.112	SIEM / Syslog servers	The system must support integration with Security Information and Event Management (SIEM) and Syslog servers to send logged information about security events (in JSON or HP Arcsight CEF formats)		
THF.REQ.113	Proxy servers	The system must support integration with Proxy Servers via ICAP protocol to detonate files extracted both from raw enencrypted (HTTP) traffic as well as decrypted TLS/SSL (HTTPS) traffic		
THF.REQ.114	Monitoring solutions	The system must support integration with network monitoring solutions (like Zabbix, Nagios, Grafana, Prometheus, etc.) via SNMP protocol to monitor solution's modules performance and availability		
THF.REQ.115	Mail servers	The system must support integration with Mail Servers for BCC monitoring (via SMTP, POP3, IMAP) and inline blocking via SMTP		

Threat Hunting Framework (Technology) with L3 CERT monitoring (THF)				
Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations
THF.REQ.116	File shares	The system must support integration with network file shares using NFS, FTP, SMB (Samba, CIFS) and WebDAV protocols		
THF.REQ.117	SOAR	The system must support integration with Security Orchestration, Automation, and Response (SOAR) solutions for automated response on cyber threats		

SSL Interceptor

SSL Interceptor			
Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Deviations
SSLI.REQ.001	Should be high performance dedicated hardware with multicore CPU support and not a part of UTM/ Firewall/ Router or any other device. Proposed appliance should support virtualization and support up to 16 Virtual instances with minimum 2 virtual instances from Day1		
SSLI.REQ.002	The appliance should support minimum 90 Gbps of SSL throughput to support security device functions and should be deployed in high availability using open standard VRRP (No proprietary protocol).		

SSL Interceptor			
Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Deviations
SSLI.REQ.003	The appliance should have minimum 8 X 10G SFP+ and 8 x 1G ports with prepopulated SFPs and dual power supply. Proposed appliance should have minimum 128 GB RAM and 4 TB hard disk		
SSLI.REQ.004	Hardware based SSL acceleration with 80 Gbps of bulk SSL encryption throughput and 75,000 ECC TPS (ECDSA-SHA256), 100,000 2k SSL transactions per second (TPS). Should support both 2048 and 4096 bit keys for encrypted application access.		
SSLI.REQ.005	Proposed device should support minimum 8 Million L7 requests per second. Device should also support standard VRRP for high availability		
SSLI.REQ.006	The SSL Intercept device shall support SSL termination with TLS 1.2, TLS 1.1, TLS 1.3 protocols. The SSL Intercept device shall be able to detect and decrypt all TCP ports that utilize SSL/TLS (TCPS) communication.		
SSLI.REQ.007	The SSL Intercept device shall support both outbound SSL traffic (forward proxy) and inbound SSL traffic (reverse proxy). The SSL Intercept device shall able support inline bridge mode, decrypt/encrypt SSL traffic without change the SRC/DST IPs and network IP segment topology. The SSL Intercept device shall support SPAN port functions for external passive security devices.		

SSL Interceptor			
Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Deviations
SSLI.REQ.008	The SSL Intercept device shall able support explicit Forward Proxy functions. For privacy policies, the SSL Intercept shall support URL bypassing by static configuration. For compliance, the SSL Intercept shall support selective URL bypassing by reputable online URL classification services.		
SSLI.REQ.009	For outbound, the SSL Intercept device shall use the same SSL version and SNI options as client, re-encrypt application data, which may be modified by the external security devices (such as WAF, DLP) to the original destination.		
SSLI.REQ.010	The SSL Intercept device shall support secured RESTful API or XML-RPC for simple 3rd party remote management. The SSL Interception device shall support secured WebUI (HTTPS) access. No HTTP. The SSL Interception device admin access shall be supported by local DB, external Radius/TACACS		
SSLI.REQ.011	Device should support SSL Interception to work by having client establish trust relationship with SSL appliance, decrypt the communication, re-encrypt and send to server. Device should be able to Inspect both inbound and outbound SSL traffic and provide application visibility, traffic can be redirected to security zone for threat inspection		

SSL Interceptor			
Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Deviations
SSLI.REQ.012	Should support certificate parser and solution should integrate with client certificates to maintain end to end security and non-repudiation. The appliance should support Certificate format as "OpenSSL/Apache, *.PEM", "MS IIS, *.PFX", and "Netscape, *.DB". Should support OCSP protocol to check the validity of the certificates online. Certificate bases access control, CRL's (HTTP, FTP, and LDAP) support.		

10. SSL VPN Gateway

SSL VPN Gateway			
Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Deviations
SSLVPN.REQ.001	The appliance should be dedicated SSL VPN Gateway and not a part of UTM/ firewall/ NGFW/ ADC device It should have 1x1GbE port for management and 8x10GbE SFP+ ports.		
SSLVPN.REQ.002	The appliance should have multicore CPU, 64GB RAM, 4TB HDD and dual power supply.		
SSLVPN.REQ.003	The solution Should have dedicated hardware SSL card and should support 45 Gbps of SSL Throughput		
SSLVPN.REQ.004	The appliance should be capable of creating multiple virtual portals and support minimum 1000 concurrent users scalable to 10000 concurrent users on the same appliance without changing any hardware		
SSLVPN.REQ.005	The device should support on demand provisioning of L3 VPN client using ActiveX or JAVA applet, standalone and command line L3 VPN client support.		
SSLVPN.REQ.006	The solution should support different network pools defined per user or group.		
SSLVPN.REQ.007	The appliance should support 45 Gbps of compression throughput. This capability shall be compatible with most modern browsers, requiring no additional software. Proposed appliance should support Desktop over VPN feature to provide access to desktop from remote for WFH purpose.		
SSLVPN.REQ.008	The solution should support desktop publishing on IOS and Android phones along with device ID based authorization. The solution should support enterprise Appstore for android and IOS phones. The solution should support SDK for IOT devices. Should also support SAA, SAML, Hardware binding and AAA support along with SSO. Solution must support machine		

SSL VPN Gateway			
Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Deviations
	authentication based on combination of HDD ID, CPU info and OS related parameters, mac address to provide secure access to corporate resources.		
SSLVPN.REQ.009	The solution should support following Authentication methods:		
SSLVPN.REQ.010	a) Active Directory, b) LDAP , c) RADIUS ,d) Local database e) SAML f) Google O-Auth Support g) SMS		
SSLVPN.REQ.011	The solution must provide ranking of at least 4 authentication methods for granular authentication of VPN users		
SSLVPN.REQ.012	Appliance must support Access control options based on:-		
SSLVPN.REQ.013	a) User and group, b) Source IP and network, c) Destination network ,e) Service/Port, f) Host name or IP address ,g) IP range, h) Subnet and domain, I) Day, date, time and range		
SSLVPN.REQ.014	Should have IPV6 support with IPv6 to IP4 and IPv4 to IPv6 translation and full IPv6 support. Also should have IPV6 support with DNS 6 to DNS 4 & DNS 4 to DNS 6 translation-based health check for intelligent traffic routing and failover. Solution should support full DNS server functionality to support all kind of DNS records including A,AAAA, MX, CNAME, PTR DNS records.		
SSLVPN.REQ.015	The solution should provide comprehensive and reliable support for high availability with Active- active & active standby unit redundancy mode using standard VRRP (RFC-2338) for HA interconnection over network. Should support both device level and VA level High availability.		

11. Hardware Security Module (HSM), Anti Ransomware and Encryption Solution

Hardware Security Module (HSM), Anti Ransomware and Encryption Solution			
Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Deviations
ENC.REQ.001	The solution would be a hardware, tamperproof box having support for operating systems like Windows, Linux, Solaris, AIX		
ENC.REQ.002	Host Interface: Should have at least 4 Gigabit Ethernet ports with port bonding. Should support for 10G fiber network connectivity with port bonding. Should have IPv4 and IPv6 support.		
ENC.REQ.003	Minimum 5 partitions from day one and each partition should be protected with unique set of userid and password to grant access as per CCA IVG guidelines. Minimum Performance: RSA-2048: 1,000 TPS.		
ENC.REQ.004	Cryptographic APIs: PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL		
ENC.REQ.005	Asymmetric: Support for various cryptographic algorithms: Full Suite B support, Asymmetric Key RSA (1024-4096 bits), DSA , ECDSA , ECDH, Ed25519, ECIES, ECC (No separate license of Algorithm to be charged)		
ENC.REQ.006	Symmetric: AES, Triple DES, DES, ARIA, SEED, RC2, RC4, RC5, CAST (No separate license of Algorithm to be charged).		
ENC.REQ.007	Random Number Generation: comply with AIS 20/31 to DRG.4 using HW based true noise source alongwith NIST 800-90A compliant CTR-DRBG		
ENC.REQ.008	Digital Encryption: BIP32 for blockchain		
ENC.REQ.009	5G Cryptographic Mechanisms for Subscriber Authentication: Milenage, Tuak, and Comp128		
ENC.REQ.010	The solution should have Built-in Data Discovery and Classification to discover sensitive PII data in local storages using templates including detection of datatypes within images with OCR feature.		

Hardware Security Module (HSM), Anti Ransomware and Encryption Solution			
Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Deviations
ENC.REQ.011	The Solution should support Intelligent Remediation of discovered sensitive data by encryption.		
ENC.REQ.012	The proposed box should be minimum FIPS 140-2 level 3 certified. FIPS certification should be in the name of the proposed OEM.		
ENC.REQ.013	The proposed box or the card/module used inside the HSM should be Common Criteria EAL 4+ certified in the name of the proposed OEM		
ENC.REQ.014	Key Management Solution should provide Transparent Encryption for large scale high performance file system encryption - including specific support for Oracle, Teradata, Pure Storage and SAP HANA		
ENC.REQ.015	The proposed box must have built-in Clustering (Active/Active) and Load Balancing capabilities. No external load balancer should be required.		
ENC.REQ.016	API Support –REST (JWT), KMIP, PKCS#11, JCE, .NET, MSCAPI, MS CNG, NAE-XML , C, Java API's and libraries for integration in to custom applications.		
ENC.REQ.017	Should have the functionality of entire Key life-cycle tasks including generation, caching, versioning, rotation, destruction, import and export as well as provide abilities to manage certificates and secrets. Key Versioning should not require any downtime for the application.		
ENC.REQ.018	The Solution should support capability of PDF exporting of Scanned data report.		
ENC.REQ.019	The KMS must have centralized management of key synchronization and Key upload across multiple Public cloud providers such as AWS, Azure and GCP along with the ability to support automated scheduled key rotation and expiry via a simple GUI.		
ENC.REQ.020	Solution must have Full life cycle key management via GUI of cloud encryption keys generated and residing in Azure, AWS, Salesforce and O365 as well as Bring Your Own Keys (”BYOK”) for cloud		

Hardware Security Module (HSM), Anti Ransomware and Encryption Solution			
Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Deviations
	encryption keys generated in 'MANAGER' loaded up to Azure/ AWS/ Salesforce/ O365.		
ENC.REQ.021	Integration of key management BYOK API's with Azure, GCP and AWS from day one. RESTful APIs must be tested and validated on multiple CP solutions.		
ENC.REQ.022	Centralized cloud key management must provide access to each cloud provider (AWS, Salesforce, Azure and GCP) from a single browser window, including across multiple accounts or subscriptions		
ENC.REQ.023	Cryptographic keys (both the local master keys and lower-level encryption keys) will be stored and protected within the secure confine of the FIPS 140 hardware, and will never leave the hardware, whether in plain text or encrypted format		
ENC.REQ.024	Solution must have Application Whitelisting feature to prevent Ransomware attacks. Solution should Block Untrusted Binaries from Encrypting Data.		
ENC.REQ.025	Solution should Identify "trusted applications" – binaries which are approved to perform encryption/decryption of business critical files.		
ENC.REQ.026	Solution should be able to check the integrity of those "trusted applications" with signatures to prevent polymorphic malware from getting into approved binaries.		
ENC.REQ.027	a.) Solution must have Fine-grained Access Control to prevent access to Ransomware hackers.		
ENC.REQ.028	b.) Solution should define who (user/group) has access to specific protected files/folders and what operations (encrypt/decrypt/ read/ write/directory list/execute) they can perform.		
ENC.REQ.029	c.) Solution should prevent privileged users from examining and even accessing critical resources.		
ENC.REQ.030	Solution should transparently encrypt data at rest residing in database servers, file servers and SAN boxes (KMIP).		

Hardware Security Module (HSM), Anti Ransomware and Encryption Solution			
Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Deviations
ENC.REQ.031	The proposed OEM should have a minimum turnover of INR10 cr in each of the past two consecutive years (audited balance sheet/ ITR).		
ENC.REQ.032	24/7 telephonic and email OEM support. OEM should have their own warehouse in India. Bidder to furnish Manufacturer Authorization Certificate as per enclosed format. To ensure that the proposed OEM has a reasonable presence in the market, OEM should be present in India for at least 7 years (Certificate of Incorporation to be furnished) on the date of bid submission.		
	Data In Motion		
ENC.REQ.033	Layer 2, 3 and 4 Network Encryption should be designed and implemented between multiple locations.		
ENC.REQ.034	Network Encryptors should be certified by international standards on FIPS 140-2 Level 3 and CC (at least EAL2+).		
ENC.REQ.035	Full Duplex, line rate AES-256 encryption for up to 100 Gigabit networks		
ENC.REQ.036	Network Encryptors Should support advanced fault detection.		
ENC.REQ.037	Should have strong SHA-256 hash function, 2048-bit digital certificates and hardware based key management.		
ENC.REQ.038	The encryption devices should exchange a new session key automatically on a pre-set interval of 1-60 minutes., which automatically generated by a TRNG or a PRNG.		
ENC.REQ.039	Network Encryptors should have built-in Hardware-based Random Number Generator and must be verifiable by customer.		
ENC.REQ.040	The cryptographic unit should be tamper-proof. The unit detects tamper assaults and reacts accordingly by its tamper response (zeroing all secret keys and secret security parameters).		
ENC.REQ.041	The Encryption devices, regardless of performance level, have to be interoperable.		

Hardware Security Module (HSM), Anti Ransomware and Encryption Solution			
Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Deviations
ENC.REQ.042	Network Encryptors should not require Smart cards to do the authentication and backup, all the authentication between devices should be based on the X.509 certificates.		
ENC.REQ.043	The network encryption should be transparent to the L2 and L3 core network of the Telco operator.		
ENC.REQ.044	Network Encryptors should support TACACS+ for remote authentication and SNMPv3 protocol.		
ENC.REQ.045	Latency of Network Encryptor should be below 10µs when they are deployed on the 1Gb links, independently of the packet/Ethernet frame size. Should ensure high quality of real time applications such as VoIP and video.		
ENC.REQ.046	Network Encryptors in HQ should be able to fit in 19” rack in a 1U space.		
ENC.REQ.047	Network Encryptors should support all modes of operation: point-to-point, point-multipoint, multipoint-multipoint.		
ENC.REQ.048	Point-point connection has to support Transmission security to prevent statistical analysis on the encrypted data.		
ENC.REQ.049	Devices should support AES CTR, CFB or GCM modes.		
ENC.REQ.050	It is mandatory devices are future-proof and can be fully reprogramed in case new algorithms appear.		
ENC.REQ.051	The encryptor has to have support for custom Elliptic Curves.		
ENC.REQ.052	The Encryption devices should also provide optional EtherType change.		
ENC.REQ.053	Device management has to be supported locally, via Management port or via In-band management on Data channel.		
ENC.REQ.054	The vendor should provide Virtual Encryptors for the customer to test functionality and settings of the devices in a virtual lab.		

Hardware Security Module (HSM), Anti Ransomware and Encryption Solution			
Sr. No.	Minimum Requirement Description	Compliance (Yes / No)	Deviations
ENC.REQ.055	The protection of the cryptographic parameters during management distribution must have the same symmetrical mechanism with equal or higher security level than the protection of the payload data.		

10 Technical Requirement Specification – TRS for Hardware

1.1. SAN Storage

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
Make				
Model				
1.	Storage Controller	The Storage system should a SAN supporting all Block and File protocols scaling to at least 4 controllers in the same cluster in active-active configuration. The scale out storage should be able to expand the capacity & performance in linear scalability by adding controllers to offer storage system for SAN OR NAS.		
2.	Cache required	The SAN system should have minimum 256 GB data cache post protection overheads across supplied controllers with an ability to protect data on cache if there is a controller failure or power outage. Cache should be protected for Writes either through a battery backup or by destaging to flash/disk.		
3.	Drive Support	The SAN system must support intermixing of dual ported 12Gbps SSD , SAS and SATA drives to meet the capacity and performance requirements of the applications. The system must support a minimum of 600 disks in a dual controller architecture and 1200 disks in a scale-out-architecture.		
4.	Protocols	The storage should be configured with iSCSI, FC, FCOE, NFS(NFSv3,NFSv4, NFSv4.1-RFC 5661) SMB(,SMB2 & SMB3) , S3 protocols for use with different applications and should support the maximum capacity offered by the storage system. If bidder does not support all protocol natively then additional		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
		appliance in HA should be offered for mentioned protocols.		
5.	RAID configuration	Should support RAID 6 or equivalent		
6.	High Availability	The storage system must be configured to continuously serve data in event of any controller failure. In addition to this, it must also be possible to withstand failure of any 3 disks per RAID-Group.		
7.	Storage Capacity	Storage must supplied with 223 TB usable capacity at DC & 150 TB usable capacity at DR ,on dual ported minimum 8 Gbps NL-SAS Disk with appropriate RAID Group giving 3 disks failure per RAID group		
8.	Front-End and Backend connectivity	The proposed storage system should has 8 x 16Gbps FC for SAN host connectivity across dual controller/node.		
9.	Rack Mountable	The storage should be supplied with rack mount kit. All the necessary patch cords (Ethernet and Fiber) shall be provided.		
10.	Storage Scalability and Upgradability	The Storage should be a true scale-out architecture. It should not be just a federation/group of controllers which can be managed by single management software. Scale out storage should be have like a single storage with more than two controllers.		
11.	Storage Functionality	The storage shall have the ability to expand LUNS/Volumes on the storage online and instantly.		
12.	Storage Functionality	The storage shall have the ability to create logical volumes without physical capacity being available or in other words system should allow over-provisioning of the capacity. The license required for the same shall be supplied for the maximum supported capacity of the offered storage model.		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
13.	Storage Functionality	The storage should be configured with Quality of Service feature for IOPs/Throughput for both Block and File.		
14.	Storage Functionality	The storage shall support logical partitioning of controllers in future such that each partition appears as a separate Virtual storage in itself.		
15.	Storage Functionality	The proposed storage system should be configured to provide data protection against two simultaneous drive failures.		
16.	Storage Functionality	The required number hard disks for parity & spares, should be provided exclusively of the usable capacity mentioned.		
17.	Storage Functionality	The offered storage should be offered with storage-based replication for entire offered capacity. Storage should offer WAN optimization that it should be able to preserve/maintain storage efficiency like dedup and compression while replicating data from DC to DR to save bandwidth. Storage should support 3 DC DR replication architecture.		
18.	Storage Functionality	SAN should have redundant hot swappable components like controllers, disks, power supplies, fans etc.		
19.	Point-in-times images	The storage should have the requisite licenses to create point-in-time snapshots. The storage should support minimum 200 snapshots per volume/LUN. The license proposed should be for the complete supported capacity of the system for both block and file.		
20.	Encryption for Data at Rest	The proposed storage array must support data at rest encryption offering industry standard certification/compliance. The storage array may		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
		implement data at rest encryption using self-encrypting drives or controller-based functionality there by not impacting performance.		
21.	Management	Single management, easy to use GUI based and web enabled administration interface for configuration, storage management and performance analysis tools for both block and file.		
22.	Remote Support & Diagnostics	Storage management should support call facility with web based self-service portal providing an integrated, efficient monitoring and reporting capability and supporting data collection. Management software should provide features like: 1. Automated call home feature 2. Nonintrusive alerting 3. Performance and Capacity reports 4. Ongoing health check analysis		
23.	OS support	Support for industry-leading Operating System platforms including: LINUX , Microsoft Windows, etc. Any Multipathing software required for the solution must be supplied for unlimited host connectivity		
24.	De-Duplication, Compression and Compaction	Proposed storage should support Iline block level data de-duplication, compression and compactio for all kinds of data (structured & unstructured) on both block and file.		

1.2. Backup through D2D

Sl. No	Features	`	Compliance (Yes/No)	Deviations (Yes/No)
1	Multiple protocols support	Proposed purpose-built backup appliance should be able to interface with various industry leading server platforms, operating systems and must support LAN/SAN based D2D backup and VTL backup simultaneously via NFS v3, CIFS, FC , OST and NDMP protocols.		
2	Deduplication efficiency	Appliance should support global and inline data duplication using automated variable block length deduplication technology.		
3	Standard protocols supported	Appliance should be offered with protocols like VTL, OST, CIFS, NDMP and NFS. All of the protocols should be available to use concurrently with global deduplication for data ingested across all of them.		
4	Multiple Backup software OEM support	Appliance should support industry leading backup software and should support deduplication at backup server/ host / application level so that only changed blocks travel through network to backup device.		
5	Backup Sizing & Retention policy (functional requirement)	Appliance (PBBA) should be sized appropriately for backup of source/front end data.		

Sl. No	Features	`	Compliance (Yes/No)	Deviations (Yes/No)
		Appliance should be quoted with adequate capacity considering 3% daily change rate for entire duration of the project. Any additional software, backup storage capacity (in addition to minimum 160 TB usable capacity and any other component required as per sizing needs to be provided by the Bidder at the time of bid.		
6	Cloud Enabled	Appliance should have the capability to tier backup data in deduplicated format to an external cloud storage (on premise / public cloud).		
7	I/O Port	Appliance should have the ability to perform different backup, restore, replication jobs simultaneously and must support communications and data transfers through 16GB SAN, 10 Gb & 1 Gb ethernet LAN over copper and SFP+. The proposed backup appliance should be offered with min. 1 x 1Gbps NIC, 8x 10Gbps NIC and 4 x 16Gbps FC ports and should support redundant controller for high availability of appliance in future.		
8	Backup Window	The proposed appliance must support backup throughput up to 30 TB/hr. while maintaining a single deduplication pool with RAID 6 and minimum one hot spare disk as well per disk enclosure.		
9	DR Readiness	Appliance should support different retentions for primary and DR backup storage and should support instant copy creation on remote site for better DR readiness with support for transmitting only		

Sl. No	Features	`	Compliance (Yes/No)	Deviations (Yes/No)
		deduplicated unique data in encrypted format to remote sites.		
10	Data Security	Appliance should support Retention Lock (WORM) feature which ensures that no backup data is deleted accidently and deliberately. Even Administrator should not be able to delete the backup data deliberately and accidently till the retention of the backup get expired. In case the data is replicated to DR/Secondary site, no additional licenses must be required at DR site to maintain retention lock on replicated data.		
11	Powe failure protection	Appliance should be offered with battery backed up RAM / NVRAM for protection against data loss in power failure scenario and continuous automated file system check to ensure data integrity.		
12	Self-service & Multi DB support	Appliance should Support Enterprise Applications and Database Backups without integration with Backup Software, for better visibility of Backups to Application and database Owners, thus ensuring faster and direct recovery on application/database level.		
13	Replication support for backup DR & data security	Appliance should support bi-directional, many-to- one, one-to-many, and one-to-one replication.		
14	Data Security	Appliance should support 256-bit AES encryption for data at rest and data-in-flight during replication. It should offer internal and external key management for encryption.		

Sl. No	Features	`	Compliance (Yes/No)	Deviations (Yes/No)
15	Disk configuration	Appliance should be offered RAID-6 with SAS/SATA/NL-SAS disk drives		
16	Multi OS Support	Software should be available on various OS platforms like Windows, Linux, etc. The backup server should be compatible to run on both Windows and Linux OS platforms		
17	Data Security	Should be able to encrypt the backed-up data using 256-bit AES encryption on the backup client and should not demand for additional license, any such license if needed should be quoted for the total number of backup clients asked for.		
18	Multi DB support	Should also support online LAN Free SAN based backups of databases through appropriate agents.		
19	Auto performance tuning	Should be able to dynamically break up large save-sets into smaller save-sets to be backed up in parallel to allow backups to complete faster for Windows, Unix and Linux clients.		
20	Backup schedule	Should have in-built calendar-based scheduling system and also support check-point restart able backups for file systems. It should support various level of backups including full, incremental, differential, synthetic and virtual synthetic backups.		
21	Data security	The proposed backup software should have the capability to enable WORM on the backup sets from the backup software console on proposed disk backup appliance. The implementation should ensure that no data can be deleted on the backup appliance even by the administrator.		

Sl. No	Features	`	Compliance (Yes/No)	Deviations (Yes/No)
22	Backup License	Bidder should provide capacity based licenses (Perpetual) with all modules & features asked in RFP.		
23	DB & Snapshot support	Must have Agent/Modules for online backup of applications and databases. Must support NAS and storage array based snapshot backup for off host zero downtime and zero load on the primary backup client with wizard based configuration.		
24	REST API support for automation	Should also have configurable ReST API support for management, administration and reporting on backup infrastructure via custom applications and out of box integration with reputed virtualisation solutions for complete orchestration.		
25	Reporting	The proposed solution should have inbuilt feature for extensive alerting and reporting with pre-configured and customizable formats. The proposed solution must have capability to do trend analysis for capacity planning of backup environment not limiting to Backup Application/Clients, Virtual Environment, Replication etc.		
26	DR capabilities	The proposed backup software should be able to recreate backed up data from existing volumes from metadata backups. The solution should offer recovery of specific volumes for recovery from metadata in case of a disaster recovery.		
27	Multi Hypervisor support & integration	The proposed Backup software should have the capability for Block based backups with granular recovery capability for faster backups on supported Disk platforms.		

Sl. No	Features	`	Compliance (Yes/No)	Deviations (Yes/No)
28	Ease of administration	The proposed backup solution should provide search capability from a web portal to allow search for a single file from complete backup store.		
29	Security & role based access	The backup solution should be capable of integration with active directory infrastructure for ease of user rights management along with role based access control to regulate the level of management.		
30	Ease of administration	The solution should have the capability to manage and monitor backups at remote locations from a single backup server, where clients can backup data to a local disk backup device without the need of local media server or sending primary backup copy over the WAN.		
31	Flexible deployment options	The solution should have the capabilities to backup as well as archive data to cloud with cloud service providers. In addition to this if data has to be moved from Cloud A to Cloud B the solution should be capable of cloud portability.		
32	Storage Capacity	160 TB		

1.3. Blade Server

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
Make				
Model				
1.	Processor	Populated with Four Intel Xeon Scalable processors, each CPU with 28 cores, min. 2.0 Ghz		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
2.	Chipset	Latest compatible chipset supporting above processor		
3.	Memory	Populated with 1.5 Tb Memory. Server should have minimum 48 DIMM slots RDIMMS& LR DIMMS		
4.	Hard Drives	2x 1.92TB for OS on RAID 1 & 4 x 3.84 TB for Data on RAID 6. Server should be configured with integrated RAID controller to support RAID level 0,1,5,6 on internal disks (Faulty drives shall not be returned during the warranty period and shall be property of the department,)		
5.	Ethernet ports	Dual port 25GbE network for ethernet		
6.	FC ports	The Chassis should have redundant FC switches (N+N), each switch should have min. 4 no. of 16Gbps FC uplinks to SAN		
7.	Remote management	In addition to the above dedicated Remote Management should be done/ All the blades in the chassis should be remotely managed through Chassis		
8.	Bus Slots	Minimum of 3 PCI expansions/Mezzanine expansions.		
9.	OS Support	Windows, Linux based		
10.	Systems Management	Smart Embedded Systems Management should be able to automate task like discovery deploy monitor and update.		
		Should not be dependent on agents to for life cycle management.		
		Should be able to provide Single console to manage Servers.		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
		Power management tool – Single interface to optimize and control every usage		
		Should be able to integrate to 3rd party management tools.		
11.	Remote Management	Solution should have embedded features that helps to manage Servers in physical, local and remote environments, operating in-band or out-of-band, with or without a systems management software agent.		
		Should include Power Management, necessary licenses should be included.		
		Should support remote scripted reconfiguration tools		
		Should be able to monitor all systems components (BIOS, HBA's, NICs)		
12.	Security	Power-on password, administrator password.		
		The server should have Hardware root of trust		
13.	Systems Management Software	The server should come with systems management software to provide update management, configuration management, patch management and virtualization management.		
14.	Accessories	All the necessary tools & tackles licenses, cables/ connectors for Ethernet/ Fibre/ USB/ Power etc. required for making the system operational shall be provided by the bidder.		
15.	Industrial Standard Compliance	ACPI 2.0 Compliant, PCI 2.0 or higher Compliant, WOL Support		

1.4. Blade Chassis

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
Make				
Model				
1.	Chassis	Rack Mountable Chassis to accommodate Support for minimum 4 numbers of 4 Proc blade servers or 8 Numbers of 2 Proc Blade Servers.		
2.	Management Modules	Should provide onsite Fully Redundant Management Solution with each chassis.		
		The blade chassis should be configured with Hot swap IP based KVM Switch for Management or KVM Management should be integrated in Remote Management Controller.		
3.	Mid-plane	Should have passive mid-plane/no mid plane/ back-plane architecture		
4.	IO Connections	Hot swap and redundant cooling fans and all fans should be fully populated		
		Dual end-to-end redundant Network connectivity for each blade		
		The blade chassis should have at least 6 I/O Modules/ switch bays		
5.	OS support	Chassis should support industry standard operating systems like Microsoft Windows Server, Redhat Enterprise Linux, SuSE Linux Enterprise Server		
6.	Power supplies	The enclosure should be populated fully with power supplies of the highest capacity available with the vendor. Power supplies should support N+N as well as N+1 redundancy configuration, where N is greater than 1		
		Power Management Features like		
		i. To cap the power of individual server or a group.		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
		ii. Intelligently assign power to the appropriate server in the pool based on policy settings.		
		iii. To show the actual power usage and thermal measurements data of servers		
7.	Accessories	The blade chassis should be configured with cables, connectors and accessories required to connect the Power distribution units to the power supplies		
8.	Ethernet Switches	The Chassis should have redundant Ethernet switches(N+N), each switch should have 4x10G sfp+ and 4 no. of 10G baseT uplinks		
9.	FC Switches	The Chassis should have redundant FC switches (N+N), each switch should have min. 2 no. of 16Gbps FC uplinks to SAN		
10.	Management	System Management and deployment tools to aid configuring the Blade Servers and OS Deployment should be provided.		
		The chassis should be equipped for providing MAC and WWN address across the slots or chassis instead of individual Host Bus Adapter/NIC of the Blade. The solution provided must not have any single point of failure and must be configured in failover		

1.5. Server Load Balancer

Sl. No.	Features	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
Make:				
Model:				

Sl. No.	Features	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
1.	Load Balancing	Should be appliance-based Load balancer and not a general server or feature on router or firewall. support inbound/outbound load balancing, server load balancing and SSL offloading		
		Load Balancing methods - Round Robin, Least Connections, Weighted RR, Weighted LC, Fastest Response, etc.		
2.	Operating System	The appliance-based Solution should be provided in high availability with hardened Operating System.		
3.	Operating System Performance	The underlying operating system and hardware should be capable of virtualization and support upto 16 virtual instances with each virtual instance having dedicated resources including hard disk, CPU, RAM, Operating system and SSL resources		
4.	Hardware Parameters	The appliance should have minimum 8 x 10G SFP+ ports all populated from day 1. It should have minimum 64 GB RAM and 4 TB hard disk		
5.	Forward proxy mode	The solution should support explicit forward proxy mode deployment		
6.	Transparent mode	The solution should also support transparent mode deployment and WCCP v2/PBR (Policy-based Routing)		
7.	Support multiple deployment	The solution should allow to deploy the appliance in explicit proxy as well as transparent mode.		
8.	DNS Functionality	It should support advance functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSEC, DNS DDOS, application load balancing from day one. It should be capable of handling complete Full DNS bind records including A,MX, AAAA, CNAME, PTR, SOA etc.		
9.	High Availability	Provision of active/active and active/passive High Availability		

Sl. No.	Features	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
10.	Reverse Proxy support	The proposed solution should support reverse Proxy and should support HTTP, FTP and HTTPS and all applications hosted in the data center.		
11.	HTTPS Decryption	The solution should support HTTPS decryption.		
12.	HTTPS decrypted Performance	The solution should have a dedicated SSL card and support minimum 35000 TPS on RSA 2k Key and 35000 TPS on ECC		
13.	Layer 7 Parameters	The appliance should support minimum 5 million new L7 Requests per second		
14.	IP V6 Support	The solution should provide compressive support for IPv6 functions to help with ipv4-to-ipv6 transition without business disruption and must provide support for dual stack, DNS64, NAT 64, DNS 46, NAT 46, IPv6 NAT		
15.	Remote support	The remote support from principal company should be available via India Toll Free and Email.		
16.	Secure Remote Access	The device should support machine authentication on the basis of HDD ID, CPU-ID, OS related features, MAC-ID		
17.	Diagnostic Tools	The appliance should have diagnostic network utilities like telnet, traceroute, lookup etc.		
18.	Updates and Upgrades	The appliance should provide seamless version upgrades and updates.		
19.	Secure Web Based management	The appliance should be manageable via HTTP or HTTPS		
20.	CLI based management	The appliance should be manageable via command line using SSH		
21.	Console access	For emergency, the appliance should have console access		

1.6. Link Load Balancer

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
Make:				
Model:				
1.	Load Balancing	Should be appliance-based Load balancer and not a general server or feature on router or firewall. support inbound/outbound load balancing for minimum 10 links from day 1		
		Load Balancing methods - Round Robin, Least Connections, Weighted RR, Weighted LC, Fastest Response, etc.		
2.	Operating System	The appliance-based solution should be provided in high availability with hardened Operating System.		
3.	Operating System Performance	The underlying operating system and hardware should be capable of virtualization and support up to 16 virtual instances with each virtual instance having dedicated resources including hard disk, CPU, RAM, Operating system and SSL resources		
4.	Hardware Parameters	The Proposed appliance should have minimum 8 x 10G SFP+ ports all populated from day 1. It should have minimum 64 GB RAM and 4 TB hard disk		
5.	Forward proxy mode	The solution should support explicit forward proxy mode deployment		
6.	Transparent mode	The solution should also support transparent mode deployment and WCCP v2/PBR (Policy-based Routing)		
7.	Support multiple deployment	The solution should allow to deploy the appliance in explicit proxy as well as transparent mode.		
8.	DNS Functionality	It should support advance functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSEC, DNS DDOS, application load balancing from day one. It should be capable of handling complete Full DNS bind records including A,MX, AAAA, CNAME, PTR, SOA etc.		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
9.	High Availability	Provision of active/active and active/passive High Availability		
10.	Reverse Proxy support	The proposed solution should support reverse Proxy and should support HTTP, FTP and HTTPS and all applications hosted in the data center.		
11.	FQDN Load Balancing	The solution should support Domain name support for outbound link selection for FQDN based load balancing.		
12.	Health Check	The solution shall provide individual link health check based on physical port, ICMP Protocols, user defined l4 ports and destination path health checks.		
13.	Layer 7 Parameters	The Appliance should support minimum 5 million new L7 Requests per second		
14.	IP V6 Support	The solution should provide compressive support for IPv6 functions to help with ipv4-to-ipv6 transition without business disruption and must provide support for dual stack, DNS64, NAT 64, DNS 46, NAT 46, IPv6 NAT		
15.	Remote support	The remote support from principal company should be available via India Toll Free and Email.		
16.	Secure Remote Access	The device should support machine authentication on the basis of HDD ID, CPU-ID, OS related features, MAC-ID		
17.	Diagnostic Tools	The appliance should have diagnostic network utilities like telnet, traceroute, lookup etc.		
18.	Updates and Upgrades	The appliance should provide seamless version upgrades and updates.		
19.	Secure Web Based management	The appliance should be manageable via HTTP or HTTPS		
20.	CLI based management	The appliance should be manageable via command line using SSH		
21.	Console access	For emergency, the appliance should have console access		

1.7. Global Load Balancer

Sl. No	Features	Minimum Requirements	Compliance (Yes / No)	Deviations (if any)
Make:				
Model:				
1.	Load Balancing	Should be appliance-based Load balancer and not a general server or feature on router or firewall. The solution should support site selection feature to provide global load balancing features for disaster recovery and site redundancy.		
		Load Balancing methods - Round Robin, Least Connections, Weighted RR, Weighted LC, Fastest Response, etc.		
2.	Operating System	The appliance-based solution should be provided in high availability with hardened Operating System.		
3.	Operating System Performance	The underlying operating system and hardware should be capable of virtualization and support up to 16 virtual instances with each virtual instance having dedicated resources including hard disk, CPU, RAM, Operating system and SSL resources		
4.	Hardware Parameters	The Proposed appliance should have minimum 8 x 10G SFP+ ports all populated from day 1. It should have minimum 64 GB RAM and 4 TB hard disk		
5.	Forward proxy mode	The solution should support explicit forward proxy mode deployment		
6.	Transparent mode	The solution should also support transparent mode deployment and WCCP v2/PBR (Policy-based Routing)		
7.	Support multiple deployment	The solution should allow to deploy the appliance in explicit proxy as well as transparent mode.		
8.	DNS Functionality	It should support advance functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server		

Sl. No	Features	Minimum Requirements	Compliance (Yes / No)	Deviations (if any)
		with DNSEC, DNS DDOS, application load balancing from day one. It should be capable of handling complete Full DNS bind records including A, MX, AAAA, CNAME, PTR, SOA etc.		
9.	High Availability	Provision of active/active and active/passive High Availability using open standard VRRP		
10.	Global Load Balancing	The solution should support global server load balancing algorithms including - Weighted round robin, Weighted Least Connections, Administrative Priority, Geography, Proximity, Global Connection Overflow (GCO), Global Least Connection (GLC), IP Overflow (IPO)		
11.	FQDN Load Balancing	The solution should support Domain name support for outbound link selection for FQDN based load balancing.		
12.	Health Check	The solution shall provide individual link health check based on physical port, ICMP Protocols, user defined l4 ports and destination path health checks.		
13.	Layer 7 Parameters	The Appliance should support minimum 5 million new L7 Requests per second		
14.	IP V6 Support	The solution should provide compressive support for IPv6 functions to help with ipv4-to-ipv6 transition without business disruption and must provide support for dual stack, DNS64, NAT 64, DNS 46, NAT 46, IPv6 NAT		
15.	Remote support	The remote support from principal company should be available via India Toll Free and Email.		
16.	Diagnostic Tools	The appliance should have diagnostic network utilities like telnet, traceroute, lookup etc.		
17.	Updates and Upgrades	The appliance should provide seamless version upgrades and updates.		

Sl. No	Features	Minimum Requirements	Compliance (Yes / No)	Deviations (if any)
18.	Secure Web Based management	The appliance should be manageable via HTTP or HTTPS		
19.	CLI based management	The appliance should be manageable via command line using SSH		
20.	Console access	For emergency, the appliance should have console access		

1.8. Core Switch

Sl. No	Features	Minimum specs	Compliance (Yes/No)	Deviations (Yes/No)
	Make			
	Model			
1.	General Features	Non-blocking equipment		
2.	General Features	Chassis based Equipment with (minimum 7 Interface Card slot)		
3.	General Features	Support of redundant and Hot Swap FAN`s		
4.	General Features	Power supply (AC/DC) slots: 4		
5.	General Features	SFP`s Hot Swap		
6.	General Features	The modular switch should be capable of providing different density of ports supporting 1G/2.5G/5G/10G/25G/40G/50G/100G interfaces with different line cards as required.		
7.	General Features	The modular switch should support 2 controller slots and it should provide HA within the controller slots in the chassis without any interruption to the switch operations.		
8.	General Features	The modular switch should be loaded with 2 controller cards & min of 48nos. of 1/10G SFP+		
9.	General Features	After populating the above ports minimum of 3 nos. of line cards slots to be available for further expansion		
10.	General Features	Total Chassis switching capacity: 10.24 Tbps		

Sl. No	Features	Minimum specs	Compliance (Yes/No)	Deviations (Yes/No)
11.	General Features	Switching capacity per 10G line card: 960Gbps & 767Mpps		
12.	General Features	Chassis size not more than 11RU		
13.	General Features	Operating Temperature: 0 ° C to 45 ° C		
14.	General Features	Storage Temperature: -20 ° C to + 70 ° C		
15.	General Features	Humidity (operation): 10% to 90% non-condensing		
16.	Network Virtualization Technologies	2 or more switches must be able to form a single virtual switch unit to achieve high resiliency, by allowing connecting devices to dual home to the virtual switch unit using standard link aggregation protocol in a non-blocking architecture.		
17.	Network Virtualization Technologies	Virtualization technology must support a unified data and management plane with a single IP address for management and communications		
18.	Network Virtualization Technologies	Virtualization technology must support the SPB-M protocol, without using of VRRP or Link Aggregation protocols to run it.		
19.	Network Virtualization Technologies	When operating in a chassis virtualization environment, the switch must be able to be upgraded individually without requiring every device in the logical chassis to reboot together.		
20.	L3 Protocols and Features	Multiple Virtual Routing and Forwarding (VRF) to segment Layer 3 traffic into virtual routing domains on the same switch. Each routing instance independently maintains its own routing and forwarding table, peer, and interface information.		
21.	L3 Protocols and Features	Routing Information Protocol v1, v2, RIPng.		
22.	L3 Protocols and Features	Open Shortest Path First Protocol V2, V3		

Sl. No	Features	Minimum specs	Compliance (Yes/No)	Deviations (Yes/No)
23.	L3 Protocols and Features	Border Gateway Protocol V4		
24.	L3 Protocols and Features	Virtual Routing Redundancy Protocol V2, V3		
25.	L2 Protocols and Features	Ethernet – IEEE 802.3i 10BASE-T.		
26.	L2 Protocols and Features	Fast Ethernet – IEEE 802.3u 100BASE-TX.		
27.	L2 Protocols and Features	Gigabit Ethernet – IEEE 802.3z 1000BASE-X, IEEE 802.3ab 1000BASE-T, IEEE 802.3af Power over Ethernet, IEEE 802.3at PoE Plus		
28.	L2 Protocols and Features	10G Ethernet - IEEE 802.3ae, IEEE 802.3an 10 GBase-T, IEEE 802.3bz 2.5/5 GigE		
29.	L2 Protocols and Features	40G Ethernet - IEEE 802.3ba, IEEE 802.3bm 40/100 GigE		
30.	L2 Protocols and Features	IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports.		
31.	L2 Protocols and Features	IEEE 802.3bm (CAUI-4,100GBASE-SR4 clause 95), IEEE 802.3bj (100Base-KR4 clause 93, 100GBase-CR4), IEEE 802.3ba (100GBASE-LR4,ER4 clause 88), IEEE 802.3by 25 Gig Ethernet		
32.	L2 Protocols and Features	IEEE 802.1ak (Multiple VLAN Registration Protocol MVRP)		
33.	L2 Protocols and Features	Shortest Path Bridging (SPB) to provide mesh connection with all links active - IEEE 802.1aq		
34.	L2 Protocols and Features	Link Layer Discovery Protocol (LLDP) for exchanging information with neighbour – 802.1AB.		
35.	L2 Protocols and Features	4,094 VLAN IDs per switch.		
36.	L2 Protocols and Features	VLAN trunking and tunnelling – IEEE 802.1Q (VLAN) and IEEE 802.3Q tunnelling (Q-in-Q).		

Sl. No	Features	Minimum specs	Compliance (Yes/No)	Deviations (Yes/No)
37.	L2 Protocols and Features	Link aggregation – IEEE 802.3ad.		
38.	L2 Protocols and Features	Spanning Tree Protocol (STP) – IEEE 802.1D.		
39.	L2 Protocols and Features	Rapid Spanning Tree Protocol (RSTP) – IEEE 802.1w.		
40.	L2 Protocols and Features	Multiple Spanning Tree Protocol (MST) – IEEE 802.1s.		
41.	L2 Protocols and Features	Per-VLAN Spanning Tree Plus (PVST+) and Per-VLAN Rapid Spanning Tree (PVRST).		
42.	L2 Protocols and Features	Spanning-Tree Protocol Port Fast Forwarding.		
43.	L2 Protocols and Features	Spanning-Tree Root Guard (STRG) which prevents edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.		
44.	L2 Protocols and Features	User Port mechanism which drop the packets or shuts down the port when it detect control packets like BGP, BPDU, RIP, OSPF, VRRP, DVMRP, PIM, ISIS, DHCPSERVER and DNS-REPLY.		
45.	L2 Protocols and Features	Jumbo frames of 9,216 bytes.		
46.	L2 Protocols and Features	Automatic media-dependent interface crossover (MDIX) which automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed.		
47.	L2 Protocols and Features	Unidirectional Link Detection Protocol (UDLD) that allows unidirectional links caused by incorrect fiber-optic wiring or port faults to be detected and disabled on fiber-optic interfaces.		
48.	Multicast Protocols and Features	IGMPv1/v2/v3 snooping and Multicast Listener Discovery (MLD) v1/v2 for fast client joins and leaves of multicast		

Sl. No	Features	Minimum specs	Compliance (Yes/No)	Deviations (Yes/No)
		streams and limit bandwidth-intensive video traffic to only the requestors.		
49.	Multicast Protocols and Features	Protocol Independent Multicast – Sparse-Mode (PIM-SM), Source Specific Multicast (PIM-SSM).		
50.	Multicast Protocols and Features	Protocol Independent Multicast – Dense-Mode (PIM-DM), Bidirectional Protocol Independent Multicast (PIM-BiDir)		
51.	Multicast Protocols and Features	Distance Vector Multicast Routing Protocol (DVMRP)		
52.	Multicast Protocols and Features	Multicast Listener Discovery (MLD) v1/v2 snooping		
53.	Security Features	Per-port broadcast, multicast, and unicast storm control which prevents faulty end stations from degrading overall systems performance.		
54.	Security Features	Build in mechanism which rate limits the traffic to the switching processor CPU and thereby ensuring stability, availability and predictable network performance.		
55.	Security Features	TACACS or RADIUS authentication to facilitate centralized control of the switch and restrict unauthorized users from altering the configuration.		
56.	Security Features	Controls communication between peer users in a way that each session comprises of a set of user ports and/or a set of network ports. The user ports within a session cannot communicate with each other and can only communicate through network ports		
57.	Security Features	Per-port broadcast, multicast, and unicast storm control which prevents faulty end stations from degrading overall systems performance.		
58.	Security Features	Build in mechanism which rate limits the traffic to the switching processor CPU and thereby ensuring stability, availability and predictable network performance.		

Sl. No	Features	Minimum specs	Compliance (Yes/No)	Deviations (Yes/No)
59.	Access Control Lists (ACL) Features	VLAN based ACL (VACL) on all VLANs to prevent unauthorized data flows to be bridged within VLANs and to provide granular control for limited access within a VLAN or subnet.		
60.	Access Control Lists (ACL) Features	Port-based ACL for Layer 2 interfaces to allow security policies to be applied on individual switch ports.		
61.	Access Control Lists (ACL) Features	Time-based ACL to control the switching of data based on the time of day and week. These security settings are implemented automatically during the specific periods of the day or days of the week.		
62.	Quality of Service (QoS) Features	Standard 802.1p CoS and DSCP field classification provided, using marking and reclassification on a per-packet basis by source and destination IP address, source and destination MAC address, or Layer 4 TCP or UDP port number.		
63.	Quality of Service (QoS) Features	Automatic QoS that simplifies QoS configuration in voice over IP (VoIP) networks by issuing interface and global switch commands to detect IP phones, classify traffic, and help enable egress queue configuration.		
64.	Quality of Service (QoS) Features	Control-plane and data-plane QoS ACLs on all ports help ensure proper marking on a per-packet basis.		
65.	Quality of Service (QoS) Features	Strict priority queuing to ensure that the highest-priority packets (such as voice or other mission critical packets) are serviced ahead of all other traffic.		
66.	Quality of Service (QoS) Features	Rate limiting is provided based on source and destination IP address, source and destination MAC address, Layer 4 TCP and UDP information, or any combination of these fields, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps.		

Sl. No	Features	Minimum specs	Compliance (Yes/No)	Deviations (Yes/No)
67.	Quality of Service (QoS) Features	Ingress policing and egress shaping so as to provide asynchronous data flows upstream and downstream from the end station.		
68.	Quality of Service (QoS) Features	Eight egress queues per port help enable differentiated management of different traffic types across the stack.		
69.	Switch Management and Operation Features	Port mirroring (one to one, many to one) which allows monitoring of traffic on one or more ports and send the monitored traffic to a destination ports.		
70.	Switch Management and Operation Features	Remote Port Mirroring which expands the port mirroring functionality by allowing mirrored traffic to be carried over the network to a remote switch.		
71.	Switch Management and Operation Features	Sampling technology like sFlow which gives visibility into the activity of the network, by providing network usage information.		
72.	Switch Management and Operation Features	Switch must be able to synchronize the date and time with an external time source using protocol like NTP. This is to ensure all switches are having the same time and help in troubleshooting.		
73.	Switch Management and Operation Features	Support Open Standard Plug-N-Play Operation such that a new switch can auto detect and join into existing fabric using protocol like LACP, SPB and MVRP.		
74.	IPv6 Specifications	Telnet, SSH, FTP and SFTP over IPv6		
75.	IPv6 Specifications	DNS for IPv6		
76.	IPv6 Specifications	ICMPv6 and neighbour discovery protocol (NDP) for IPv6		
77.	IPv6 Specifications	SNMP traps to IPv6 trap receiver.		
78.	Enhanced Security Features	Restricts access to the switch only for certain IP addresses (configured as management station).		
79.	Enhanced Security Features	Bans those IP addresses permanently from further access on invalid authentication attempts reaching threshold limit.		

Sl. No	Features	Minimum specs	Compliance (Yes/No)	Deviations (Yes/No)
80.	Enhanced Security Features	Provides option to configure privileges for all access types, align IP services dynamically with AAA authentication configuration.		
81.	Enhanced Security Features	Restricts only one session per user		
82.	Enhanced Security Features	Option for password obscuring to prohibit disclosure while entering the password.		
83.	Enhanced Security Features	Option to configure user passwords with SHA-224/256 (SHA-2) or SHA-2+AES encryption.		
84.	Enhanced Security Features	SSH/SSL Pub Key		
85.	Enhanced Security Features	Restricts only one session per user		
86.	Enhanced Security Features	Separate user password for SNMPv3 frame authentication/encryption.		
87.	Enhanced Security Features	Provides option to verify the integrity of the images in a given directory is matching with the SHA-2 (SHA256 or 512 key) shared along with the image file.		
88.	Enhanced Security Features	Process Self-Test functional commands to view the major hardware and software process status.		
89.	Enhanced Security Features	Support of TLS 1.2 version for TLS connections.		
90.	Programmable RESTful API	Programmable RESTful API		
91.	Programmable RESTful API	Fully programmable OpenFlow 1.3.1 and 1.0 agent for control of native OpenFlow and hybrid ports.		
92.	Programmable RESTful API	OpenStack networking plug-in		
93.	Programmable RESTful API	Software-controlled VXLAN hardware VTEP gateway		

Sl. No	Features	Minimum specs	Compliance (Yes/No)	Deviations (Yes/No)
94.	Multipath Ethernet Technologies	Uses IP-encapsulated MAC routing that works over any network that supports IP and is designed to scale across multiple datacentres.		
95.	Multipath Ethernet Technologies	Preserves existing Layer 3 failure boundaries, provides multihoming and built-in loop prevention across multiple datacentres		
96.	Additional Features	Support for MACsec, IEEE 1588 PTP transparent clock, Multiprotocol Label		
97.	Additional Features	Switching (MPLS)		
98.	Additional Features	Support Data Center Bridging features including Priority-Based Flow Control (802.1Qbb), Enhanced Transmission Selection(802.1Qaz) and Data Center Bridging Exchange (DCBx) to enable LAN-SAN convergence with iSCSI and FCoE.		
99.	Additional Features	Support 802.1aq Shortest Path Bridging to enable the creation of a fully meshed architecture with all active network path		
100.	Additional Features	The switch must offer simplified programmatic management using RESTful web services with XML and JSON support.		
101.	Additional Features	The switch must support out-of-band management and monitoring capability that bypasses the network modules and offer remote management to the management module directly		
102.	Additional Features	The switch must support Intuitive CLI in a scriptable Python and Bash environment through console, Telnet or Secure Shell (SSH) v2 over IPv4/IPv6		
103.	Additional Features	The switch must support Virtual eXtensible LAN (VXLAN) Snooping feature which attempts to detect and identify VXLAN traffic by sampling packets to determine if they are VXLAN encapsulated packets.		

Sl. No	Features	Minimum specs	Compliance (Yes/No)	Deviations (Yes/No)
104.	Additional Features	The switch will attempt to detect and identify remote applications by scanning IP packets and comparing the packets to pre-defined bit patterns (application signatures). Once an application is identified, the switch collects and stores information about the application flow in a database on the local switch		
105.	Additional Features	The switch must support build in DHCP server providing IPv4 and IPv6 address to end devices.		
106.	Additional Features	The switch must support build in cloud agent which will perform a call home and manage by the management server in the cloud. The same switch must also be able to manage by on-premises management server in the event when cloud is not available.		
107.	Additional Features	The switch must support a Fabric Technology that can self-configure, self-attachment and self-healing of the network through Auto-Fabric, eliminating many manual task and human error during deployment process.		
108.	Additional Features	The switch must come with IoT Device Profiling which uses DHCP Finger Printing and MAC OUI (MAC Vendors) to identify IoT devices.		
109.	Additional Features	The switch must have the capability of propagating switch configurations, such as user profiles or device profiling signature across the network to other switches. This feature leverages the publisher/subscriber relationship, community names and topics to publish configuration information between switches.		
110.	Additional Features	Port Security secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address-flooding.		

Sl. No	Features	Minimum specs	Compliance (Yes/No)	Deviations (Yes/No)
111.	Additional Features	Early ARP discard - ARP packets destined for other hosts are discarded to reduce processing overhead and exposure to ARP DoS attacks.		
112.	Additional Features	Prevent IP address spoofing using user port mechanism which can either drop the packets or shuts down the port		
113.	Compliance and certifications	FCC 47 CFR Part 15 Class A, EN55022, EN55024, EN61000-3-2, EN61000-3-3, EN61000-4-D1242, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN61000-4-8, EN61000-4-11, CISPR22:1997 (Class A), VCCI (Class A)		
114.	Compliance and certifications	US UL 60950, IEC/EN/ 60950-1, EN 60825-1 Laser, EN 60825-2 Laser, CDRH Laser, FIPS 140-2, Common Criteria EAL2, Common Criteria NDcPP, ITU-T G.8032/Y.1344		

1.9. Managed Access Switch

Sl. No	Features	Minimum specs	Compliance (Yes/No)	Deviations (Yes/No)
Make				
Model				
1	General	Non-blocking equipment		
2		Total RU: 1 RU maximum		

Sl. No	Features	Minimum specs	Compliance (Yes/No)	Deviations (Yes/No)
3		Power Supply must be internal and integrated into the switch		
4		SFP`s Hot Swap		
5		Minimum of 24 ports 10/100/1000 Base T RJ45 with PoE+		
6		Minimum of 2 SFP+ ports (1/10Gbps) for Uplink or VFL		
7		Minimum of 2 1000BaseT/SFP combo ports upgradeable to 10GbaseT/SFP+		
8		Equipment MUST support Variable Speed Fans		
9		Maximum Stack of 4 elements (Single Management IP)		
10		Minimum switching capacity of 128Gbps		
11		Switch capacity with all ports (full duplex + VFL) of 92Gbps		
12		Minimum VFL (aggregated) of 40Gbps		
13		Minimum Processing Capacity (Mpps): 137 Mpps		
14		Operating Temperature: 0°C to 45°C		
15		Humidity (operation): 5% to 95% non-condensing		
16		Power Supply efficiency (max load) of 95.7%		
17		MTBF (hours) @ 25ºC: 1.447.000		
18		System power consumption idle of 32W		
19		System power consumption 100% traffic all ports of 46W		
20		PoE Budget of 380W		
21	Resiliency and high availability functionalities	Unified management, control and virtual chassis technology		
22		Virtual Chassis 1+N redundant supervisor manager		
23		Virtual Chassis In-Service Software Upgrade (ISSU)		
24		Smart continuous switching technology		
25		IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) encompasses IEEE 802.1D Spanning Tree Protocol (STP) and IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)		
26		Per-VLAN spanning tree (PVST+) and 1x1 STP mode		

Sl. No	Features	Minimum specs	Compliance (Yes/No)	Deviations (Yes/No)
27		IEEE 802.3ad/802.1AX Link Aggregation Control Protocol (LACP) and static LAG groups across modules		
28		Virtual Router Redundancy Protocol (VRRP) with tracking capabilities		
29		IEEE protocol auto-discovery		
30		Bidirectional Forwarding Detection (BFD) for fast failure detection and reduced re-convergence times in a routed environment		
31		Redundant and hot-swappable power supplies		
32		Built-in CPU protection against malicious attacks		
33		Split Virtual Chassis protection		
34	L3 protocols and features	Static routing for IPv4 and IPv6		
35		Up to 64 IPv4 and 4 IPv6 static routes		
36		Up to 32 IPv4 and 4 IPv6 interfaces		
37	layer-2 capabilities	Up to 16k MAC Addresses		
38		Up to 4000 VLANs		
39		Up to 1.5k total system policies		
40		Latency: < 4 µs		
41		Max Frame: 9216 bytes (jumbo)		
42	Multicast protocols and features	IGMPv1/v2/v3 snooping to optimize multicast traffic		
43		Multicast Listener Discovery (MLD) v1/v2 snooping+		
44		Up to 1000 multicast groups		
45	Security features	Autosensing IEEE 802.1X multiclient, multi-VLAN support		
46		MAC-based authentication for non-IEEE 802.1X hosts		
47		Web based authentication (captive portal): a customizable web portal residing on the switch		
48		Dynamically provide pre-defined policy configuration to authenticated clients — VLAN, ACL, BW		

Sl. No	Features	Minimum specs	Compliance (Yes/No)	Deviations (Yes/No)
49		User Network Profile (UNP) simplifies NAC by dynamically providing pre-defined policy configuration to authenticated clients — VLAN, ACL, BW		
50		Secure Shell (SSH) with public key infrastructure (PKI) support		
51		Terminal Access Controller Access- Control System Plus (TACACS+) client		
52		Centralized Remote Access Dial- In User Service (RADIUS) and Lightweight Directory Access Protocol (LDAP) administrator authentication		
53		Centralized RADIUS for device authentication and network access control authorization		
54		Learned Port Security (LPS) or MAC address lockdown		
55		Access Control Lists (ACLs); flow-based filtering in hardware (Layer 1 to Layer 4)		
56		DHCP Snooping, DHCP IP and Address Resolution Protocol (ARP) spoof protection		
57		ARP poisoning detection		
58		IP Source Filtering as a protective and effective mechanism against ARP attacks		
59		Role-based authentication for routed domains		
60		BYOD provides on-boarding of guest, IT/non-IT issued and silent devices; restriction/remediation of traffic from non-compliant devices. RADIUS CoA dynamically enforces User Network Profiles based on authentication, profiling, posture check of devices using Unified Policy Access Manager (UPAM)		
61	Quality of Service (QoS) features	Priority queues: Eight hardware based queues per port for flexible QoS management		
62		Traffic prioritization: Flow-based QoS with internal and external (a.k.a., remarking) prioritization		

Sl. No	Features	Minimum specs	Compliance (Yes/No)	Deviations (Yes/No)
63		Bandwidth management: Flow-based traffic policing and bandwidth management, ingress rate limiting; egress rate shaping per port		
64		Queue management: Configurable scheduling algorithms — Strict Priority Queuing (SPQ), Weighted Round Robin (WRR)		
65		Congestion avoidance: Support for End- to-End Head-Of-Line (E2EHOL) Blocking Protection		
66		Auto QoS for switch management traffic		
67	Software Defined Networking (SDN) features	Fully programmable RESTful web services interface with XML and JSON support. API enables access to CLI and individual mib objects.		
68	Management features	Intuitive CLI in a scriptable BASH environment via console, Telnet, or Secure Shell (SSH) v2 over IPv4/IPv6		
69		Powerful WebView Graphical Web Interface via HTTP and HTTPS over IPv4/ IPv6+		
70		File upload using USB, TFTP, FTP, SFTP, or SCP using IPv4/IPv6		
71		Human-readable ASCII-based configuration files for off-line editing, bulk configuration, and out-of-the-box auto-provisioning		
72		Multiple microcode image support with fallback recovery		
73		Dynamic Host Configuration Protocol (DHCP) relay for IPv4/IPv6		
74		DHCPv4 and DHCPv6 server		
75		Loopback IP address support for management per service		
76		Policy- and port-based mirroring		
77		Remote port mirroring		

Sl. No	Features	Minimum specs	Compliance (Yes/No)	Deviations (Yes/No)
78		sFlow v5 and Remote Monitoring (RMON)		
79	Compliance and certifications			
80		EN 50581, EN 55022, EN 55024: 2010 ,EN 61000-3-2, EN 61000-3-3, EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11		
81		Compliant with RoHS, EN 60825-1/2		

1.10. SAN Switch

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
Make				
Model				
1.	Fibre Channel Generation	32GBps		
2.	Total Active Ports	48 Ports		
3.	Fibre Channel Port Speed (Gbps)	32		
4.	Media Type	SR		
5.	Aggregate Switch Bandwidth FC (end to end full duplex)	1536 Gbps		
6.	Form factor (U)	Max 2U		
7.	Autosensing (Gbps)	8/16/32		
8.	Port Types	U/E/F/M/D		
9.	AC Power Supply’s	Dual Redundant Hot Swappable AC Power Supply		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
10.	Non-Blocking Architecture	Yes		
11.	ISL Trunking	Yes		

1.11. Aggregation Switch

Sl. No	Features	Specifications	Compliance (Yes / No)	Deviations (Yes / No)
	Make			
	Model			
1	**General Features**	Non-blocking switching fabric with all Transceivers from same OEM		
2		Support for redundant and hot swappable power supplies and hot swappable SFPs		
3		Minimum installed of 48 SFP+ ports, with growth capacity up to 72 SFP+		
4		Support a minimum of 6 ports at 40Gbps per equipment.		
5		Minimum Switching Capacity (Gbps): 1440 Gbps,Minimum Processing Capacity (Mpps): 1000Mpps		
6		Operating Temperature: 0 ° C to 45 ° C, Storage Temperature: -10 ° C to + 70 ° C,Humidity (operation): 5% to 90% non-condensing		
8	**Network Virtualization Technologies**	The switch must be capable of creating a low latency, virtualization fabric architecture that scales to 600Gbps throughput.		
9		All switches must be able to form a single virtual switch unit to achieve high resiliency, by allowing connecting devices to dual home to the virtual switch unit using standard link aggregation protocol in a non-blocking architecture.		
10		Virtualization technology must support a unified data and management plane with a single IP address for management and communications		

Sl. No	Features	Specifications	Compliance (Yes / No)	Deviations (Yes / No)
11		Virtualization technology must support the SPB-M protocol, without using of VRRP or Link Aggregation protocols to run it.		
12		Support up to 6 switches to be virtualized into a single virtual switch unit.		
13		When operating in a chassis virtualization environment, the DC switch must be able to be upgraded individually without requiring every device in the logical chassis to reboot together.		
14		The switch must support MAC Retention which allows a system of stackable switches to retain the MAC address of the primary switch for a fixed or indefinite time, even after multiple takeovers. This minimizes the recalculation of protocols, such as Spanning Tree and Link Aggregation.		
15	**L3 Protocols and Features**	Multiple Virtual Routing and Forwarding (VRF) to segment Layer 3 traffic into virtual routing domains on the same switch. Each routing instance independently maintains its own routing and forwarding table, peer, and interface information.		
16		RIPv1, v2, RIPng, OSPF V2,OSPF V3, BGPv4, VRRPv2,VRRPv3, Policy based Routing,DHCP Relay, ICMPv6, Network Discovery Protocol (NDP), IGMP v1/v2/v3 snooping, IPv4/IPv6 security ACL		
17	**L2 Protocols and Features**	Ethernet – IEEE 802.3i 10BASE-T,Fast Ethernet – IEEE 802.3u 100BASE-TX,Gigabit Ethernet – IEEE 802.3z 1000BASE-X and IEEE 802.3ab 1000BASE-T,10G Ethernet - IEEE 802.3ae,40G Ethernet - IEEE 802.3ba, IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports,IEEE 802.1ak (Multiple VLAN Registration Protocol MVRP)		
18		Shortest Path Bridging (SPB) to provide mesh connection with all links active - IEEE 802.1aq		
19		Link Layer Discovery Protocol (LLDP) for exchanging information with neighbour – 802.1AB.		
20		4,094 VLAN IDs per switch, Jumbo frames of 9,216 bytes.		

Sl. No	Features	Specifications	Compliance (Yes / No)	Deviations (Yes / No)
21		VLAN trunking and tunnelling – IEEE 802.1Q (VLAN) and IEEE 802.3Q tunnelling (Q-in-Q).		
22		Link aggregation – IEEE 802.3ad,Spanning Tree Protocol (STP) – IEEE 802.1D,Rapid Spanning Tree Protocol (RSTP) – IEEE 802.1w,Multiple Spanning Tree Protocol (MST) – IEEE 802.1s,Per-VLAN Spanning Tree Plus (PVST+) and Per-VLAN Rapid Spanning Tree (PVRST),Spanning-Tree Protocol Port Fast Forwarding.		
23		Spanning-Tree Root Guard (STRG) which prevents edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.		
24		User Port mechanism which drop the packets or shuts down the port when it detect control packets like BGP, BPDU, RIP, OSPF, VRRP, DVMRP, PIM, ISIS, DHCPSERVER and DNS-REPLY.		
25		Automatic media-dependent interface crossover (MDIX) which automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed.		
26		Unidirectional Link Detection Protocol (UDLD) that allows unidirectional links caused by incorrect fiber-optic wiring or port faults to be detected and disabled on fiber-optic interfaces.		
27	**Multicast Protocols and Features**	IGMPv1/v2/v3 snooping and Multicast Listener Discovery (MLD) v1/v2 for fast client joins and leaves of multicast streams and limit bandwidth-intensive video traffic to only the requestors.		
28		Multicast VLAN Registration (MVR) continuously sends multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons.		
29		Protocol Independent Multicast – Sparse-Mode (PIM-SM), Source Specific Multicast (PIM-SSM).		

Sl. No	Features	Specifications	Compliance (Yes / No)	Deviations (Yes / No)
30		Protocol Independent Multicast – Dense-Mode (PIM-DM), Bidirectional Protocol Independent Multicast (PIM-BiDir)		
31		Distance Vector Multicast Routing Protocol (DVMRP)		
32		Multicast Listener Discovery (MLD) v1/v2 snooping		
33	**Security Features**	Per-port broadcast, multicast, and unicast storm control which prevents faulty end stations from degrading overall systems performance.		
34		Build in mechanism which rate limits the traffic to the switching processor CPU and thereby ensuring stability, availability and predictable network performance.		
35		TACACS or RADIUS authentication to facilitate centralized control of the switch and restrict unauthorized users from altering the configuration.		
36		Controls communication between peer users in a way that each session comprises of a set of user ports and/or a set of network ports. The user ports within a session cannot communicate with each other and can only communicate through network ports		
37	**Access Control Lists (ACL) Features**	VLAN based ACL (VACL) on all VLANs to prevent unauthorized data flows to be bridged within VLANs and to provide granular control for limited access within a VLAN or subnet.		
38		Port-based ACL for Layer 2 interfaces to allow security policies to be applied on individual switch ports.		
39		Time-based ACL to control the switching of data based on the time of day and week. These security settings are implemented automatically during the specific periods of the day or days of the week.		
40	**Quality of Service (QoS) Features**	Standard 802.1p CoS and DSCP field classification provided, using marking and reclassification on a per-packet basis by source and destination IP address, source and destination MAC address, or Layer 4 TCP or UDP port number.		

Sl. No	Features	Specifications	Compliance (Yes / No)	Deviations (Yes / No)
41		Automatic QoS that simplifies QoS configuration in voice over IP (VoIP) networks by issuing interface and global switch commands to detect IP phones, classify traffic, and help enable egress queue configuration.		
42		Control-plane and data-plane QoS ACLs on all ports help ensure proper marking on a per-packet basis.		
43		Strict priority queuing to ensure that the highest-priority packets (such as voice or other mission critical packets) are serviced ahead of all other traffic.		
44		Rate limiting is provided based on source and destination IP address, source and destination MAC address, Layer 4 TCP and UDP information, or any combination of these fields, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps.		
45		Ingress policing and egress shaping so as to provide asynchronous data flows upstream and downstream from the end station.		
46		Support for end-to-end head-of-line (E2E-HOL) blocking prevention, IEEE 802.1Qbb Priority-based Flow Control (PFC) and IEEE 802.3x Flow Control (FC) for congestion avoidance.		
47		Eight egress queues per port help enable differentiated management of different traffic types across the stack.		
48	**Switch Management and Operation Features**	Port mirroring (one to one, many to one) which allows monitoring of traffic on one or more ports and send the monitored traffic to a destination ports.		
49		Remote Port Mirroring which expands the port mirroring functionality by allowing mirrored traffic to be carried over the network to a remote switch.		
50		Sampling technology like sFlow which gives visibility into the activity of the network, by providing network usage information.		
51		Switch must be able to synchronize the date and time with an external time source using protocol like NTP. This is to ensure all switches are having the same time and help in troubleshooting.		

Sl. No	Features	Specifications	Compliance (Yes / No)	Deviations (Yes / No)
52		Support Open Standard Plug-N-Play Operation such that a new switch can auto detect and join into existing fabric using protocol like LACP, SPB and MVRP.		
53	**IPv6 Specifications**	Telnet, SSH, FTP and SFTP over IPv6,DNS for IPv6, ICMPv6 and neighbour discovery protocol (NDP) for IPv6, SNMP traps to IPv6 trap receiver.		
54	**Software Defined Networking (SDN) Features**	Programmable RESTful API		
55		Fully programmable OpenFlow 1.3.1 and 1.0 agent for control of native OpenFlow and hybrid ports.		
56		OpenStack networking plug-in compatible with Grizzly or higher		
57		Software-controlled VXLAN hardware VTEP gateway		
58	**Multipath Ethernet Technologies**	Uses IP-encapsulated MAC routing that works over any network that supports IP and is designed to scale across multiple datacenters.		
59		Preserves existing Layer 3 failure boundaries, provides multihoming and built-in loop prevention across multiple datacenters		
60		Support forwarding model on 16-way Equal-Cost Multi-Path (ECMP) routing to add capacity dynamically without network disruption		
61		Support L3-VPN service or VPN-Lite routing protocol for handling L3 traffic.		
62	**Additional Features**	Support seamless VM mobility by classifying the incoming server traffic based on MAC address, IP address or VLAN tag and assign an appropriate profile to the servers. The profile will determine the VLAN, priority, security and rate limiting parameters of that servers.		
63		Support Data Center Bridging features including Priority-Based Flow Control (802.1Qbb), Enhanced Transmission Selection(802.1Qaz) and Data Center Bridging Exchange (DCBx) to enable LAN-SAN convergence with iSCSI and FCoE.		

Sl. No	Features	Specifications	Compliance (Yes / No)	Deviations (Yes / No)
64		Support Multi-hop FCoE transit switching with FCoE Initialization Protocol (FIP) snooping capability		
65		Support 802.1aq Shortest Path Bridging to enable the creation of a fully meshed architecture with all active network path		
66		The switch must offer simplified programmatic management using RESTful web services with XML and JSON support.		
67		The switch must support the implementation of Edge Virtual Bridging (EVB) and Virtual Ethernet Port Aggregator (VEPA – IEEE802.1Qbg)		
68		The switch must support out-of-band management and monitoring capability that bypasses the network modules and offer remote management to the management module directly		
69		The switch must support Intuitive CLI in a scriptable Python and Bash environment through console, Telnet or Secure Shell (SSH) v2 over IPv4/IPv6		
70		The switch must support high availability hardware Virtual Extensible LAN (VXLAN) Virtual Tunnel End Point (VTEP) gateway so as to support layer 2 overlay network that is used to segment and tunnel device traffic through a data center or cloud network infrastructure. (applicable to model 2e and 2f only)		
71		The switch must support Virtual extensible LAN (VXLAN) Snooping feature which attempts to detect and identify VXLAN traffic by sampling packets to determine if they are VXLAN encapsulated packets.		
72		The switch will attempt to detect and identify remote applications by scanning IP packets and comparing the packets to pre-defined bit patterns (application signatures). Once an application is identified, the switch collects and stores information about the application flow in a database on the local switch		
73		The switch must support build in DHCP server providing IPv4 and IPv6 address to end devices.		

Sl. No	Features	Specifications	Compliance (Yes / No)	Deviations (Yes / No)
74		The switch must support build in cloud agent which will perform a call home and manage by the management server in the cloud. The same switch must also be able to manage by on-premises management server in the event when cloud is not available.		
75		The switch must support a Fabric Technology that can self-configure, self-attachment and self-healing of the network through Auto-Fabric, eliminating many manual task and human error during deployment process.		
76		The switch must come with IoT Device Profiling which uses DHCP Finger Printing and MAC OUI (MAC Vendors) to identify IoT devices.		
77		The switch must have the capability of propagating switch configurations, such as user profiles or device profiling signature across the network to other switches. This feature leverages the publisher/subscriber relationship, community names and topics to publish configuration information between switches.		
78		Port Security secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address-flooding.		
79		Early ARP discard - ARP packets destined for other hosts are discarded to reduce processing overhead and exposure to ARP DoS attacks.		
80		Prevent IP address spoofing using user port mechanism which can either drop the packets or shuts down the port		
81	**Industry Certifications**	EN55022:1998:2006, EN55024 :1998:A1:2001+A2:2003, EN61000-3-2, EN61000-3-3, EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN61000-4-8, EN61000-4-11,		

1.12. Intranet Router – 20 Mbps

Appliance hardware should be scalable to support up to 40 Mbps of throughput in each direction with all services like IPSec, DoS Protection and Stateful Firewall. Software license of 20 Mbps must be enabled from Day-1, upgradable up to 40 Mbps without requiring any hardware upgrade

Sl No.	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Make		
	Model		
1	The system should support at least 4 WAN Ports to be terminated on the branch device and 2 LAN interfaces and should also support at least 1 slot supporting 3G/4G SIM connections/LTE dongle		
2	The system should support internet links that can be authenticated using PPPOE		
3	The system should support 4G/LTE links natively on the branch device as a WAN link with the ability natively install at least one SIM card from an ISP or local Wireless Broadband Service Provider either using SIM Module or USB support for Broadband Dongle.		
4	The system should support termination of Internet Leased Line (ILL) on the branch device.		
5	The system must support minimum 1000 concurrent IPSec tunnel to support full mesh/partical mesh topology		

Sl No.	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
6	Appliance hardware should be scalable to support up to 40 Mbps of throughput in each direction with all services like IPSec, DoS Protection and Stateful Firewall. Software license of 20 Mbps must be enabled from Day-1, upgradable up to 40 Mbps without requiring any hardware upgrade		
7	The same device must support complete security features including Next Generation Firewall features like URL/IP filtering and Unified Threat Management portfolio (IPS, Antivirus, SSL decryption, etc.). If required by User, these features should be enabled on same device in future without any additional cost for hardware		
8	Appliance should support at least 500,000 IP routes		

1.13. Internet Router – 500 Mbps

Sl No.	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Make		
	Model		

Sl No.	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
1	Appliance should have 4x10/100/1000T Ethernet/SFP WAN ports, 1x4G LTE and 2 LAN ports. Appliance should have free slot to accommodate additional interface like Ethernet/4G LTE		
2	The system should support internet links that can be authenticated using PPPOE		
3	The system should support 4G/LTE links natively on the branch device as a WAN link using local Wireless Broadband Service Provider or USB support for Broadband Dongle.		
4	The system should support termination of Internet Leased Line (ILL) on the branch device.		
5	Appliance should support at least 1 Million IP routes to accommodate internet routing table		
6	The system should terminate MPLS as well as Broadband links to device and must be able to use both the links for traffic. Any failure of a link must result in steering traffic on another link without any manual intervention.		
7	The system must support minimum 2000 concurrent IPSec tunnel to support full mesh/partical mesh topology		
8	Appliance hardware should be scalable to support up to 500 Mbps of throughput in each direction with services like IPSec, DoS Protection and Stateful Firewall. Software license of 200 Mbps must be enabled on the device from Day-1		

Sl No.	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
9	The same device must support complete security features including Next Generation Firewall features like URL/IP filtering and Unified Threat Management portfolio (IPS, Antivirus, SSL decryption, etc.). If required by User, these features should be enabled on same device in future without any additional cost for hardware		

1.14. Core Router

Sl No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Make			
	Model			

Sl No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
1	General Requirement	The network should be implemented as true software defined network architecture, SD-WAN network architecture should have clear separation of management, control and data plane functions. Management and control plane should be centralized with capability to be separated for each tenant in such a way that management, control and data traffic are not intermingled. All Component of SD WAN should be on premise or on cloud. Management plane: management plane is responsible for configuration of SD-WAN policies including routing, security, SLA etc. Control Plane: Control plane is responsible to maintain centralized routing table, controls route advertisement as per policy, creates end to end segments on network, instruct data plane to change traffic flow as per policy. Data Plane: Data plane is responsible to forward traffic in encrypted tunnels, apply local policy like QoS, ACL etc. The network should be implemented as true software defined network architecture with a centralized control plane residing in the Central Controller, also Data Plane and Control Plane should be separate end-to-end		
2		Proposed solution should be in the form of Hardware and Virtual Appliance and must be Rack Mountable with Dual Power Supply for DC, DR and NDC in case of Hardware appliance.		
3		The software defined network centralised components need to be installed on-premises or on-cloud. All the required resources need to be provided by the Bidder and relevant cost to be included in submitted commercial proposal		
4		The communication between the software defined network controller and the branch device running on the remote entity should be secure and encrypted.		
5		The tunnel creation should be automatic without any manual configuration on the edges and the controller.		

Sl No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
6		The architecture should allow for internet break out at the local at branch, centralized location, remote entity (remote location) based on the application and the policy defined in the software defined network controller.		
7		The solution should allow network service insertion & service chaining to expand the agility and utility of the network. The solution should have ability to do services chaining with external PNFs or hosted VNFs. The VNF capability should be available on any SD-WAN edge devices.		
8		The system architecture should be transport agnostic and should support MPLS , ILL , Broadband, LTE, Dual Sim in Active Active Mode and other transport.		
9		The SD-WAN should be able to load balance across links simultaneously		
10		The SD-WAN should support SNMP V3, IPFix, Syslog exporter, etc for monitoring and reporting purpose		
11		The SD-WAN solution must be able to apply Qos policies to all the traffic seen in network ,including both optimized and non-optimized traffic flows ,including TCP,UDP and other non-TCP traffic types.		
12		The SD-WAN solution should include a Qos mechanism that is able to protect delay sensitive flows like Voice, Video, and VDI.		
13		The SD-WAN should support IPv4 & IPv6 dual stack from Day-1		
14		The SD-WAN should support 802.1Q		
15		The solution should support following IPv6 capabilities: * IPv6 addressing, IPv6 name resolution, IPv6 statistics, IPv6 neighbour discovery * ICMPv6, DHCP IPv6 * Support for the following IPv6 features: OSPFv3, BGP Routing over IPv6, IPv6 Dual Stack		

Sl No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
16		The software defined network controller must have REST APIs available for 3rd party integration or integration with custom automation tools		
17		SD-WAN solution should support multi-tenancy . This way multiple sub-organizations in User network (like Employees, Vendors, Partners, etc.) can utilize same Physical CPE , WAN Circuit and SD-WAN central components with total isolation across management, control and data plane		
18		SD-WAN solution should support route manipulation on LAN , WAN and Overlay to achieve various hybrid network integration requirements.		
19		SD-WAN solution should support native firewall to secure the Branch with Direct Internet Access for LAN or Guest users.		
20		SD-WAN solution should support Site to Site IPSec tunnel on LAN/WAN side with any third party IPSEC capable appliance for hybrid deployments.		
21		SD-WAN solution should build dynamic IPSEC tunnels using Asymmetric encryption (DH group) and should generate unique key for each site for better security.		
22		SD-WAN software must be supported on any standard x86 appliances for Branch ,Hub and DC.		
23		SD-WAN solution should have capability to mitigate the effect of packet drop in underlay up to some extent for specific or all applications using Forward Error Correction and Packet Replication to improve end-user experience		
24		The solution should allow to activate these features like FEC/Packet replication when configured SLA thresholds are breached and should deactivate the same when SLA of the link is within threshold again		

Sl No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
25		SD-WAN solution must support Hub-Spoke , Full-Mesh , Spoke-Hub-Hub-Spoke and Partial Mesh topologies.		
26		There has to be minimum two factor authentication between Controllers and central and branch devices before they established communication with each other. Out of two factors, one factor has to be PKI (certificate). The communication between the software defined network controller and the branch device running on the remote entity should be secure and encrypted		
27				
28		The solution should allow Branch sites without a common WAN provider to communicate with each other. (Ex. Branch1 has WAN1 connectivity and Branch 100 has WAN2 connectivity only, then they should be able to communicate with each other)		
29		SD-WAN solution should have intelligence to route Voice traffic based on MOS (mean opinion score) score		
30	Virtual Private Network	The system should allow creation of an encryption policy that has a unique encryption key attached		
31		The system should allow automated, policy driven and time-based refresh of the encryption key per virtual private network		
32		The system should only allow dynamic tunnels to be created without any static overlays between branch devices and the hub device.		
33		The system should support for Hub & Spoke, Partial Mesh, full mesh, topologies.		

Sl No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
34		The system should allow for alternate hub destinations to be created for application specific traffic using a policy defined for it.		
35		The system should be able to retrieve the network information without any peering protocols like BGP, OSPF or any other routing protocol over WAN.		
36		The system should ensure that the virtual private network specific configuration is not be attached to physical or logical WAN or LAN Links or IP addresses or physical interfaces on the branch device.		
37		The system should ensure that any change in physical connectivity (Link 1 to Link 2 connectivity in case of multiple links being terminated on the branch device) or any change is physical connectivity type (Link 1 connectivity changed from internet broadband to MPLS or vice versa, in case of multiple WAN links being terminated on the Branch device) does not require any change in virtual private network configuration in the controller or physical/virtual device at location.		
38		The system must be able to make virtual private network paths dynamically on power on without using of any routing protocols on the WAN side.		
39		The system should support the following encapsulation types: A. IPSEC B. GRE C. UDP D. No Encapsulation		
40		The system should be able to automatically pick the tunnel encapsulation type based on the application and based on the policy specified in the software defined network controller.		

Sl No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
41		The system should support the following authentication algorithms for Data Integrity: a. SHA-512 b. SHA-384 c. SHA-256		
42		The system should support the following encryption algorithms for Data Security a. AES-256 c. Any other FIPS approved encryption		
43		The system should ensure that virtual private network configuration and policy is performed in the controller. The addition of one or more branch devices into the network should not require any changes in the virtual private network configuration in software defined network controller.		
44	Network Performance, Traffic Management & Path Steering	The system should be able to prioritize inbound and outbound traffic.		
45		The system should be able to select the optimum path based on the network parameters like Latency, Jitter, packet loss and network capacity.		
46		The system should be able to identify Department critical applications and should prioritize this traffic over others during congestion.		
47		The solution must allow sub-second convergence in case of link or node failure. All traffic should move to other available link/node in <1 second		
48		The system should ensure that the session is not impacted when switching between paths		

Sl No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
49		The system should be able to support multiple internet break out points based on the application (e.g. The system should do a direct internet break out at the branch location for Microsoft Office 365 traffic while rest of the internet traffic should be egressed through a centralized security infrastructure in the data center or the cloud).		
50		The system should load balance the application traffic per packet and per session based on the requirement of the User.		
51		The SLA management should have fallback mechanism in place i.e. in case if both the links at a branch location fail to meet SLA, the traffic should not drop.		
52	Authentication, Authorization and Accounting (AAA)	The central management system should authenticate and authorize every administrator/user accessing the Central/branch device using the RADIUS/TACACS+ in the backend for the user authentication and authorization.		
53		All the admin activities should be logged and stored for audit purpose		
54		The system must be able to integrate with enterprise Active Directory services to provide user/user group-based control for various applications		
55		The solution should support 802.1x mechanism to allow network access control, MAC based whitelisting of devices and certificate-based authentication to allow only trusted devices with access into the network.		
56		The solution should be able to integrate with User existing Security Information and Event Management (SIEM) solution.		
57	Security	The system should implement a stateful firewall with Access Lists and/or Time-based Access lists to provide supervision and control on the branch device that can be centrally provisioned and managed from the software defined network controller.		

Sl No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
58		The SD-WAN should support DDoS mitigation functionality and protect DDOS attack like UDP Flood, Ping of Death etc.		
59		Controller and the device should be able to access only through web based for configuring and controlling. SSH,USB port and telnet should be disabled by default and console should be password protected.		
60		SD-WAN devices should have authentication and authorization only with the preconfigured Controller/Management server/Management Console which is placed in DC/DR		
61		The solution must upgradable into Next-Generation Firewall features like URL Filtering, IP Filtering, DNS proxy and DNS firewall. These features will not be enabled on the device since Day-1, however if requested by user, the same device must be able to support these features without need for any hardware upgrade.		
62	Visibility, Analytics, Monitoring & Reporting	The system should support application-level monitoring and traffic control to improve Department-critical application performance, facilitate capacity management and planning, and reduce network operating costs.		
63		The system should support the ability to automatically detect applications, report the application traffic, and allow for marking and filtering via policy.		
64		The system should allow user to define custom application based on multiple parameters such as protocol values, ports, patterns etc and tag application by family and sub-family like Department, non-Department, SaaS, by Risk categories etc. It should have capability to define traffic policies for such applications and categories and analytics report should capture all custom names and tags as defined by administrators		

Sl No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
65		The system should actively measure the link capacity without impacting more than 10% of the capacity of the link to carry traffic.		
66		The system should allow administrators of the network to be grouped with well-defined roles assigned to them. The system should support monitoring only user role, network change administrator role and an overall system administrator role with permissions to manage the software defined network controller.		
67		The system should allow monitoring of Packet loss ratio, Delay, Jitter, and Bandwidth utilization of each WAN link		
68		The SD-WAN should support granular Real-Time/near real time Monitoring and Historical Reporting like: a. Statistic bandwidth usage of available links b. Network statistics, including continuous performance monitoring of loss, latency, and packet loss for all network paths and link utilization		
69		The SD-WAN should be able to generate report for a. Traffic statistics of all the included path b. Specific application utilization c. Path performance		
70		The SD-WAN MUST provide following reports of Individual Link Quality on daily, weekly, monthly, yearly or configurable period basis. a. Packet loss in the links b. Jitter on the links c. Latency of Links		

Sl No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
71		The solution must be able to generate notifications for 1.Link Flaps at the remote branch location 2.ISP link quality degrade (high latency, high packet drops, etc) 3.Link utilization along with threshold 4. CPU, Memory and Disk Utilization of the Branch Device		
72		The notifications generated by the software defined network controller must be forwarded as email to a pre-configured email address. Moreover same should also be reflected on dashboard.		
73		The system must be able to monitor, and report top 20 applications by usage across all branch locations, in branch locations along with the data rate and flow usage. This data must be stored by the controller for a minimum of 30 days.		
74		The system must be able to monitor and report Top 10 LAN users by bandwidth usage and applications accessed by them in a branch location along with the data rate and flow usage. This data must be stored by the controller for a minimum of 30 days.		
75		The administration should be able to drill down the report for troubleshooting. for e.g. application accessd by a specific users along with bandwidth consumed during defined amount of time.		
76		The solution must be able to monitor and report top talkers in the network with respect to applications by usage, branch users utilizing maximum bandwidth and top access circuits utilized in the network. The administration should be able to drill down these reports for troubleshooting. For e.g. application accessed by specific users along with bandwidth consumed during defined amount of time.		
77		The data traffic from branch sites must not be impacted in case of failure to reach any of the controllers (headless situation). Data paths must be maintained for at least 12 hours without reachability to central management system (controller, orchestrator)		

Sl No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
78		SD-WAN devices should have capability to bind with any static hardware (i.e. switch, ATM etc.) MAC IDs available in the LAN at respective location. The Control/Management of MAC-ID binding and MAC-ID repository should be at central controller. The central controller/SDWAN device should probe the binded MAC-IDs for that SDWAN device on periodical basis/reboot/restart/power-on time. The SDWAN device should be automatically disabled if binded MAC IDs are Unrecognized/Unreachable by the SD-WAN device. OR SD-WAN devices should have capability to white-list devices (i.e. PC, NW Switch, ATM, Kiosk etc.) MAC IDs available in the LAN at respective location and SDWAN device should not allow access to any unrecognized/unknown MAC ID(s). The control/management of MAC-ID white-listing and MAC-ID repository should be at central controller. (The Bidders must be able to showcase the above feature during PoC)		
79	Management & Orchestration	The system should support a centralized single plane of management system to allow device configuration, policy provisioning, software updates and assurance capabilities for all components including SDWAN, security, VPN etc.		
80		The Solution should have simplified orchestration which should be placed in DC and DRC for provisioning, automation to control and to push configuration for all the devices.		
81		The solution should come with a web-based administration interface and GUI.		

Sl No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
82		Central Management Console to be provided in DC & DR. Both DC and DR SD-WAN controllers should be in active-standby mode. In case DC infra goes down, all the management and control traffic must also failover to DR to ensure manageability of devices is not impacted and Department continuity is achieved during such catastrophic events		
83		The system should provide a dashboard that provides state of appliances (Online, Offline, Current Software release, etc.)		
84		The system should support Zero Touch provision/minimum touch provisioning for Rapid site provisioning, Rapid deployment of new policies, configuration in a way that is secure and offers high performance.		
85		The system should be able to notify external systems of events such as faults/alarms as Syslog messages, SNMP (SNMPv3) traps, Telemetry		
86		The system must be able to send e-mail and SMS notification for events and alerts. The valid email addresses and numbers for receiving the SMS notifications should be configurable centrally.		
87	Network wide Policy Enforcement	The system should support centralized application of policies network wide or across subset of branch locations from the centralized software defined network controller.		
88		The system should allow definition and enforcement of traffic forwarding policies on the basis of application(s), application categories, from specific subnet(s), to specific subnet(s) and custom IP Address(es) for traffic from LAN to WAN on a branch.		
89		The system should allow definition and enforcement of traffic forwarding policies that allow encapsulation of the traffic with IPSEC		

Sl No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
		or UDP or GRE or no Encapsulation for all traffic going from the LAN to WAN or from WAN to LAN.		
90		The system should allow monitoring of Packet loss ratio, Delay, Jitter, and Bandwidth utilization of each WAN link. Administrator should be able to use these parameters to define traffic steering policies and monitor policy violations during threshold breach		
91		The system should allow definition and enforcement of WAN link load balancing policies that allow steering of application flows on a WAN link with best quality (flow based and packet-based load balancing) with the quality defined in terms of latency, packet loss and jitter.		
92		The SD-WAN should support both packet & flow-based load balancing across all links simultaneously to achieve better application performance. Load balancing must be configurable for different applications, for example FTP application should use per packet load balancing to optimize usage of all WAN links during large file transfers whereas applications like SAP should use per session load balancing to make optimum use of all underlay connectivity		
93		The SD-WAN must integrate transparently into the existing routing infrastructure. The solution should have capability to coexist with existing routing protocols (e.g. OSPF, BGP (iBGP and eBGP), IPSEC etc.).		
94	Multicast	The solution must support Multicast protocols in the overlay like PIM SM and PIM SSM		
95		The SD-WAN deployment must support Static RP, BSR and Anycast RP in order to provide deployment flexibility in the network		
96		The solution should support IGMP v2/v3		

Sl No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
97	Provisioning & Deployment	The system should allow for plug and play installation of branch devices without requiring any manual configuration or minimal manual configuration at the remote location		
98		The system should allow automatic software/patch/version upgrades from the software defined network controller across all deployed devices or a group of devices in the branch offices, data center and the cloud.		
99		The solution must allow to schedule upgrades for single or batch of devices and the process must be completely automated. In case of upgrade failure, the system should roll back to previous stable configuration and generate logs to analyse upgrade failure		
100		The system should be available and running when the software is being downloaded into the branch device from the central software defined controller.		
101	Data Center Deployment	The system should allow deployment of the SD-WAN Gateway appliance in the Data Center as a rack mounted physical appliance		
102		The SD-WAN Gateway appliance deployed in the Data Center should be able to peer with the existing routers in the Data Center		
103		The SD-WAN Gateway appliance should be capable of being deployed behind or in front of the existing firewall in the Data Center		
104		The SD-WAN Gateway appliance should also be available as software that can be deployed on hardware appliance (Intel x86 server) in the Data Center		
105		The system should allow for the automatic failover of the VPN tunnels to the disaster recovery data center from the branch if the data center is not reachable from the branch location [if the WAN connectivity to the Data Center is down or if the application hosted in the data center is not accessible.]		

Sl No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
106	High Availability	The solution must allow failover of complete management plane, control plane and data plane traffic from DC to DR in case of catastrophic failure at DC level.		
107		The software defined orchestrator should be architecturally highly available with Active-Active, Active-Stand as per discretion of User for high availability		
108	Data Center (DC) and Disaster Recovery Center (DR) SD-WAN Edge Device Specifications	The SD-WAN must be delivered by a physical hardware platform or Virtual platforms in DC/DR and should be rack mountable with Dual Power supply		
109		Appliance should support minimum 5000 IPSec tunnels		
110		The DC/DR SD-WAN appliances must handle upto 5 Gbps IPSec throughput in each direction with all feature Licenses enabled from Day-1 as mentioned in this RFP		
111		The SD-WAN device should have minimum: a. 8x1G Ethernet Routed Ports b. 4x10G SFP+ based WAN ports c. OOB management Port d. Console Port for local device access e. 2xUSB Ports which can support 4G LTE dongle for backup connectivity		
112		Appliance should support at least 10,00,000 IP routes including multicast		
113		Appliance should be IPv6 compatible from day-1		
114		Appliance should be provided with redundant AC power supplies and power cords		
115		Appliance hardware should be scalable to support up to 5 Gbps of throughput with all services like IPSec, DoS Protection and Stateful Firewall. Software license of 2 Gbps in each direction should be enabled on Day-1		

Sl No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
116		The same device must support complete security features including Next Generation Firewall features like URL/IP filtering and Unified Threat Management portfolio (IPS, Antivirus, SSL decryption, etc.). If required by User, these features should be enabled on same device in future without any additional cost for hardware		
117				
118	License and Support	The devices and software should be supported by the OEM on 24X7X365 basis		
120		All the functionality and feature license should be pre-installed and it should be usable from day one of operation.		
121		During the tenure, all the software/Patch/OS upgradation should be done by the Bidder/OEM with no Cost to User		
122		All the license part should be applied to all SD-WAN devices through central SDWAN controller		
123		Device should support minimum 10 segments/VRF/virtual domain for end-to-end segmentation of traffic like - Branches, HQ, department.		

1.15. Web Application Firewall

Sl. No.	Features	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
	Make:			
	Model:			

Sl. No.	Features	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
1.	Appliance	The appliance should be dedicated appliance and from different vendor than firewall and NGFW. Proposed appliance should support virtualization with each instance having capability to assigned dedicated hardware resources including I/O interfaces, memory, CPU, Hardware SSL card cores		
2.	Hardware Parameters	The Appliance should have deducted 8 x 10G SFP+ all prepopulated from day 1. Appliance should have minimum 128 GB RAM and 4 TB hard disk built in		
3.	Compliance	Should protect against OWASP top 10 vulnerabilities. The proposed WAF should be ICSA/ EAL4+/ NDPP/NSS Lab certified		
4.	Performance Parameters	The appliance should support minimum 45 Gbps of SSL throughput. Should support minimum 5 million L7 RPS and 20 Million Concurrent connections per second		
5.	HTTPS Performance Parameters	The appliance should support 50 K RSA SSL TPS for 2048 key and 35K ECC SSL TPS. The appliance should have dedicated SSL Acceleration hardware card for handling SSL Traffic.		
6.	Security Posture	Should support negative and positive security model. The positive security recognizes the characteristics of normal application traffic by automatic traffic learning in order to form the positive security model (whitelist model), which allows only traffic matching these whitelists to pass.		
7.	IP V6	Should respectively support working modes and protocol detection based on IPv4 and IPv6 environments, and be able to support IPv4 and IPv6 dual-stack environments;		
8.	Security features	Should support http normative inspection; support HTTP protocol decoding and check related fields, including URI, request method, response status code, HTTP header fields and other HTTP elements, etc.		

Sl. No.	Features	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
9.	Security features	The legality of the HTTP protocol should be verified based on the RFC, including the length of the HTTP Request line, URL length, protocol name length, header value length, transmission sequence and application format (such as HTML parameters, Cookie version and format, Multipart/form-data encoding of file upload) etc.;		
10.	Security features	Should support the analysis of common HTTP encoding types, such as ULR decoding, Base64 decoding, JSON decoding, hexadecimal conversion, slash inversion, XML analysis, PHP deserialization analysis, etc., and support recursive decoding;		
11.	Security features	Should provide HTTP protocol protection function, and deal with incomplete packets, retransmitted packets and forged malformed packets through the protocol verification mechanism.		
12.	Security features	Should detect and block SQL injection attacks, support injection detection based on get, post, cookie, etc., and support the detection of code bypassing SQL injection;		
13.	Security features	Should prevent XSS cross-site attacks, including the detection of storage and reflection cross-site methods, and the detection of code bypassing XSS cross-site attacks;		
14.	Security features	Should support attack detection for Struts2 command vulnerabilities, and can block remote command execution caused by Struts2 vulnerabilities;		
15.	Security features	Should protect against command injection attacks, such as Linux and Windows system command execution;		
16.	Security features	Should protect against common types of injection attacks, including SSI, LDAP, XPATH, mail header, file injection, etc.;		

Sl. No.	Features	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
17.	Security features	Should support the detection of uploading webshell attacks. The detection method should be based on the content of the uploaded file, while protecting against illegal access to the webshell;		
18.	Security features	Should support HTTPS-based attack protection and detection of attack behaviour in encrypted data packets;		
19.	Security features	Should prevent the leakage of sensitive information caused by crawlers, and can identify common web crawlers, such as google, yahoo, baidu etc. It can also detect and block the scanning behaviour of mainstream scanners;		
20.	Security features	Should have the ability to detect and filter the attacks of abnormal HTTP requests, such as put and delete methods, HTTP request header parameters, such as user-agent and range fields; whitelist filtering based on URL and parameters; HTTP request referrer field.		
21.	Security features	Should support Anti-leech to prevent the attacker from using technical means to bypass other commercial end-user windows (such as advertisement) and providing services belonging to other service providers to end users on their own website.		
22.	Security features	Should support Web Anti-Defacement (WAD) function to detect and prevent the defaced web pages from being returned to the client. It should returns the cached original web page to make the anti-defacement effects unnoticeable or returns a 503 error page to the client to end the service.		
23.	Security features	Should have regular own Signature updates and the signature database upgrade process should not affect the normal operation of WAF, including the detection and protection of attacks;		

Sl. No.	Features	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
24.	Security features	Support report group management, including security report, audit report, configuration management report;		
25.	Security features	Support log multi-condition query (combined query), log fields include but not limited to: time, login IP, administrator, user type, event type, operation type, event ID, object type, object name, variable name, original Value, modified value, details;		
26.	High Availability	The WAF should support HA deployment (Active/Active or Active/Passive) using standard VRRP, allowing two or more WAFs to form an HA cluster to ensure continuity of work and achieve redundancy protection.		
27.	High Availability	The solution should provide comprehensive and reliable support for high availability and N+1 clustering through Standard VRRP RFC 2338 on Per VIP based Active-active & active standby unit redundancy mode.		
28.	Appliance	The appliance should be dedicated appliance and from different vendor than firewall and NGFW. Proposed appliance should support virtualization with each instance having capability to assigned dedicated hardware resources including I/O interfaces, memory, CPU, Hardware SSL card Cores		

1.16. Next Gen Firewall

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
	Make:		
	Model:		
	External Firewall as part of Next Gen Firewall		

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
1	The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened operating system that eliminates the security risks associated with general-purpose operating systems		
2	The Proposed Firewall Vendor should be from leading OEM.		
3	Firewall appliance should have at least 4x 40 GE QSFP+ /100 GE QSFP28, 10x 10 GE SFP+ 8x GE RJ45 along with 2 x GE Management ports (SFP Transceivers to be populated as per solution requirement)		
4	Firewall appliance should have dual hot swappable power supply.		
5	Firewall Throughput should be 100 Gbps on 64 byte		
6	Firewall should support minimum 50 Gbps of VPN throughput		
7	Firewall should support 200 site-to-site & 10,000 client to site VPN Tunnels.		
8	Firewall should support minimum 10,000 concurrent SSL VPN users and should be scalable in future		
9	Firewall should support 750,000 new sessions per second		
10	Firewall should support 20 Million concurrent sessions		
11	The solution should support minimum 18 Gbps of NGFW (FW + IPS + AVC) throughput for Mix / production traffic		
12	The threat prevention (FW + AVC + IPS + Antivirus /Antimalware) throughput should be at least 17 Gbps on Mix / Production traffic		
13	The Firewall solution should support NAT66, NAT46, NAT64, DNS64 & DHCPv6		
14	The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode. Both modes can also be available concurrently using Virtual Contexts.		

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
15	The proposed system should have integrated Traffic Shaping functionality.		
16	The proposed system should support		
17	a) IPSEC VPN		
18	b) PPTP VPN		
19	c) L2TP VPN		
20	The device shall utilize inbuilt hardware VPN acceleration:		
21	a) IPSEC (DES, 3DES, AES) encryption/decryption		
22	b) SSL encryption/decryption		
23	The system shall support the following IPSEC VPN capabilities:		
24	a) Multi-zone VPN supports.		
25	b) IPSec, ESP security.		
26	c) Supports NAT traversal		
27	d) Supports Hub and Spoke architecture		
28	e) Supports Redundant gateway architecture		
29	The system shall support 2 forms of site-to-site VPN configurations:		
30	a) Route based IPSec tunnel		
31	b) Policy based IPSec tunnel		
32	The system shall support IPSEC site-to-site VPN and remote user VPN in transparent mode.		
33	The system shall provide IPv6 IPSec feature to support for secure IPv6 traffic in an IPSec VPN.		
	Virtualization		

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
34	The proposed solution should support Virtualization (Virtual Firewall, Security zones and VLAN). Minimum 10 Virtual Firewall license should be provided and should be scalable to 100 by adding licences / blades in future		
	Intrusion Prevention System		
35	The IPS capability shall minimally attain NSS Certification		
36	IPS throughput should be minimum 24 Gbps for Mix / Production traffic		
37	The IPS detection methodologies shall consist of:		
38	a) Signature based detection using real time updated database		
39	b) Anomaly based detection that is based on thresholds		
40	The IPS system shall have at least 10,000 signatures		
41	IPS Signatures can be updated in three different ways: manually, via pull technology or push technology. Administrator can schedule to check for new updates or if the device has a public IP address, updates can be pushed to the device each time an update is available		
42	In event if IPS should cease to function, it will fail open by default and is configurable. This means that crucial network traffic will not be blocked and the Firewall will continue to operate while the problem is resolved		
43	IPS solution should have capability to protect against Denial of Service (DOS) and DDOS attacks. Should have flexibility to configure threshold values for each of the Anomaly. DOS and DDOS protection should be applied and attacks stopped before firewall policy look-ups.		
44	IPS signatures should have a configurable action like terminate a TCP session by issuing TCP Reset packets to each end of the connection, or silently drop traffic in addition to sending an alert and logging the incident		
45	Signatures should a severity level defined to it so that it helps the administrator to understand and decide which signatures to enable for what traffic (e.g. for severity level: high medium low)		

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
	Antivirus		
46	Firewall should have integrated Antivirus solution with ICSA Lab certification or equivalent.		
47	The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy based or based on firewall authenticated user groups with configurable selection of the following services:		
48	a) HTTP, HTTPS		
49	b) SMTP, SMTPS		
50	c) POP3, POP3S		
51	d) IMAP, IMAPS		
52	e) FTP, FTPS		
53	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.		
54	The firewall solution should be able to scan the uploads for malicious content with inbuilt antivirus database and also be integrated with proposed Sandbox to scan and mitigate zero day / unknown malwares being downloaded from internet. The Sandbox should be proposed with minimum 24 VMs on day 1, should be able to scan file sizes up to 100 mb and more with real-world throughput of 2400 files per hour and it should be supplied with minimum 4 x GE and 2 x10G interfaces.		
55	The proposed Firewall should support CDR functionality to strip suspected active content from files and deliver a sanitised file in real time by removing the malicious content from the files received.		
	Application Control		
56	The proposed system shall have the ability to detect, log and take action against network traffic based on over 3500+ application signatures		

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
57	The application signatures shall be manual or automatically updated		
58	The administrator shall be able to define application control list based on selectable application group and/or list and its corresponding actions		
	Data Leakage Prevention		
59	The proposed system shall allow administrator to prevent sensitive data from leaving the network. Administrator shall be able to define sensitive data patterns, and data matching these patterns that will be blocked and/or logged when passing through the unit.		
	Web Content Filtering		
60	The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules.		
61	The proposed solution should be able to enable or disable Web Filtering per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS traffic.		
62	The proposed system shall provide web content filtering features:		
63	a) which blocks web plug-ins such as ActiveX, Java Applet, and Cookies.		
64	b) Shall include Web URL block		
65	c) Shall include score based web keyword block		
66	d) Shall include Web Exempt List		
67	The proposed system shall be able to queries a real time database of over 110 million + rated websites categorized into 70+ unique content categories.		
	High Availability		
68	The proposed system shall have built-in high availability (HA) features without extra cost/license or hardware component		

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
69	The device shall support stateful session maintenance in the event of a fail-over to a standby unit.		
70	High Availability Configurations should support Active/Active or Active/ Passive		
	Logs and Report		
71	The Logs and Reporting platform must be a dedicated same OEM appliance and VM/software running on server will not be accepted.		
72	The Logs and Reporting platform support running on-demand and scheduled reports		
73	Should have 24 TB of Hard Drive Capacity after enabling RAID for logging and reporting if not please quote separate appliance		
74	Should support RAID Levels 1 , 5 and 10		
75	Real-time display of information allows you to follow real-time trends in network usage such as the source IP address and the destination URL for HTTP traffic .		
76	All log files and messages are searchable and can be filtered to drill down and locate specific information.		

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
Make:			
Model:			

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
1	**Internal fire wall parameter as part of Next Gen Firewall**		
2	NGFW with Layer 3 - Layer 4, NAT, VPN, Application Visibility and Control (AVC), User Identity, Next Generation Intrusion Prevention System (IPS), Zero Day Protection / Advance Malware protection, Web Security Essentials / URL Filtering		
3	Traffic handled: TCP, UDP, HTTP/TCP, TCP/UDP		
4	Packet Size (KB): 1024 Or higher		
5	Throughput (Real World/Prod Performance) (Under Test Condition: 38 Gbps		
6	Concurrent Session/Concurrent\ Connection: 35 M		
7	New session/Connection per second: 500 K		
8	Number of GE Copper interface: 16		
9	Number of 10G SFP+ interface : 8		
10	Number of QSFP+ 40 G interface: 2		
11	Number of GE Small Form-Factor Pluggable (SFP) interface : 10		
12	Number of Ipsec VPN Peers supported (Site to Site) : 125000		
13	Number of Ipsec VPN Peers supported (Client to Site) : 125000		
14	Number of SSL VPN Peers supported (Client to Site) : 125000		
15	Type of Storage Disk HDD with 1000 GB		
16	Power Supplies : Dual Hot swap and redundant fan		
17	High Availability from day 1: Active - Active		

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
18	Interface Expansion slots supported (Additional Free for Future Use) : 2 Firewall Policies		
19	for the Firewall provided with the License : Web Security Essentials / URL Filtering, IPS License, Application Visibility License, APT (Advance Persistent Threat) License (Anti Malware Protection , C& C attacks, Geo IP Protection, Zero Day Threat Protection), Gateway Anti-virus, Gateway Anti-spam		
20	NGIPS Signature supported : 25000		
21	Security Intelligence : IP, URL, Domain: Common Criteria /NDPP/NSS/ICSALabs		
22	IPv6 Ready from day 1		
23	Certification : within Guidelines of Make in India Policy, we will need Indian Standard Certification for IT Security in IC3S (EAL 4) provided by STQC. Alternatively at least 1 out of the below International Equivalent Security Certificates will be Considered, : NSS Labs or Ndpp or ICSA Labs.		
24	Reporting : Reporting Must be Included in the Bundle from Day 1, Should support SDWAN, VDOM/VCONTEXT/VSHIELD(25 Virtual Firewall to be supported from Day 1) from Day 1, 4 Nos of Hot Swappable SSD Bays Should be there from Day 1, New Sessions of 500K or above should be there from Day 1, Minimum 2 Numbers of Empty Expansion Slots for Future addition of Ports should be there from Day 1 in Addition to the number of Fully Populated(with Transceivers wherever applicable) Ports asked in the Configuration i.e., (16* 1 G Copper, 10* 1G SFP, 8*10 G SFP+, 2*40 G QSFP+ should be Populated from Day 1 , In Addition 2 Free Expansion Slots for Future Ports Requirement)		

1.17. Data Leakage Prevention

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
Make:			
Model:			
1	Proposed solution should be Network DLP solution with automatic data classification for minimum 5000 users need to be provided from day 1. All corresponding hardware and Operating system to be provided by the bidder to ensure proper functioning of the solution		
2	The solution should cover both Active and passive FTP including fully correlating transferred file data with control information and have the ability to monitor popular IM protocols (AIM, Yahoo, MSN, IRC) and properly classify tunnelled IM traffic (HTTP). Proposed solution should be inclusive of data leakage prevention, data classification any related OS etc.		
3	The solution must have Identity and Role Based policy capabilities that integrate with AD/LDAP/HR database. The solution should be capable of role based access based Enforcement of Information Security and the solution should enforce "Automatic Access Control" on Data and Information so that each role can have defined access to sensitive data.		
4	The solution must be able to apply different policies to different employee groups. The solution should have a comprehensive Information Classification methodology that would be readily deployable. The solution must use automated policy mechanism and should have built-in Automated Policy Synthesis mechanism. The solution should be able to monitor and prevent Advanced Persistent Threats pertaining to the classified data.		
5	The solution should have built-in Ontologies on International PII and PCI- DSS capabilities and has the ability to add or customized new ontologies. The solution should have rule or policy-based capabilities such as assigning access rights, restricting where users can store sensitive data, and so forth		
6	The solution should have ability to detect and protect new or unseen documents, which content is similar to the data categorization, which has been taught via data		

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
	categorization. The solution should have ability to detect scanned documents, which contains sensitive data in text form		
7	Proposed solution should have no restriction to the size of the document for inspection and classification		
8	The solution should be able to classify unstructured data, namely word/excel/PowerPoint/pdf documents. The solution should be able to label the documents in headers/footers with a pre-selection capability for either header or footer or both. The solutions should be able to insert metadata tags in the documents and emails which can be read by DLP Solutions		
09	The solution shall ensure the enforcement of classification and should not allow user to bypass classification option in the said document's types. The solution should have capability to detect differential classification between an email and it's attachments and block the email from being sent		
10	The solution should have some guidance mechanism while user selects a classification level, to inform the users what is the context of a said classification level as per organization's policy. The solution should enable the classification of Word, Excel and PowerPoint documents. Proposed DLP product should have its own data classification solution		
11	The solution should be able to identify information like Aadhaar, Passport numbers for automated classification thru either inbuilt capability or should have capability to define regular expressions. The solution should suggest a classification based in content but should allow user to change the classification if required by taking a justification for the same and recording it in logs.		
12	The solution should support the ability to warn or prevent users from sending password-protected Microsoft Office documents via email. (The metadata in password-protected Office documents is encrypted, so this capability provides an alternative way to enforce policy.) The solution should provide a pre-built starter set of reports for the reporting database (in Excel) and Views and documentation to enable customers to write their own reports.		

1.18. Security Incident and Event Management

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
	Make:		
	Model:		
	Functional Specifications		
1	There should be no limitation on number of devices to be integrated.		
2	Next generation platform shall encompass log data with added context and threat intelligence. It should support to integrate with Packet and EDR solution to provide complete network and endpoint visibility through deep packet inspection, high speed packet capture and analysis.		
3	Real time contextual information and threat intelligence feeds shall be infused for real time threat detection.		
4	The solution should provide an integrated SOC dashboard and Incident analysis system that could provide a single view into all the analysis performed across all the different data sources including but not limited to logs, endpoint, and packets.		
5	The proposed solution should be able to continue to collect log data during database backup, de-fragmentation, and other management scenarios, without any disruption to service.		
6	The system should receive feeds from a threat intelligence repository maintained by the OEM which consists of inputs from various threat sources and security devices across the globe		
7	The system should be capable to consume Threat Intelligence from Third Party sources		
8	The central correlation engine database should be updated with real time security intelligence updates from OEM		
9	The solution should provide central management of all components and administrative functions from a single management console. The Solution should have a centralized management for various components from a single GUI		

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
10	The monitoring shall be cross-device and cross -vendor and shall be both out of the box and scalable to cover additional devices and applications as required. The solution must provide weighted alerts to allow for prioritization.		
11	Compliance and Security relevant reports should be available out of the box. The solution must be able to customize the out of the box reports as well. Following compliance reports must be provided out of the box • Basel II • Bill 198 • Family Educational Rights and Privacy Act (FERPA) • Federal Financial Institutions Examination Council (FFIEC) • Federal Information Security Management Act (FISMA) • Gramm-Leach-Bliley Act (GLBA) • Good Practice Guide 13 (GPG13) • Health Insurance Portability and Accountability Act of 1996 (HIPAA) • International Standardization Organization 27002 (ISO 27002) • North American Electric Reliability Corporation – Critical Infrastructure Protection (NERC CIP) • National Industrial Security Program Operating Manual (NISPOM) • Payment Card Industry (PCI) • Sarbanes-Oxley Act of 2002 (SOX) • Statement on Standards for Attestation Engagements (SSAE 16)		
12	The solution should have built-in incident management feature to generate tickets for the alert events generated by the SIEM		
13	Solution should have an OOTB bidirectional integration with Threat Intelligence Platform		
14	Solution should be able to alert the analyst of any threat intel match in real time by infusing the threat intel with raw logs during normalization phase.		
15	Solution should have Deep Packet Inspection (DPI) to provide visibility in all layers of the OSI stack (Layer 2-7) including application payload data.		
16	Proposed Network Threat Detection platform should adopt technics to provide visibility into channels that are trying to blend in with other traffic, but do not		

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
	follow normal protocol behaviour. Proposed solution should understand the behaviour of the protocol and highlight in case of any discrepancy		
17	Solution should have the capability to explore the root cause of any attack pinpointing the attributes and metadata of an attack.		
18	Solution should provide analysis with real-time threat information feeds from OEM and other global intelligence sources		
19	Solution should be managed and monitored from SIEM unified console for Correlation, Alerting and Administration so that historical event searching, and log packet correlation is possible		
20	The proposed solution must be able to provide the complete platform to perform Network forensics solution		
21	Solution should support creating additional parsers for protocols and object analysis without any additional license		
22	The solution should support high rate of packet capture without compromising on ability to read the data for correlation, reporting and threat hunting.		
23	Should support integration with an ETDR solution for end endpoint threat visibility and file system analysis		
24	Solution should allow investigation of logs and raw packets data from a single console		
25	Solution should be focused on unsupervised machine learning so that it does not require any human/analyst to create data science models.		
26	Solution should support user-based behaviour analytics		
27	Solution should be an additional component as part of SIEM and should have same UI as the SIEM solution to provide event level and historical level analysis along with behavioural analysis along with below:		
28	Provide an aggregated analytics UI dashboard to security analysts with ability for detailed drilldown investigation of specific events.		
29	Solution should be able to track user's activities locally and remote network sites and should be able to report usage behaviour across the entire network.		
30	Solution should support Machine Learning (ML) driven risk scores and risk profiles for user		

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
31	UBA should be a pure unsupervised machine learning engine with no need to configure any settings not limited to baselines, thresholds, decays, risks scores. Also, there should not be any need to configure thresholds through settings during learning or production phase		
32	Solution should provide a native threat intelligence repository which is updated on a periodic basis		
33	Solution should provide insights on data reputation, network activity (observations), false positive counts, and status		

1.19. Network Access Control

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
Make:			
Model:			
1	The NAC solution must eliminate 'blind spots',and provides a wealth of actionable data.		
2	The NAC solution should be able to integrate with multi-vendor network infrastructure devices		
3	The deployment of NAC solution should not require changing any existing infrastructure/device.		
4	The NAC solution should support discovery, control of all end point and should be able to take IOC from third party device like SIEM, Firewall, AV server etc without any extra module/appliance/licenses.		
5	The proposed NAC solution have all the license from day one.		

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
6	The NAC solution must offer Network Visibility, Device Profiling, Easy and powerful Onboarding process, Endpoint Compliance, Network Provisioning and Threat Identification module provide security actions through integration.		
7	The system should not have a single point of failure.		
8	The system should not be based on SPAN port integration.		
9	Should allow organization to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent security policy.		
10	NAC solution must be vendor agonistic solution suited for heterogeneous network.		
11	NAC solution must be integrated with existing network and security equipment and application.		
12	Should be capable of working with endpoint agents and agentless.		
13	NAC solution must have the ability to inventory all devices on a network including non-PC equipment like printers, smart phones, IP-phones, and appliances.		
14	Should authorize access via VLAN assignment and/or applying access control lists (ACLs).		
15	The NAC solution must integrate with infrastructure devices by using SNMP, CLI and RADIUS.		
16	The NAC Solution should not be dependent on 802.1x & RADIUS integration.		

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
17	The NAC solution must be scalable allowing to implement the solution on a small scale initially and expanding it later.		
18	The NAC solution MUST be best in class fully out-of-band NAC solution that fits in any heterogeneous network.		
19	Guest management capabilities must be quickly and easily to set up guest account without engaging IT staff.		
20	NAC solution must be based on perpetual license model.		
21	System can be delivered On-Premise via either a Physical Appliance, Virtual Appliance.		
22	System must support Hybrid deployment.		
23	**Endpoint profiling Requirements**		
24	Should support profiling for clientless devices based on a DHCP fingerprint, NMAP scan, Vendor OUI, location, open ports, WMI, Winrm and the existence of the persistent agent		
25	Should support profiling for iPhone, iPad, Android, network printers, IP surveillance cameras. etc		
26	Profiling via SNMP, NMAP, TCP & UDP characteristic must be supported		
27	Profiling via WMI must be supported		
28	Should provide the ability to create custom profiling rules.		

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
29	**Authentication and Enforcement Requirements:**		
30	Should support RADIUS MAC-address whitelisting & blacklisting natively		
31	Should support flexible authentication options to include, 802.1X, Web Authentication and MAC Authentication		
32	Should support LDAP integration		
33	Should support Microsoft Active Directory integration.		
34	Should support RADIUS Identity store.		
35	Should support Token Server with backend LDAP		
36	Should support seamless integration with Active directory in the Infrastructure without the need for any additional components.		
37	Should support both user and machine authentication without any additional configurations.		
38	Should be able to append additional attributes to incorporate the authenticator's location, device type, vendor etc apart from the user attributes.		
39	Should provide the ability to authenticate an endpoint using an agentless scanning capability		
40	Should allow only authenticated/managed devices to connect to organization networks and enforces security policies by blocking, isolating, and repairing		

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
	noncompliant machines in a quarantine area without needing administrator attention.		
42	**Endpoint Compliance and Remediation Requirements**		
43	Should support both agent-based (Persistent Agent, Dissolvable Agent) and agentless endpoint inspection.		
44	Should perform system checks on service packs, patches, critical updates enabled, Antivirus & AntiSpyware, static IP, services/processes running, invalid services/processes, file existence, any Microsoft registry settings.		
45	The solution must provide a quarantine role that ties into the integrated patch management systems. Within this quarantine role the solution shall provide a "self-remediation" web captive portal. Non-compliant devices must be quarantined dynamically and provided with instructions for self-remediation or can be interfaced with auto-remediation systems such as BigFix and PatchLink.		
46	**Management and Reporting requirements**		
47	Offers a built-in monitoring, reporting, and troubleshooting console to assist helpdesk operators and administrators streamline operations.		
48	It should have a policy creation template with pre-defined templates and wizard for creating policies for easy Enterprise-wide policy deployment		
49	Should support the option of having dedicated reporting and monitoring system		
50	Should include integrated monitoring, reporting, and troubleshooting engine accessible through a web-based GUI		

Sl. No:	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
51	**Post Connect Assessment (Automated Response)**		
52	The proposed solution must provide ongoing integrity through an automated response via the integration with other Inline /out-of-band security solutions.		
53	Automated Response integration should allow the organization to quickly identify critical security events with precision and reduce threat containment.		
54	The solution should provide automated response to contain threats via multiple control methods.		

1.20. Server for Vehicle Mounted Camera- rack mounted with storage and rack

Sl. No	Features	Minimum Requirements	Compliance (Yes / No)	Deviations (if any)
	Make:			
	Model:			
1	Form Factor	Rack mounted		
2	Configured CPU	Intel/Xenon Processors (To be populated with 8 Cores 3.1 GHz clock speed, 20 MB Cache) or Better		
3	Storage	200TB usable storage Dual ported 12 gbps NL SAS the system must support SSD for data caching, hot swappable HDD, with 2 spare slots for further expansion		

Sl. No	Features	Minimum Requirements	Compliance (Yes / No)	Deviations (if any)
4	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 6,10, 50 with 8 GB Cache		
5	Ethernet ports	3 x RJ 45 Ports 10/100/1000		
6	Power Supply	Redundant Power Supply		
7	USB Ports	2xUSB 3.0 and 2x USB 2.0,		
8	Display Port	1 VGA, 1 HDMI		
9	Alarm and Alert	It must include HDD Failures, tampering HDD, connectivity failure, temperature , fan speed, UPS/Power supplies status TPM 1.2 at compute and data storage layer		
10	Operating System	Dual dedicated operating system (like windows etc) M2 SSD drives on RAID 1, shall have redundant storage drives, cooling fans, and power supplies. The storage OS should be separate from server OS and should not be general purpose OS for storage.		
11	Cyber Resilient	Cyber resilient architecture with security features like threat detection, and "Keep Your Hard Drive", etc features		
12	Monitor & KBD/Mouse	22” screen & USB Keyboard & Mouse or monitoring and configuration at rack level with unified display screen, keyboard mouse		

Sl. No	Features	Minimum Requirements	Compliance (Yes / No)	Deviations (if any)
Specification and compliance of 42U floor standing rack				
13	Material	The frame should be made of MS profiles de- signed to accept front and rear doors and side panels, which close within the frame itself.		
14	Size (Width)	800mm		
15	Height	42U		
16	Depth	Depth overall: 1200mm		
17	Mounting Angle & Lock handles	Two Pairs of 19" Mounting Angles, should have Proper Locks with handles on both front and rear doors with unique key		
18	Doors	Front and Rear perforated door with perforation for better air movement across the Rack.		
19	Profile	Minimum 9 folded profile required for better strength		

Sl. No	Features	Minimum Requirements	Compliance (Yes / No)	Deviations (if any)
20	Top & Bottom Cover	Top cover and Bottom panels with cable entry facilities. Cable entry cut out		
21	Equipment cooling	Each rack should be compatible with floor- throw as well as top-throw Data centre cooling system.		
22	Floor Standing acces-sories	All Floor Mounting accessories required to setup the rack. Castors and levelling legs		
23	Earthing	Enclosures shall be bonded to the protective earth system using a minimum 2.5 sq. mm conductor.		
24	Power Distribution	Each rack should have One Power Distribution Unit (PDU) with IEC C13 12x 10 Amp, C19 4 x 16 Amp with 32 Amp MCB		
25	Colour & Powder Coating	Colour should be Black. Rack to be powder coated with Nano ceramic pre-treatment pro- cess using a zirconium coat. Powder coating thickness shall be 80 to 100 microns. The Powder coating process should be RoHS compliant		

Sl. No	Features	Minimum Requirements	Compliance (Yes / No)	Deviations (if any)
26	Load Rating	Minimum 1000 Kg load bearing on 19" Angles and 1400 Kgs overall		
27	Standard	Rack should conform to DIN 41494 Standard and UL Listed		

1.21. Desktops

1.21.1. Including Hindi Keypad on Keyboard with OS and Antivirus

Sl. No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Make			
	Model			
1	Processor	11th Generation or latest Intel Core i7, Min 8 cores		
2	Form Factor	Small form Factor (SFF) less than 8L, Tool Less Chassis, MIL Standard Tested		
3	Motherboard	Intel Q570 or higher chipset		
4	Memory	16 GB Single DIMM DDR4 RAM expandable up to 128 GB or higher, 4 DIMM Slots		
5	HDD	256GB PCIe SSD & 1 TB SATA (Faulty drives shall not be returned during the warranty period and shall be property of the department, OEM declaration regarding this to be given along with the bid)		
6	Monitor	21.5-inch LED Backlit Full HD (Same make as Desktop)		

Sl. No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Make			
	Model			
7	Keyboard	Standard OEM Wired USB Keyboard (Same make as Desktop)		
8	Mouse	Standard OEM Wired USB Optical Scroll Mouse (Same make as Desktop)		
9	Ethernet	Integrated Ethernet 10/100/1000 NIC		
10	Ports	10 USB ports with at least 6 USB 3.2 ports including 1 USB Type C, 2 DisplayPort & 1 HDMI Port, 2 PCIe Slots		
11	Operating System	Preloaded Windows 11 Professional 64 Bit (OEM Declaration for Genuine Preloaded OS to be provided in bid)		
12	Certification	Energy Star, EPEAT, Certified for Windows & Ubuntu		
13	Power Supply	92% Efficient with min 300W		
14	Graphics	4GB Dedicated Graphics Card		

1.22. Thin Client

1.22.1. Including Hindi Keypad on Keyboard with OS and Antivirus

Features - Thin Client				
Sl. No.	**Features**	**Minimum Specifications**	**Compliance (Yes/No)**	**Deviations (Yes/No)**
	Make			
	Model			
1.	Graphics	Intel HD Graphics		

Features - Thin Client				
2.	Monitor	21” Or higher “TFT OEM colour touch screen monitor. TCO Monitor. Same brand as Desktop		
3.	Keyboard	107 Keys or more, USB bilingual (English + Hindi keys) keyboard		
4.	Mouse	2 button Optical scroll Mouse		
5.	Operating System	Supported by Windows, Linux etc.		
6.	Power	320 W or less		

1.23. Laptop

SL. No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Make			
	Model			
1.	Processor	11th Generation Intel Core i7 Processor, min 4 cores		
2.	Display	14" Full HD Anti-Glare		
3.	Memory	16 GB DDR4, upgradable to 32GB using 2 DIMM Slots (Field Replaceable Modules)		
4.	Graphics	2 GB Dedicated Graphics Card		
5.	Storage	512GB SSD (Faulty drives shall not be returned during the warranty period and shall be property of the department, OEM declaration regarding this to be given along with the bid)		
6.	Connectivity Technology	Integrated Dual Band Wi-Fi 2x2 802.11ax + Bluetooth 5.1		
7.	Keyboard	Spill Resistant backlit keyboard and multi point touch pad		
8.	Ports	HDMI out, RJ-45, headphone/microphone combo jack, 2 USB 3.2, 1 USB 2.0, 1 USB Type C		

SL. No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Make			
	Model			
9.	Battery	52 WHr or higher with upto 8-hours backup during normal usage		
10.	Audio and Visual	Built in microphone and stereo sound speakers, webcam		
11.	Weight	Not more than 1.6 Kgs. Including battery		
12.	Carry Case	OEM backpack		
13.	Operating System	Windows 11 Professional 64 Bit preloaded (OEM Declaration for Genuine Preloaded OS to be provided in bid)		
14.	Certification & Testing	Energy Star; EPEAT, ROHS, Windows Certified, Ubuntu Linux Certified		
15.	Productivity	MIL Grade Tested, Hardware TPM 2.0		

1.24. Tablets-Android with Stylus

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Make			
	Model			
1	Display Size	10" or better		
2	Display	TFT LCD or better		
3	RAM	8Gb or Better		
4	Storage	128Gb or Better		
5	Processor	Qualcomm Snapdragon 680 or better or equivalent		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
6	Operating System	Android 11 or better		
7	Battey capacity	6000mah or better		
8	Connectivity technologies	Bluetooth, Infrared, Wi-Fi, USB		
9	Resolution	1080X2340 or better		
10	Network	GSM / HSPA / LTE / 5G		
11	Charger	25W or better Fast Charging		
12	Main Camera	12MP or better		
13	Front Camera	8MP or better		
14	WLAN	Wi-Fi 802.11 a/b/g/n/ac/6e, dual-band, Wi-Fi Direct, hotspot		
15	Bluetooth	5.0, A2DP, LE		
16	GPS	Yes, with A-GPS, GLONASS, GALILEO, BDS		
17	Stylus	Required		
18	Screen guard and cover	Bidder to provide rugged tablet cover and screen guard		

1.25. IP phones with Headset

Sl. No.	Requirement	Description	Compliance (Yes/No)	Deviations (Yes/No)
	Make			
	Model			
1.	General Requirement	Minimum 2.8 inches x 2.1 inches – Diagonal width: 3.5 inches Colour Screen		

Sl. No.	Requirement	Description	Compliance (Yes/No)	Deviations (Yes/No)
2.	General Requirement	Minimum 8 buttons		
3.	General Requirement	4 softkeys		
4.	General Requirement	Hard buttons for Various Functions		
5.	General Requirement	Wideband audio in handset and headset		
6.	General Requirement	Ergonomic hearing aid compatible		
7.	General Requirement	Message waiting indicator		
8.	General Requirement	Two Gigabit Ethernet (10/100/1000) line interfaces		
9.	General Requirement	PoE Class (IEEE 802.3af) registers as class 1 device and supports 802.3az.		
10.	General Requirement	Support for SIP & H.323 protocol		
11.	General Requirement	Standards-based codec support: G.711, G.726, G.729A/B, G.722, Opus.		
12.	General Requirement	Should support WIFI & Bluetooth		
13.	General Requirement	IP Phone should support SIP Advanced Full functions with Offered PBX and should be of the same OEM of PBX.		

Sl. No.	Requirement	Description	Compliance (Yes/No)	Deviations (Yes/No)
Headset Specifications				
	Make			
	Model			
14.	General Requirements	➢ Padded Headband and Ear Cups ➢ Double-ear standard headset ➢ Digital Stereo Sound ➢ Noise Cancelling Mic ➢ In-Line Controls ➢ High ambient-noise attenuation headphones ➢ Flexible gooseneck microphone positioning ➢ 300-degrees boom mic rotation for ON/OFF mic-mute switch ➢ Rugged design ➢ USB/Aux Computer Headset		

1.26. Heavy duty Printer

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
1.	Make			
2.	Model			
3.	**General**			
4.	Warm-up time	20 Seconds		
5.	First Output time	Full Colour:8 Seconds B / W: 6 Seconds		
6.	Memory	1.5 GB		
7.	Weight	Up to 85Kg		
8.	Power Source	220-240V, 50 / 60Hz		
PRINTER				
9.	Printer Language	Standard: PCL5c, PCL6, PDF direct print, Media print (JPEG / TIFF)		
10.	Option	Adobe PostScript		
11.	Resolution	Maximum:1200x1200 dpi		
12.	Interface	Standard: USB2.0, SD slot, Ethernet 10 base-T, Ethernet1000 Base-T		
13.	Option	Bi-directional IEEE1284, Wireless LAN(IEEE802.11a / b / g / n), Bluetooth		
14.	Network Protocol	Standard: TCP/ IP (IPv4, IPV6) Optional Or SPX		
15.	Windows environments	Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2003R2, Windows Server 2008, Windows Server 2008R2, Windows Server 2012		
16.	Print speed	20 pages per minute		
17.	Mac OS environments	Yes		
18.	UNIX environments	Yes		
SCANNER				

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
19.	Scanning Speed	Full Colour/ B&W:Maximum 50ipm		
20.	Resolution	Standard: 600dpi Maximum: 1200dpi		
21.	File Format	TIFF, JPEG, PDF, High compression PDF, PDF-A		
22.	Bundled drivers	Yes		
23.	Scan to	Email: SMTP, POP, IMAP4 Folder: SMB, FTP, NCP		
COPIER				
24.	Copying process	Dry Electrostatic Transfer System		
25.	Multiple copying	Up to 900 copies		
26.	Resolution	600dpi		
27.	Zoom	From 25 to 400%		
FAX(OPTION)				
28.	Circuit	PSTN, PBX		
29.	Resolution	Standard: 8x3.85 line/ mm, 200x100 dpi, 8x7.7 line/mm, 200x200 dpi		
30.	Modem speed	Maximum: 30 Kbps		
31.	Memory capacity	Standard: 4 MB Maximum: 28 MB		
PAPER HANDLING				
32.	Recommended paper size	A3, A4, A5, A6, B4, B5, B6		
33.	Paper input capacity	Standard: 1200 sheets(55x2 trays+100-sheet Bypass) Maximum: 2300 sheets		
34.	Paper output capacity	Maximum: 625 sheets		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
35.	Paper weight	Paper tray(s):60-300 g / m2 Bypass: 52-300 g or m2 Duplex unit: 52-169 g or m2		
ECOLOGY				
36.	Power consumption	Maximum: 2000 W Ready mode: 300 W		
SOFTWARE				
37.	Standard	SmartDeviceMonitor, Web SmartDeviceMonitor, Web Image Monitor		

1.27. ID Card Printer

Sl. No	Features	Compliance (Yes/No)	Deviations (Yes/No)
	Make		
	Model		
1	**Side printing:** Single or dual		
2	**Print method:** Dye sublimation / resin thermal transfer		
3	**Resolution:** 300 dpi		
4	**Print speed:** 16 seconds per card / 225 cards per hour or better		
5	**Included Software:** printer maintenance and diagnostic software with Colour Assist feature		
6	**Data protection:** AES-256 encryption on the printer over a secure network		
7	**Card capacity:** 100 card input, 30 card output (Dual-sided: up to 100 cards)		

Sl. No	Features	Compliance (Yes/No)	Deviations (Yes/No)
8	Single-wire Ethernet and USB 2.0 interface for inline printing and encoding		
9	Wireless connectivity with Wi-Fi accessory (on Ethernet-enabled printers)		
10	Dual-sided printing module		
11	Magnetic stripe and/or smart card encoding (contact/contactless)		
12	Printer cleaning kit		
13	Ethernet with internal print server		

1.28. 7" LCD Monitor

Sl. No	Features and minimum specifications	Compliance (Yes/No)	Deviations (Yes/No)	Sl. No
	Make			
	Model			
1	Size	Minimum 7" LCD with arrow keys and number buttons		
2	Luminance	400cd/m2		
3	Viewing angle	70/70/50/70 (L/R/U/D)		
4	Resolution	800 × 480 or better		
5	Back-light Type	LED		
6	Video Inputs	Two (compatible with the proposed mNVR)		
7	Functionality	Live view and play back		
8	Power Source	mNVR		

1.29. *AV for Conference Room*

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
Display Device: Bidder may continue using the same display device, provided extended maintenance can be availed, if not bidder has to provide equivalent or higher model product.				
1.	Make			
2.	Model			
3.	Screen Size (Diagonal) and Aspect Ratio	Minimum 65-inch and 16:9, touch screen		
4.	Brightness	350 cd/ m2 (Typ)		
5.	Contrast Ratio	4,000:1		
6.	Viewing Angle	120° /120°		
7.	Detection Method	Infrared Blocking Detection Method		
8.	PC Connection Port	USB (3.0 Compliant)		
9.	VIDEO In / Audio In (L Or R)	Yes		
10.	HDMI In	HDMI Type A Connector x 2		
11.	DVI-D In / Audio In (L Or R)	DVI-D 24-pin x 1 / Stereo Mini Jack (M3) x 1 (Shared with PC In)		
12.	PC In / Audio In (L Or R)	Mini D-Sub 15-pin x1 (Female), Plug & Play (VESA DDC 2B) / Stereo Mini Jack (M3) x 1 (Shared with DVI-D In)		
13.	PC Out	Mini D-Sub 15-pin x1		
14.	USB A	USB TYPE A Connector x 1 (For Memory Viewer)		
15.	USB B	USB TYPE B Connector x 1 (For Touch Panel)		
16.	External Speaker	50 W [25 W + 25 W] (10 % THD)		
17.	DIGITAL LINK	RJ45 x 1 (Shared with LAN)		
18.	Built-In wireless LAN function	IEEE802.11b / g / n, :IEEE802.		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
19.	Picture -in-Picture Capability	Picture-in-Picture mode		
20.	Other Features	Picture-in-whiteboard mode		
		Instant playback of content via USB		
		wireless solution with multiscreen functions		
		Quick start whiteboard		
		Write and draw on media from external devices		
21.	Touch Features	up to four people can write at a time, and saving option with email to anyone		
22.	Video Conferencing	Yes		
	Others			
23.	Matrix Switcher	• Should support TMDS digital RGB HDMI and single-link DVI digital video signals are supported. • Should support Digital Video RGB digital video • Should support Digital video support • Should support Digital Audio support • Should Support hot plug detection (HPD) of display as a pass-through signal • Should support Video Input • Should support Video Output • Should support communication on Serial port control, mini stereo jack , Ethernet control port, HDMI		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
24.	Cable Cubby	Should be sleek metallic cable cubby with interface facility of Power, RGB ,Audio, VGA, HDMI,LAN		
25.	Rack	Yes (to accommodate all products		
26.	External accessories	Yes (to furnish and accommodate all items of room)		

1.30. *AV for Conference Room - 50 seating capacity*

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
Projector				
1.	Make			
2.	Model			
3.	Projector Panel size	0.6"diagonal		
4.	Display Method	Transparent LCD panel(x3, R / G / B)		
5.	Pixels	786,432 (1,024 x 768) x3, total of 2,359,296 pixels		
6.	Lens	F1.60-2.12, f15.30-24.60mm		
7.	Brightness	4200 lumens		
8.	Contrast (Full on /Full off)	4000:01:00		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
9.	Keystone Correction Range	Vertical ±40°(±30° when easy setting); Horizontal ±30° (±20° when easy setting)		
10.	Built-in Speaker	10 w(monaural)		
11.	Terminals	HDMI IN 19-pin x 1, HDCP compatible		
		Computer RGB 1 IN D-sub HD 15-pin (female) x 1		
		Computer RGB 2 IN /1 OUT D-sub HD 15-pin (female) x 1		
		LAN RJ-45 x 1, for network connection, 100 base-TX/ 10 base-T, complaint with PJLink		
		USB A (type A0 connector x 1, for USB memory viewer		
		USB B (type B) connector x 1, for USB display		
12.	Wireless LAN	IEEE 802.11a / b / g /n		
13.	Operating range	Approx. 30 m (98 ft 5 in)		
14.	Security	Instructure mode WPA-PSK(TKIP or AES), WPA2-PSK(TKIP or AES), WEP (128 bit / 64 bit)		
15.	Wireless facilities	Miracast compatible		
16.		projection from iOS or android devices		
17.	Lamp Life	up to 6000 hrs		
Mixer				
18.	Frequency response	20 Hz to 20 kHz, ±0.05 dB		
19.	THD + Noise	0.03% @ 1 kHz at nominal level		
20.	S/ N	>90 dB (balanced) at rated maximum output		
21.	CMRR	>75 dB @ 20 Hz to 20 kHz		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
22.	Audio Input	4 stereo, balanced or unbalanced		
23.	Connectors	(4) 3.5 mm captive screw connectors, 5 pole		
24.	Impedance	>17k ohms unbalanced, 23k ohms balanced, DC coupled		
25.	Nominal level	+4 dBu (1.23 V)		
26.	Maximum level	+20 dBu (7.75 V), (balanced or unbalanced), at 1% THD+N		
27.	Number Or signal type	4 mono, balanced Or unbalanced		
28.	Connectors	(2) 3.5 mm captive screw connectors, 5 pole (double stacked)		
29.	Impedance	<50 ohms unbalanced; 100 ohms balanced		
30.	Nominal level	+4 dBu (1.23 V)		
31.	Maximum level (Hi-Z)	>+23 dBu, balanced; or >+17 dBu, unbalanced at 1% THD+N		
32.	Maximum level (600 ohm)	>+21 dBm, balanced; or >15 dBu, unbalanced at 1% THD+N		
33.	External power supply	100 VAC to 240 VAC, 50-60 Hz, external, to 12 VDC, 1 A (max.), regulated		
34.	Power input requirements	12 VDC, 0.2 A		
35.	Temperature Or humidity	Storage: -40 to +158 °F (-40 to +70 °C) Or 10% to 90%, noncondensing		
36.	Temperature Or humidity	Operating: +32 to +122 °F (0 to +50 °C) Or 10% to 90%, noncondensing		
37.	Cooling	Convection, no vents		
38.	Rack mount	Yes, with optional 1U rack shelf		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
39.	Furniture mount	Yes, with optional mini under desk mounting kit		
40.	Pole mount	Yes, with optional mini projector mounting kit		
41.	Enclosure type	Metal		
42.	Enclosure dimensions	1.7" H x 4.3" W x 3.0" D (1U high, quarter rack wide)		
43.	Enclosure dimensions	(4.3 cm H x 10.9 cm W x 7.6 cm D)		
44.	Enclosure dimensions	(Depth excludes connectors.)		
45.	Vibration	ISTA 1A in carton (International Safe Transit Association)		

1.31. Interactive Screen for EOC (Emergency Operations Centre)

Bidder may continue using the same Interactive Screen for EOC, provided extended maintenance can be availed, if not bidder has to provide equivalent or higher model product.

1.32. *Mobile Data Terminal (MDT)*

Sl. No.	Features	Minimum Specifications	Complied (Yes/No)	Deviations (if any)
Make				
Model				
1	Processor	Octa core CPU up to 2.2 GHZ		
2	Memory	RAM at least 4 GB		
3	Storage	At least 64 GB or higher		
4	Operating System	Android 10 or higher		
5	Google Recommended	AER		
6	Generation	4G, LTE, 5G readiness(preferable) and support APN networks		
7	GSM	Yes, Support dual SIM		
8	Screen size	7inches or more with capacitive multi touch support i.e. multiple finger touch parallel		
9	Voice and speaker	Voice recording should be possible, built-in microphone, built-in Speaker. It has to support Video conferencing		
10	Camera & Video	5MP Front and 13 MP rear with LED Flash (integrated)		
11	Feature	Should work as AVLS device for AVLS or CAD application, supports turn by turn navigation with voice and install auto updates for CAD, GIS and other relevant application		
12	Screen luminosity	Min. 500 nits, Daylight readable		
13	Ruggedness	At least IP 65 certified preferably IP 67 standard complied and MIL 810G Certified		
14	Speakerphone	Hands free Support		
15	Keyboard	Virtual on Screen		
16	Integration Support	Should be able to integrate with CAD, GIS and other application like MDT security etc.		
17	GPS	Yes, and support for inbuilt GLONASS		
18	Audio Playing Format	MP4, wav files format etc.		

Sl. No.	Features	Minimum Specifications	Complied (Yes/No)	Deviations (if any)
19	Environment Specification	(-)0 °C to 50°C, Humidity 95% RH, Non-condensing		
20	Ports	USB Type C port, charging port, Headset through BT Support, DC charging support etc.		
21	Expansion Slots	Integrated		
22	Power Supply	230V, 50 Hz AC Supply		
23	Bluetooth	Yes (v 4.0 or above)		
24	Adapter	AC Input:100-240V		
25	Battery	Minimum 3000 mAh power with 8 hours backup in Active mode, Preferably with hot swappable feature		
26	Charger	Electric Charger (DC charger) Built-in rechargeable battery Convertor required in case of no USB port in the vehicle		
27	Mounting	On-vehicle rugged docking station with required locking		
28	Wireless	Yes with 802.11 a/b/g/n/ac standard, should be dual band		
29	IPv6 Compliant	Yes		
30	Security Features	Password Security		
31	Certification	Valid Bureau of Indian Standards (BIS) certificate		
32	Charger Certification	IEC 60950, IS13252:2010, ROHS		
33	OEM Experience	The OEM should have an experience of providing minimum 3,000 MDTs in last 5 years The MDTs should be deployed and operational on at least 2 projects in India		

1.33. Smart phones

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Make			

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Model			
1	Display Size	5.5 to 6.5 inches		
2	Display	AMOLED		
3	RAM	6Gb or Better		
4	Storage	128Gb or Better		
5	Processor	Qualcomm Snapdragon 680 or better or equivalent		
6	Operating System	Android 11		
7	Battey capacity	5000mah or better		
8	Connectivity technologies	Bluetooth, Infrared, Wi-Fi, USB		
9	Resolution	1080X2340 or better		
10	SIM	Dual SIM		
11	Network	GSM / HSPA / LTE / 5G		
12	Charger	15W or better Fast Charging		
13	Main Camera	48MP or better		
14	Front Camera	12MP or better		
15	WLAN	Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot		
16	Bluetooth	5.0, A2DP, LE		
17	GPS	Yes, with A-GPS, GLONASS, GALILEO, BDS		
18	Tempered Glass Screen Protector Compatible	Bidder to maintain glass for the project cycle		
19	Mobile cover	Bidder to provider Rugged Armor Back Cover Case with Shock-Absorbent feature for		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
		mobile for the project cycle		
20	Compliant	IP67		
21	Drop test	Should pass drop test with 5 feet height		

1.34. ROIP Application and Gateway

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
1.	Make			
2.	Model			
3.	General requirement	The system should be able to provide radio interface gateway for connectivity to all VHF Networks. The communication with the radio server and network interface equipment must be based on IP over the VOIP network.		
4.	General requirement	The officer should be able to access the system through web-based application and should be able to connect the radios frequencies devices at field level in same location or in different location of UP state		
5.	General requirement	Connectivity between RADIO Server and VHF base station will be for communication with DMR signalling should provide to have Radio features operation from Control room.		
6.	General requirement	System should have a capability to configure minimum 7 frequency and officer should have an option to select any frequency to speak with the field officer		
7.	General requirement	The RADIO Server must be integrated with Call 100 Application and should provide the communication path between the officer console and existing wireless radio equipment. All the wireless radio equipment present in vehicle must be wirelessly connected to the RADIO Server in broadcast mode over RF.		
8.	General requirement	System should support one to one and one to many communication among all devices at same location or different location over the IP network		
9.	General requirement	System should have a capability to group more than 2 radios wireless network together.		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
10.	General requirement	The radio communications should be recorded by the system with internal or external system like contact center recording and ROIP voice recording. The recording should continue and be stored for the required period of time and recorded voice files should be accessible from the Web based application also. The recorded file should be tagged with time or date stamp Or Incident ID also		
11.	General requirement	It shall be possible for the officer to organize a conference call minimum three phone lines from his console.		
12.	General requirement	The system should be integrated with fixed-line, mobile phones, PCs, IP phones etc.		
13.	General requirement	System should have an ability to listen the radio voice channel and system should have an ability to put the call on hold		
14.	General requirement	The system should support many different Land Mobile Radios in audio such as analog conventional radio and digital trunking radio through gateway		
15.	General requirement	The radio gateway location should convert the audio and control signals received from the radio into IP packets and transmit them to the main system for further processing, over an IP link.		
16.	General requirement	System should be implemented in high availability mode with no single point of failure and system should be agnostic to the make of the radio and its frequency of operation		
17.	General requirement	It should be possible to add more Radio gateway at different locations or at the same location over the IP network to connect more radio set.		
18.	General requirement	Voice logger should be able to integrate internal/external reporting module to generate the desired reports		
19.	General requirement	System should have an ability to broadcast the message over the wireless radios in vehicles and other location in UP state		
20.	General requirement	System should support Linux/ windows.		
21.	General Requirement	Should support IPv6 QoS, IPv6 Multicast support etc. from day 1		
22.	General Requirement	Should be able to control the configuration of the radio, to which it is connected. The configuration will be done by the system administrator		
23.	General Requirement	Should have Radio Interface for Analog / Digital DMR Radio/ DMR Repeater		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
24.	General Requirement	Should have **call types** like: Selective Call Group Call All Group Call Remote Monitoring Remote Radio Disable / Enable		
25.	General Requirement	Should support different message types like group, broadcast		
26.	General Requirement	Should have location tracking based upon GPS		
27.	General Requirement	Should have configurable control at central or district level		
28.	General Requirement	Bidder will provide compatible foot paddles with Radio gateway solution of standard quality		
29.	Network Requirements	• Device Payload: 1kbps idle, 32Kbps(ADPCM)/ 64kbps(ALAW) active per user • Network Loading: Minimum 128kbps Network Bandwidth • Packet Loss: <1% • Packet Delay: <100ms (Programmable depending upon net speed) • Network Type: Fully switched Ethernet, full duplex.		
30.	General	• Dimensions: 1.75 x 5.9 x 4.3 inches (H x W x D) • Weight: 360g • Operation Temperature Range: -10 to +55 Celsius • Power: 9V DC, 500mA • Network Connection: 10/100 Base-T Ethernet connection using RJ-45		
31.	Radio Signals Used	• PTT • Carrier • Receive Audio • Transmit Audio		
32.	OTHER FEATURES/ APPLICATIONS	• Wide Area Network Connectivity. • Remote PC connectivity to a known radio channel. (Optional) • Auto-Connection on link or power reset. • User Programmable IP Configuration. • Flexible Port Address Configurability. • Secured Communication by using Authentication Packets. • Connection between Static IP Network and a Static/Dynamic IP Network. • Dynamic Ip Connectivity with domain names • Web based Configuration Settings		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
		• Carrier/ Vox operated Mode (programmable). • Local Repeat Mode Feature (programmable). • Selectable CSQ or PTT priority feature. • Adjustable PTT Delay depending upon net speed. • Programmable PTT Time out Timer (TOT). • Remote Channel Change • RSSI Level Indication • DTMF Decoder (for Dialling in Server Console Configuration) • Digital Radio Support (for Server Console Configuration) • Multi-Connection Mode for Redundant Server Configuration		

1.35. *VHF 4W antenna (Transceiver VHF Mobile radio 25 Watt Synthesized)*

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Make			
	Model			
	General	Standard 0dB gain ¼ wave mobile metallic Antenna with 3 mtrs. cable, connector with magnetic base of reputed brand: OEM test Certification to be attached.		
	General	Transceiver VHF Mobile radio 25 Watt Synthesized		

1.36. Lattice Mast for VHF static set

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
Galvanized Aerial Mast				
1.	Make			
2.	Model			

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
3.	General	The 80ft mast consists of 8 sections of 10ft or 3mtr each of lattice steel structure having flange coupling at both ends for joining or interlocking sections with each other. The complete mast after fabrication is hot dip galvanised as per IS 4759 and a copy of the test report of NABL lab must be enclosed with the bid.		
4.	General	Each section of 10ft is made using vertical members of MS bright bar of minimum 16mm dia and bracing of 8mm MS rod. Coupling flange are made of MS angle 35x35x5mm.		
5.	General	Each mast is supplied with one base plate made using MS sheet of 24"x24"x8mm with hinge arrangement and 4 ground pegs. the base plate is also hot dip galvanised after fabrication.		
6.	General	4 sets (each set having 3 guys) of steel guy galvanised of suitable length of minimum 6mm dia are supplied for fixing at height of 20ft,40ft,60ft and 80ft . The mast is supplied with sufficient numbers of straning screw or turn buckle, d-sacle, dog clamp, thimbles, nut bolts all galvanised		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
7.	General	3 sects of guy anchor of 1mtr length are supplied with each mast, fully hot dip galvanised.		
8.	Other	The 80ft mast is supplied with antenna hoisting mechanism consisting of pulleys, trolley and steel guy which enables to hoist the antenna and cable from the ground without having to lower the mast.		
9.	Other	The manufacturer of the Aerial masts' credentials like MSME registration, NSIC, DGS&D or D.I. registration, ISO certification etc. must be enclosed with tender document.		
10.	Other	Test report of any NABL laboratory must be enclosed for the following : a. Hot dip galvanising as per IS-4759 b. Structural steel used in the fabrication of mast.		
11.	Other	The mast is to be supplied with antenna and cable hoisting mechanism consisting of trolley, pulley and steel guys which enables the hoisting of antenna and cable from the ground without having to lower the mast.		
12.	Other	Structural approved drawing must be enclosed with the bid		
Antenna arrangements				

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
13.	Transceiver VHF Static radio, 25 Watt Synthesized	Standard 3dB GP Antenna, of reputed brand		

1.37. *VHF static radio device*

Sl. No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Make			
	Model			
A	GENERAL			
1	Frequency Range	136-174 MHz (full band)		
2	Channel capacity	255 or more		
3	Protocol	TDMA (02 slot)		
4	Channel spacing	12.5 KHz		
5	Frequency Stability	+ 1.5PPM or better		
6	Weight	Less than 2 kg		
7	Operating Voltage	10.8 to 15.6Volt DC with reverse polarity protection		
8	Antenna Impedance	50 Ohm		
9	Communication Interface	Ethernet/USB/RS232		
10	Display	Multifunction alphanumeric LCD display with back light/LED display. Readable in day light, sun light and in night. Minimum 3 rows or better.		
11	Compatibility	Shall be fully compatible (in terms of Voice, Data & GPS etc.) with existing DMR radios & Dispatcher software of UP112		
12	Field Trial	Compatibility of the Radios with RoIP system		
B	TRANSMITTER			
1	RF Power output	25 W + 0.5 dB as Programmable		
2	Type of emission	Analog 11KOF3E Digital-4 FSK or equivalent technique complying to open standards/ non propriety digital protocol as defined by international standard body like ETSI/FCC etc.		
3	Digital Modulation	4FSK		
4	Modulation Limiting	+2.5 KHz		

Sl. No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
5	Audio Response	+1, -3dB, as per TIA 603D		
6	FM Hum noise	-40dB or better		
7	Adjacent channel power	-60dB or Better		
8	Digital Vocoder	AMBE+2		
C	**RECEIVER**			
1	Sensitivity	Analog: 0.22 uV typical (12dB SINAD) or better. Digital: 0.19µV typical @5% BER or better		
2	Adjacent channel Selectivity	60 dB or better as per TIA603A-1T		
3	Inter –modulation	70dB or better as per TIA603A-1T		
4	Audio output	Minimum 3 watt with built speaker		
5	Audio distortion	3% or better		
D	**ENVIRONMENTAL SPECIFICATION**			
1	Operating Temperature	-0º C to +55º C		
2	Storage Temperature	-0º C to +60º C		
3	Humidity	95% max at +40°C non-condensing		
4	Applicable MIL standard	MIL standard 810 C/D/E/F/G		
5	Applicable IP standards	IP 54		
E	FEATURE			
1	Mode of operations	Analog conventional, digital conventional		
2	Inbuilt GPS	Radio shall be GPS compatible**.**		
3	Text Messaging	Radio shall have facility of sending short messages from keypad and pre-defined messages**.**		
4	Protection	Reverse polarity protection. Protection against high VSWR		
5	Radio Programming Facility	PC programmable		
6	Handset with Mike Keypad	DTMF Front panel keypad with backlight		
7	Signal Strength indicator	Receiver signal strength indicator or digital readout		
8	OTAR	Should have provision for over the air frequency re-programming (wirelessly).		
9	Integrated Bluetooth	Should be supplied with Integrated Bluetooth for sharing data wirelessly and instantly between devices.		
10	Networking	Should be IP based for automatic roaming etc.		

Sl. No.	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
11	Over Riding	Radio Should have feature to override ongoing communication **on the same channel** if it is required by Higher officials.		
12	Integrated Wi-Fi	Radio shall have provision to upgrade with integrated Wi-Fi enable for remote software updates.		
13	Text to voice Message	Radio Shall have **facility to convert text message into vocal voice for ease of operations.**		
14	Networking	Capability for Multi-channel per site with Multi site roaming facility in IP Network		
F	**OTHER FEATURES**			
1	Alpha numeric list of 256 users for sending SMS & for selective calling			
2	Alpha numeric channel alias			
3	Alpha numeric PTT ID alias			
4	Facility to assign network access code, CTCSS/DCS			
5	Channel scan & priority channel scan			
6	Call alert			
7	Talk around			
8	Emergency call			
9	Selective call, group call			
10	Late entry			
11	Busy channels lock out			
12	Capable to kill-unkill, disable -enable			
13	Externally accessible accessory connector. (For connecting programming kit. Repeater interface, Data interface etc.)			
14	Vendor shall mention other manufacturer's models of the radios which are inter portable for voice & data communication to the system offered.			

1.38. *VHF Hand-Held Radio device*

Sl. No.	Features	Minimum Specification	Compliance (Yes/No)	Deviations (Yes/No)
Make				
Model				
A	**GENERAL**			
1	Frequency Range	136-174 MHz (split or full band)		
2	Channel capacity	255 or higher (For display)		
3	Protocol	TDMA (02 Slot)		
4	Channel spacing	12.5 KHz or better		
5	Frequency stability	±1.5 PPM or better		

Sl. No.	Features	Minimum Specification	Compliance (Yes/No)	Deviations (Yes/No)
6	Weight	Light in weight preferable, including accessories.		
7	Battery capacity	Capacity Preferable Li-ion rechargeable battery of 2000mAH or better. Vendor shall mention DC Voltage. During capacity test, battery shall give 100% of its rated capacity if discharged by C/5		
8	Antenna Impedance	50 ohm		
9	Communication Interface	Ethernet/USB/RS232		
10	Display	Multifunction alphanumeric LCD display with back light/LED display. Readable in day light, sun light and in night. Minimum 3 rows or better.		
11	Warranty	Standard warranty is for 2 years		
12	Compatibility	Shall be fully compatible (in terms of Voice, Data & GPS etc.) with existing DMR radios & Dispatcher software of UP112		
13	Field Trial	Compatibility of the Radios will be checked during Trial/Demo		
B	**TRANSMITTER**			
1	RF Power output	1 Watt to 5 Watt±0.5 dB programmable		
2	Type of Emission	Analog-11K OF 3E Digital-4 FSK or equivalent technique complying to open standards/ non propriety digital protocol as defined by international standard body like ETSI/FCC etc.		
3	Digital modulation	4FSK		
4	Modulation Limiting	± 2.5 KHz		

Sl. No.	Features	Minimum Specification	Compliance (Yes/No)	Deviations (Yes/No)
5	Audio Response	+1, -3dB, As per TIA 603D		
6	FM Hum noise	- 40dB or better		
7	Adjacent channel	power -60 dB or better		
8	Digital Vocoder	AMBE+2		
C	**RECEIVER**			
1	Sensitivity	Analog: 0.16µV (12dB SINAD) or better Digital: 0.14µV @5% BER or better		
2	Adjacent Channel Selectivity	60 dB or better as per TIA603A-1T		
3	Inter- modulation	70 dB or better as per TIA603A-1T		
4	Audio Output	Minimum 500 m watt		
5	Audio distortion	3% or better		
D	**ENVIRONMENTAL SPECIFICATION**			
1	Operating temperature range	0°C to +55°C		
2	Storage temperature	0°C to +60°C		
3	Humidity	95% max at +40°C non-condensing		
4	Applicable MIL standards	MIL standard 810 C/D/E/F/G		
5	Applicable IP standards	IP IP68 Capable		
E	**FEATURE**			
1	Mode of operations	Analog conventional, digital conventional Simple press to talk		
2	Inbuilt GPS	Portable radio should have inbuilt GPS & it has GPS antenna embedded within the radio**.**		
3	Text Messaging	Radio shall have facility of sending short messages from keypad and pre-defined messages**.**		
4	Protection	Reverse polarity protection. Protection against high VSWR		
5	Radio Programming Facility	PC programmable		
6	Front panel Keypad	DTMF front panel keypad with back light		

Sl. No.	Features	Minimum Specification	Compliance (Yes/No)	Deviations (Yes/No)
7	Battery strength indicator	Battery strength bar indicator or digital readout. Beep alert for low battery		
8	Signal Strength indicator	RSSI-Received signal strength indicator bar or digital read out.		
9	OTAR	Should have provision for over the air frequency re-programming (wirelessly).		
10	Integrated Bluetooth	Should be supplied with Integrated Bluetooth for sharing data wirelessly and instantly between devices.		
11	Networking	Should be IP based for automatic roaming etc.		
12	Over Riding	Radio Should have feature to override ongoing communication **on the same channel** if it is required by Higher officials.		
13	Integrated Wi-Fi	Radio shall have provision to upgrade with integrated Wi-Fi enable for remote software updates.		
14	Text to voice Message	Radio Shall have **facility to convert text message into vocal voice for ease of operations.**		
15	Networking	Capability for Multi-channel per site with Multi site roaming facility in IP Network		
F	**OTHER FEATURES**			
1	Simple press to talk			
2	Alpha numeric list of 256 users for sending SMS & for selective calling.			
3	Alpha numeric channel alias.			
4	Alpha numeric PTT ID alias			
5	Facility for locking the channel or keypad. (Programmable)			

Sl. No.	Features	Minimum Specification	Compliance (Yes/No)	Deviations (Yes/No)
6	Facility to assign Network access code, CTCSS/DCS			
7	Channel scan & priority channel scan			
8	Call alert			
9	Talk around mode			
10	Transmitter Time Out Timer (TOT) operation			
11	Emergency call facility (SOS)			
12	Selective call, group call.			
13	Late entry			
14	Busy channel lock out			
15	Capable to kill-unkill, disable-enable			
16	Any one of 2 tone/5 tone/DTMF signaling			
17	Text message & pre-defined messages			
18	Automatic number identification			
19	OEM shall mention other manufacturers' models of the radios which are inter-operable for voice &data communication to the system offered.			

1.39. Battery of VHF Static Radio Device

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
1	Make			
2	Model			
3	12 V 100 AH SMF VRLA BATTERY	Sealed Lead –Acid Valve regulated type		
		Nominal Voltage : 12 Volts		
		Rated Capacity at 20-hour discharge rate : 100 AH		
		Confirming Japanese Industrial Standards JIS C 8702 Or 2009 (Part 1) : Certificate to be enclosed		
		Battery should be supplied from appropriate leading OEM		

1.40. *Battery of VHF Handheld Radio Device and Charger of Battery pack*

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
4	Make			
5	Model			
6	Type of Radio - Trans receiver VHF	Rechargeable battery pack (original from OEM) of minimum		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Handheld , 1 Or 5 watts synthesized	2000mAH capacity, Ni-Mh or Li-ion, Li-polymer suitable for offered VHF hand held ratio set : certificate from OEM to be attached		
		All batteries should be mechanically and electrically interchangeable with the corresponding Trans receiver model		
		The battery capacity should not be less than the rated capacity when discharged		
		Month & year of manufacture and the logo or trademark of the OEM to be embossed or heat stamped. This logo or trademark is to be indicated in the offer		
		The sleeve of the cells used should preferably indicate the following:		
		1. Part Number		
		2. Month and year of manufacture		
		3. Voltage of cell		
		4. Capacity		
		5. Country of origin		
Charger of Battery pack of VHF Hand Held Radio set				
	General Requirement	Single unit battery charger from OEM of offered radio: certificate from OEM to be attached		
	Input voltage	230 volt AC (+ / -) 10% of 50 Hz		
	Output voltage	As per the set rechargeable battery pack for which charger is supplied		
	General Requirement	Capable of charging Battery packs of 7.2 V		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
		Or 7.4 V Ni-mH or Li-ion or Li-Polymer upto 3000 mAH capacity or better		
		Visual indication for all mode of charging status		
		Reverse polarity protection (DC input) should be provided		
		Reverse polarity protection (Battery terminal) should be provided		
		Short circuit protection should be provided		
1	Battery charging rate on constant current	The battery charger may be standard type or rapid type. In case of standard type charger, the charging current shall not exceed 400 mA and for rapid type, it shall be within 1 Amp. The charging time shall be 6 to 14 hours for standards charger and 1 to 3 hours (for charging batteries up to 1800 mAH) or 2 to 4 hours (for charging batteries from 2000 to 3000 mAH) respectively		

1.41. RFID Reader and Controller

Sl. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations (if any)
1	**Make**			
2	**Model**			
RFID for the inventory and stock verification including vehicle items.				
3	Hand Held RFID Application:	a. Shift end check of assets		
		b. Asset tracking		
		c. Inventory management & Search		
4	RFID Device	a. Android RFID Hand Held Computer with 38keys keypad layout with Gun Grip		

Sl. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations (if any)
	Specific features:	b. Should operate on India specific freq 865-867 Mhz		
		c. Compatible with EPC Gen2		
		d. Min 900 reads/ sec.		
		e. Should allow min 15 meters read range		
		f. Replaceable battery of 6000 mAh and above		
RFID Fixed reader – Setup for transition check and security Check - SURVILLANCE				
5	Fixed Reader RFID Applications	Uses Existing FASTag for Checkpoint monitoring		
		Seamless Information Flow – Alerts/Notification		
		Track vehicles - Surveillance		
		Secure Cloud based interface		
		All Weather / Nighttime Surveillance		
6	RFID - Fixed Reader Specific features:	Designed for round the clock operation with min 8 antenna support.		
		Should operate on India specific freq 865-867 Mhz		
		Compatible with EPC Gen2		
		Min 1300 reads/ sec.		
		High sensitivity of -86 DBM and above		
		LLRP, https, direct interface to cloud server		
		should support True cloud interface with intelligent IOT protocol		
		Should have Protect network services on the reader using SSL/TLS protocol with Public Key Infrastructure digital certificates to secure the communication channel against eavesdropping or tampering, and optionally authenticate peer networked nodes involved in the communication.		
		Reader configuration using pre-defined use case profiles on specific readers that can be set via the cloud		
7	GPS tracking device with additional features-	GPS tracking device with additional features- 1. Real-time tracking. 2. Check past 90 days history with location & km. 3. Over speed limits. 4. Geo-fencing (Mark your areas with alerts) 5. We can create own path on Software. 6. Check the engine health as per km.		

Sl. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations (if any)
		7. Immobilizer (Ignition ON/OFF), Only for key start vehicle. 8. Tempering Alerts if anyone wants to remove or disconnect your device. 9. Share your location. 10. Upload the details on portal like DL, RC, Insurance with renewing alerts. It will alert before 1-2 months of the expiry date. 11. If you are using a GPS device on more than one vehicle, you can also track nearby vehicles. 12. Also, check the stops in a timely.		

1.42. RFID tags

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)
	Make		
	Model		
1	Type: Passive Tags Write once Read Many Reading range 10 meter or better		
2	Frequency: Compatible with offered RFID reader		
3	Data Transfer Rate: At least 512 kbps		
4	Protocol: EPC Gen 2, ISO 18000-6C		
5	Tag Memory:Unique Tag ID – 64 bits, EPC memory – 240 bits It should be able to store the unique tag reference ID, and other key details.		
6	Tag ID:Tag should be programmed with unique Tag ID of 26/32/64 bit. Tag ID to be divided in to 2 parts –Facility code & Serial no.		
7	Material: Plastic substrate with printed antenna		
8	Physical printing of Tag ID on the Tag: The Tag ID shall be physically printed on the Tag using the Hexadecimal numbering system and shall be		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)
	adequately clear for easy visual recognition		
9	Tamper Proof RFID Label: The tags should be RFID Tamper Proof Label specially designed for tagging directly to an item. Any attempt to rip or tamper the label should result in disabling the functionality of the tags to ensure a unique one to one relationship between the tag and the vehicle thereby preventing unauthorized tag removal and transfers. Such features of the RFID label should result in following actions: 1. Destroy or Damage the Antenna 2. Break the chip antenna connection. The manufacturing process, construction of tags and associated materials should ensure reliable tamper indication even when sophisticated tamper methods of Mechanical Attack (e.g. Razor Blades, Knives etc.), Chemical Attack (using Corrosives, Solvents etc.) and Thermal Attacks are employed.		
10	Operating Temperature: 0°C to 60°C		

1.43. Earthing

Sl. No.	Requirement	Description	Compliance (Yes/No)	Deviations (Yes/No)
1.	General	Chemical Earthing Electrode with Earth Enhancing compound with Dia.14.2mmx3.0m long steel rod with 250micron Copper coated earthling electrode suitable for 18KA fault current along with 10kg earth enhancing chemical blackfill compound as per IEC 62561-7 and 1 no. industrial Poly propylene plastic pit cover. including connections from earthing to devices with conduit & cable		

1.44. Body Worn Camera

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
Make:				
Model:				
1	General	The body worn camera should consist of a single device comprising of the camera, rechargeable battery and recording unit. It should be able to capture clear high-definition video @ audio as well as take still photograph. It should be able to compress video/audio files using appropriate non-proprietary algorithm and store it on local drive.		
2	Image Resolution	Image Resolution: 35 MP or better		
3	Weight	Should not be more than 200g		
4	Field of view of lens[H]	120 degree or better		
5	Connection Interface	Mini USB 2.0 port or better, MIC, Speaker, Micro SIM card slot		
6	Storage	The body worn camera should have storage of 256 GB or above via on-board storage solid state storage or SD Card**.**		
7	Battery Life (Fully Charged)	8 Hours for continuous operation		
8	Recording Resolution	Recording Resolution: Full HD (1920*1080 Pixel or better)		
9	Frame Rate	30 FPS		
10	Operating Temperature	-0˚C to +55˚C		
11	IP Rating	water resistant of IP67 or better and test report need to be provided		
12	Viewing Angel	130˚ (diagonal) or more		
13	IR	It should also have capability of night mode recording. Support maximum 10m IR, see the face in 3m at night, see the human body in 10m		
14	Certification	CE/FCC/RoHS/ BIS		
15	Drop Test	Minimum 1.8 meter		
16	Video compression	The camera must support H.265 or better compression algorithm and should offer the compression at up to 30 frames per second		
17	Display	Min. 2.4-inch LCD Touch Screen		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
18	Replay	The body worn camera should be able to play recorded audio/video/image on screen.		
19	Processor	8 Core 64-bit processor or better		
20	Multi Stream	The body worn camera should support 2 streams, each stream should support 1080P@30fps		
21	Day & Night	IR cut filter with auto switch		
22	Network	The body worn camera should be built in 3G/4G for live streaming, Wi-Fi, Bluetooth		
23	Face captures	The body worn camera should support face detection, face picture capture, and uploaded		
24				
25	Service Centre	OEM must have its service center in India preferable in Uttar Pradesh		
26	Required Accessories	Universal Clip, Car charging adaptor and charging Dock, Charger, USB cable, Manual		
27	Docking Station	8-Port Docking Station with charging & data unloading with backup facility. Docking station should be having minimum 12inches of touch screen. Unlocks Body Camera bin by recognizing face to guarantee safe device storage (As Required with offered model)		
28				
29				
30				
31	MAC	The MAC Address of the Body Worn Camera should be registered in the name OEM supplying the cameras.		
Minimum Features for Body Worn Cameras:				
1	The Body Worn Camera shall have at least 12 hrs of recording time.			
2	The Body Worn Camera must be able to remain in stand-by mode for at least 24hrs.			
3	The Body Worn Camera shall be able to export video with the following watermarks: Date, Time etc.			
4	In order to ensure officer safety, the Body Worn Camera must be able to enter a covert mode, wherein the Body Worn Camera does not make any audible sounds or display any time of lighting. Body			

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Worn Camera should have SOS button through which officer can send emergency signal to command and control centre.			
5	The solution shall support the ability to start a recording instantly upon manual or automatic wireless initiation.			
6	The Body Worn Camera shall support push to talk feature should be present in BWC, it will help command and control centre to do audio communication with body worn camera			
7	The solution is centralized with the capability of organizing/managing incidents and be accessible via the internet to multiple users simultaneously.			
8	The solution shall support both local, remote, and hybrid storage options.			
9	The solution shall allow remote access for monitoring through Server/PC and App for viewing.			
10	The solution shall provide user authentication with a unique username and password.			
11	Authorized users can be established based on various roles and permissions by a system administrator.			
12	The solution shall provide transfer of video from body worn camera to dock station / Central Storage using 4G			
13	When video is uploaded, the videos on the system will have defined retention period before deletion to allow the officer to still review the video on the system.			
14	Solution shall be capable to automatically/manually archive video tagged as "evidence" based on video tagging and policy requirements			
15	**The Body Worn Camera shall support 1920x1080(1080p), 1280x720(720p), 720x576 (576p) resolutions.**			
16	The Body Worn Camera shall weigh less than 200 gm in order to reduce carrying load of the officer.			
17	Solution shall be capable to automatically transfer video via system workflow based on policy and requirements			
18	The solution provides for remote viewing of the stored video for non-technical staff as well as others based on the permissions granted by the system administrator.			
19	The solution can create a log/audit trail illustrating users who have viewed and copied video to an			

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	external source (e.g., HDD/Pen Drive/DVD/CD/ TF Card/any storage).			
20	The Body Worn Camera shall support 120-degree field of view and shall contain a built-in microphone.			
21	The Body Worn Camera shall support in-field tagging of captured assets with up to 64 categories.			
22	The video Codec (Compression) must be ~~H.264/MPEG4-10~~ H.265 or equivalent technology			
23				
24	Solution provides encryption in storage and transport and provides security back-up of all data.			
25	Solution must securely store all videos and recordings in a way that only Unified Government authorized users and users authorized by the client			
26	Solution must have the ability to grant access to specific files to specific persons for a specific time period.			
27	Solution must have the ability to set a variable retention rules per department preferences including:			
28	Type of case/incident recorded.			
29	Tags placed on video.			
30	Other user defined criteria.			
31	Solution must have the ability to set time tables for automatic deletions of files			
32	The system must be capable of demonstrating an industry standard method of validating the reliable transfer of data from the recorder to the backend storage system. A digital signature/watermark must be produced that can be used to validate the transfer of data.			
33	System must ensure the video has been successfully uploaded prior to deletion from the device.			
34	The Body Worn Camera shall contain an internal battery with at least 3300 mAh of capacity.			
35	Solution has the ability to preserve the raw file without editing.			
36	The Body Worn Camera shall contain storage of at least 256 GB			
37	The solution will allow for the uploading of evidence direct to server environment and/or through a local server that will accept data even if server environment is slow or unavailable.			
38	Regardless of time source used, software shall able to display recordings in local time.			
39	The system which handles the recordings shall allow multiple concurrent user log-ins.			
40	The system supports recording video with Audio			

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
41	The system operator can check video and audio recording			
42	The system supports recording video with Audio			
43	The system operator can check video and audio recording			
	a)			
	b)			
	c) System shall have a complete audit trail generated for all digital evidence to include:			
	d) Uploading.			
	e) Viewing.			
	f) Exporting.			
	g) Sharing.			
	h) Deleting.			
	i) Redacting.			
	j) Indexing.			
	k) Updating.			
	l) Purging.			
	m) Audit trail should include:			
	n) Username.			
44	The solution shall have the ability to authenticate a person's credentials through Windows Active Directory.			
45	The solution shall support role-based access control for separation of duties of assigned roles.			
46	The solution shall have the ability to produce reports which identify who have access to run reports.			
47	The solution shall generate an audit trail log depicting report additions, deletions or changes noting the user who made change, time and date stamp.			
48	The audit logs shall have the ability to capture when data is viewed and note the user, time and date stamp.			
49	The Body Worn Camera must be easily controlled by an officer while wearing gloves.			
50	The Body Worn Camera must support the ability to mute audio recordings while in the field.			
51	The Body Worn Camera must not utilize a camera lens that can be moved from a fixed position in order to reliably capture video.			
52	The Body Worn Camera must not require any type of adhesive to be mounted.			
53	The Body Worn Camera shall support the ability to toggle any type of recording light in order to preserve officer safety.			
54	The Body Worn Camera shall not incorporate any type of hall sensor into its design in order to prevent interference from electromagnetic sources in the field.			

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
55	The solution must be configurable by system administrators, with audit logs capturing all configuration changes.			
56	The solution shall be configurable by the user for role-based security level			
57	The solution must be configurable to display or edit fields based on security level.			
58	The solution shall be configurable to limit edit capability to the record creator and security level.			
59	The system should support report export			
60	The solution should be integrated with the CAD solution of Dial 112 and the feed of the camera (recorded & Live) should be made available at Dial 112 Control Room and the CCTV Control Room (SCMRC) residing in the same premises of Police Telecommunication Headquarters.			
61	Selection of the Camera Based on the Location/FRV basis should be made available at the Control Room for assessing the feed of the camera.			
62	The docking station should backup all the video, audio, pictures, log files, and should clear the storage space of BWC automatically when the BWC is connected to the docking station.			

1.45. Vehicle Mounted Camera PTZ with accessories and installation

Sl. No	Features	Compliance (Yes/No)	Deviations (Yes/No)
	Make		
	Model		
1.	Vehicle Mounted PTZ Camera should have colour camera (monochrome in night with IR on).		
2.	Vehicle Mounted PTZ Camera shall have optical Zoom of 30X and Digital zoom of 16X or better		
3.	Vehicle Mounted PTZ Camera shall have PAN Range- 360 degree endless Pan Speed 0.1~90°/s or better Tilt Range +20° ~-90° or better Tilt Speed 0.1~60°/s or better		
4.	Vehicle Mounted PTZ Camera shall have focal length of 4.5-135mm or better		
5.	Vehicle Mounted PTZ Camera shall have minimum 2 megapixels, 1920 x 1080 pixels camera resolution.		
6.	Vehicle Mounted PTZ Camera shall have 1/2.8" or better CMOS progressive scan image sensor.		

Sl. No	Features	Compliance (Yes/No)	Deviations (Yes/No)
7.	Vehicle Mounted PTZ Camera shall support H.265, H.264, MPEG-4 and M-JPEG Video Compression.		
8.	Vehicle Mounted PTZ Camera shall support G.711 or G.726 Audio Compression.		
9.	Vehicle Mounted PTZ Camera Shall Support Multiple streams		
10.	Vehicle Mounted PTZ Camera shall support 1 to 30 fps for different resolution.		
11.	Vehicle Mounted PTZ Camera shall have a minimum illumination of Color:0.005Lux@F1.6 and 0 Lux:0.0005Lux@F1.6		
12.	Vehicle Mounted PTZ Camera shall have shutter time of 1-1/100000 sec.		
13.	Vehicle Mounted PTZ Camera shall have built-in infrared LEDs with range of minimum 80m or more, Auto Day/Night.		
14.	Vehicle Mounted PTZ Camera shall have ruggedness of: a) Rugged, vibration, shock and tamper proof metal housing, and b) Anti-vibration installation with multipoint locking mechanism in horizontal and vertical direction.		
15.	The IP camera shall support Image enhancement of auto-tracking white balance (ATW), automatic gain control, wide dynamic range (WDR) and Automatic backlight compensation (BLC).		
16.	Vehicle Mounted PTZ Camera shall receive power from mNVR through power-over-Ethernet.		
17.	Vehicle Mounted PTZ Camera shall support automatic motion detection, Camera Tamper alerts		
18.	Vehicle Mounted PTZ Camera shall support RJ45 10/100 M ethernet interface.		
19.	Vehicle Mounted PTZ Camera support ONVIF Profile S & G compliant.		
20.	Vehicle Mounted PTZ Camera shall comply to IP66 rating		
21.	Vehicle Mounted PTZ Camera shall support below mention protocols: · HTTP; TCP; UDP; NTP		
22.	Vehicle Mounted PTZ Camera shall support below mention streaming methods: · Unicast, Multicast		
23.	Certification: BIS Certified		
24	Vehicle Mounted PTZ Camera shall be supplied with SS mounting for installation of cameras on Vehicles with all accessories		

1.46. MNVR with 1 TB

Sl. No	Features and minimum specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Make		
	Model		
1.	The mNVR shall have one video output.		
2.	The MNVR shall have two channel video inputs.		
3.	The mNVR shall have one audio output.		
4.	The mNVR shall support H.265 and H.264 video compression standards.		
5.	The mNVR shall support G.711 or G.726 audio compression standards.		
6.	The mNVR shall support dual streams, both streams independently con-figurable for each camera resolution and frame rate.		
7.	The mNVR shall support 1080p/ 720p/ 4CIF/ 2CIF/ CIF/ QCIF (can be set independently for each channel, for both streams) recording resolutions.		
8.	The mNVR shall support 1 to 30 fps for all channels at 1080p resolution and frame rate can be set independently for each camera, for both streams or vehicle having four CCTV cameras.		
9.	The mNVR shall have a minimum of two input (NO/NC) and one output alarm sensors.		
10.	The mNVR shall have storage of 1 TB, solid state drive (SSD) with suitable anti-vibration mechanism storage to be pluggable and easily removable, secure and protected by lock for vehicles		
11.	The mNVR will record in normal, schedule based, alarm triggered, motion detection mode. Alarms triggered modes may include alarms triggered via digital I/O input, For example, emergency button, emergency door Open, brake on, reversing, mNVR enclosure open.		
12.	The mNVR will support event based recording and tagging: a) Pre-recording – 1 to 30 min, and b) Post-recording – 1 to 30 min.		
13.	The mNVR shall support configurable shut down delay after ignition off – up to 24 h (Configurable in hours and minutes)		

Sl. No	Features and minimum specifications	Compliance (Yes/No)	Deviations (Yes/No)
14.	The mNVR shall have facility of integrated PoE switch supporting peak power requirement for CCTV cameras with infrared on and integrated PoE switch supporting peak power requirement for all CCTV cameras within Bus with infrared on.		
15.	The mNVR shall have network/communication interfaces as: a) LAN – 1 RJ45 interface (in addition to the camera ports), and b) Wi-Fi – 802.11/b/g/n (optional). c) Built-in 4G/LTE module, supporting both 2G, 3G and 4G/LTE (at least 900, 1800 and 2100 MHz frequency bands), Support for SMS, voice, data (GPRS, TCP/IP) with multiple network OTA switching capabilities.		
16.	Support embedded SIM/UICC (As per GSMA guidelines / DoT (TEC) guidelines) to cater to the automotive operational requirement such as vibration, temperature and humidity and provide long life span with at least 10 years life and more than 1 million read/write cycles.		
17.	Device shall have built-in/integrated 3 axis accelerometers and 3 axis gyroscopes for accessing driving conditions such as rapid acceleration, sudden braking and hard turn.		
18.	System shall have provision of secured data transmission to the backend from the devices through secured channel. Secured channel means en- crypted data transmission from device to backend using a secured tunnel on communication medium such as 'Secured dedicated APN or 2G/3G/4G/LTE network'		
19.	It will provide the following additional information: a) GPS data via RS 232/Ethernet to other on–bus devices, and b) Receive route number information from other on-board devices and transmit to back end. It will support transmission mode.		
20.	Always –On, turned 'On' by: a) Emergency button, or b) SMS or telephone or alerts from I/O.		
21.	The mNVR shall have ONVIF profile S compliant.		
22.	The mNVR shall support the external interfaces 1 RS232, 1 USB 2.0.		

Sl. No	Features and minimum specifications	Compliance (Yes/No)	Deviations (Yes/No)
23.	The mNVR have external GSM & GPS antenna.		
24.	The mNVR shall have minimum five configurable image settings (one to be the best quality).		
25.	The mNVR shall have tamper-proof watermark.		
26.	The mNVR video over-written to be configurable to support: A) Cyclic overwriting (oldest recording to be overwritten). b) Event tagged recording not to be overwritten for a longer period (configurable).		
27.	The mNVR shall have all input and output connections to be vibration/shock resistant and locking as per BIS (IS 16833) shock and vibration test.		
28.	The mNVR shall have LED indicators for power, recording, network.		
29.	The mNVR shall be capable of communicating system health parameters over 2G/3G/SMS along with: a) Capable of sending health parameters (cameras not-functioning, cameras tamper, storage error, storage full, video loss, camera cover) at specified frequency to the server b) Capable of sending images, video and snapshot (of configurable resolution, (1080p, 720p, 4CIF, CIF, 2CIF, QCIF) from each cam- era to the server at specified frequency (configurable). c) c) Capable of detecting failure, error or tamper of cameras or any component and sending alert to server.		
30.	The system shall support over the air configuration parameters for mNVR and cameras and over the air upgrade of firmware.		
31.	The system shall support independently configuration of motion detection zones for each camera.		
32.	The mNVR should provide video and audio download facility for the desired date/time and duration. It should be possible to connect a laptop to mNVR through network cable on RJ45 port and open mNVR' s user inter- face in a standard browser using a standard URL such as http://dvr with		

Sl. No	Features and minimum specifications	Compliance (Yes/No)	Deviations (Yes/No)
	no/minimum configuration requirement of the laptop's network settings.		
33.	After entering user-id and password, it will be possible to search, view, select and download video clips of desired duration and date/time in standard formats such as (.avi) or (.mpg). It will not be possible to delete any video or change configuration settings using this set of user-id and password.		
34.	The system shall be capable of: a) The mNVR will automatically send the video from cameras to the backend server over 4G/LTE at configurable frame rate and configurable resolution. b) In case the vehicle moves to an area where 4G coverage is not present, the mNVR will automatically shift to 3G/EDGE/GPRS (2G) connectivity to send the system health status data. Also, in such case, the mNVR will automatically shift to a lower frame rate and resolution (both configurable/self-adaptive) and send the video from cameras to the backend server over 3G/ EDGE/GPRS (2G).		
35.	The mNVR shall be powered from the battery of the vehicles. The mNVR should be capable of working on a wide range of voltage (say 8 to 32 V), in order to account for the fluctuations of the vehicle battery voltage. Also, it should be possible to have a delayed shut-down after ignition off, so that cameras can keep on recording for a specified period (say 1 h) After ignition switch-off.		
36.	USB 2.0 interface or better		
37.	Support (802.11 b/g/n) 2.4 GHz LAN-minimum 10m range		
38.	Support easy configuration		
39.	Support external SD card for backup		
40.	Support data export from mNVR		

1.47. PTZ Control unit with keyboard

Sl. No	Features and minimum specifications	Compliance (Yes/No)	Deviations (Yes/No)

	Make		
	Model		
1	Keyboard & Joysticks Keyboard shall have full function used for system control of cameras, camera functions including pan, tilt and zoom lens controls and It shall be ergonomically designed. Joystick shall be provided for achieving all control functions.		
2	Shall be powered via USB through MnVR		

1.48. GPS Device

Sl. No	Features and minimum specifications		Compliance (Yes/No)	Deviations (Yes/No)
	Make:			
	Model:			
1	GSM 850/900/1800/1900 Quad band			
2	High sensitive GPS chip			
3	High integration density of waterproof design, IP67 compliant			
4	Built-in high sensitive GPS antenna, extra strong receptivity			
5	The only one global vehicle device built in double antenna (GSM+GPS)			
6	Built-in ON/OFF power, wide voltage input range 6 - 33 V			
a)	2 - Digital Input			
b)	2 - Digital Output			
c)	1 - Analog Input			
7	Tampering/Theft Alert: Built-in vibration sensor, perform vehicle intelligent robbery protection			
8	ACC (Ignition on/off) detection, to upload status of vehicle operation			
9	Be able to external connect cut off relay (*Immobilizer) to perform gas and electricity Tele control.			
10	Be able to external connect *SOS alarm button for emergency call			
11	Built-in backup battery to perform alarm when wire is cut illegally			
a)	400 mAH Battery Backup			
12	ARAI Certified			

1.49. UPS 1 kVA

Sl. No	Features and	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Make:			
	Model:			
	Output power Capacity	1KVA/800W		
	Topology	True Online Double Conversion UPS		
	INPUT			
	Phase	Single Phase		
	Voltage	230VAC		
	Voltage Range	160-280VAC @100% Load & shall support up-to 110Vac for 50% load		
	Frequency range	47 ~53 Hz		
	Power Factor	≥0.99		
	BATTERY	36VDC		
	Battery Charging	Constant Current & Constant Voltage		
	Cold Start	Required		
	Backup time	4 Hrs		
	VAH Required	4600VAH (Minimum 4320VAH)		
	OUTPUT			
	Nominal Output Voltage	200/208/220/230/240V AC ± 1%		
	Frequency	50Hz ± 0.1Hz		
	Frequency Synchronisation	46 ~ 54 Hz		
	Voltage THD	≤ 3% THD (Linear Load) ≤ 6% THD (Non-Linear Load)		
	Crest Factor	3:1		
	Transfer time	Zero ms		
	Waveform	Pure sinewave		
	EFFICIENCY			
	AC / AC (Overall efficiency)	88%		
	Eco Mode	97%		
	OVERLOAD CAPACITY			
	105 - 110%	10 min		
	110% - 130%	1 min		
	COMMUNICATION			
	RS232	Available		
	USB Com Port	Available		
	Intelligent Slot	SNMP Required		

Sl. No	Features and	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Remote monitoring and record of backup	Through SNMP		
	ENVIRONMENT			
	Operating Temperature	0 ~ 40° C Continuous		
	Humidity	20 - 95% RH @ 0-40° C (Non - condensing)		
	Noise Level	Less than 58dBA @ 1 meter		
	LCD DISPLAY	Load Level, Battery Level, AC Mode, Battery mode, Bypass mode and Fault indicators		
	ALARM			
	Battery Mode	Required		
	Low Battery	Required		
	Over load	Required		
	Fault	Required		
	STANDARDS			
	Ingress Protection	IP20		
	Safety	EN 62040 - 1		
	EMI / EMC	EN 62040 - 2		
	Performance	IEC 62040 - 3		
	Certification	Compliance - CE/ROHS Certifications: BIS, ISO 9001, 14001, 45001, AND Govt Lab Test Report for the quoted model the date of tender opening date		
	PROTECTIONS			
	Input Over Voltage	Required		
	Input Under Voltage	Required		
	Over voltage cut off	Required		
	Short circuit /Over current protection	Required		
	Low Battery	Required		

1.50. UPS 2 kVA

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Make:			
	Model:			
1.	Output power Capacity	2KVA		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
2.	Topology	True Online Double Conversion UPS		
	INPUT			
3.	Phase	Single Phase		
4.	Voltage	230VAC		
5.	Voltage Range	160-280VAC @100% Load & shall support up-to 110Vac for 50% load		
6.	Frequency range	47 ~53 Hz		
7.	Power Factor	≥0.99		
8.	Auto Phase Sequence Correction			
	BATTERY	72/ 96VDC		
9.	Battery Charging	Constant Current & Constant Voltage . The charger capacity shall be minimum 10% of the Battery Bank capacity.		
10.	Cold Start	Required		
11.	Backup time	4 Hrs on 2KVA/1600KW Load		
12.	VAH Required	9600VAH (Minimum 8640 VAH)		
	OUTPUT			
13.	Nominal Output Voltage	200/208/220/230/240V AC ± 1%		
14.	Frequency	50Hz ± 0.1Hz		
15.	Frequency Synchronisation	47 ~ 53 Hz		
16.	Voltage THD	≤ 3% THD (Linear Load) ≤ 6% THD (Non-Linear Load)		
17.	Crest Factor	3:1		
18.	Transfer time	Zero ms		
19.	Waveform	Pure sinewave		
	EFFICIENCY			
20.	AC / AC (Overall efficiency)	90%		
	Eco Mode	97%		
21.	OVERLOAD CAPACITY			
22.	105 - 110%	10 min		
23.	110% - 130%	1 min		
	COMMUNICATION			
24.	RS232	Available		
25.	USB Com Port	Available		
26.	Intelligent Slot	SNMP must		

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
27.	Remote monitoring and record of backup	Through SNMP		
	ENVIRONMENT			
28.	Operating Temperature	0 ~ 40° C Continuous		
29.	Humidity	20 - 95% RH @ 0-40° C (Non - condensing)		
30.	**Noise Level**	Less than 58dBA @ 1 meter		
31.	**LCD DISPLAY**	Load Level, Battery Level, AC Mode, Battery mode, Bypass mode and Fault indicators		
	ALARM			
32.	Battery Mode	Required		
33.	Low Battery	Required		
34.	Over load	Required		
35.	Fault	Required		
	STANDARDS			
36.	Ingress Protection	IP20		
37.	Safety	EN 62040 - 1		
38.	EMI / EMC	EN 62040 - 2		
39.	Performance	IEC 62040 - 3		
40.	Certification	Compliance - CE/ROHS Certifications: BIS, ISO 9001, 14001, 45001,AND Govt Lab Test Report for the quoted model		
	PROTECTIONS			
41.	Input Over Voltage	Required		
42.	Input Under Voltage	Required		
43.	Over voltage cut off	Required		
44.	Short circuit /Over current protection	Required		
45.	Low Battery	Required		

1.51. UPS 20 KVA battery bank

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Make:			
	Model:			
1	Battery Capacity (At 20H Rate)	75 AH		
2	Battery Voltage	12V		
3	Battery Type	Sealed Maintenance Free (SMF) Lead acid battery		
4	Material of container	PPCP (Poly-Propylene)		
5	Number of Cells per battery	6 Cells for 12 V battery		
6	Method of connections between cells	Bolted		
7	AH Efficiency	>90%		
8	WH Efficiency	>80%		
9	Internal Resistance	6 mΩ Max @ full charge 27°C		
10	Short Circuit Current	1767 Amps		
11	Operating Temperature Range	0 to 45 Degree C		
12	Self-Discharge/Month @ 27deg C	<3% of Rated Capacity		
13	Material of container	PPCP (FR Grade Optional)		
14	Type of +ve & -ve plate	Flat Pasted		
15	Recommended Terminal Torque	4.9 N-m		
16	Certification	ISO 9001 , 14001 , 18001		
17	Test Report	Valid CPRI Test certificate must be provided		
18	Make in India	Item shall be manufactured in India		
19	Compatibility	Battery terminal shall be compatible to existing inter-cell connectors		

1.52. UPS Battery bank for 200 kVA

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
	Make			
	Model			

Sl. No	Features	Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)
1	Battery Capacity (At 20H Rate)	75 AH		
2	Battery Voltage	12V		
3	Battery Type	Sealed Maintenance Free (SMF) Lead acid battery		
4	Material of container	PPCP (Poly-Propylene)		
5	Number of Cells per battery	6 Cells for 12 V battery		
6	Method of connections between cells	Bolted		
7	AH Efficiency	>90%		
8	WH Efficiency	>80%		
9	Internal Resistance	6 mΩ Max @ full charge 27°C		
10	Short Circuit Current	1767 Amps		
11	Operating Temperature Range	0 to 45 Degree C		
12	Self-Discharge/Month @ 27deg C	<3% of Rated Capacity		
13	Material of container	PPCP (FR Grade Optional)		
14	Type of +ve & -ve plate	Flat Pasted		
15	Recommended Terminal Torque	4.9 N-m		
16	Certification	ISO 9001 , 14001 , 18001		
17	Test Report	Valid CPRI Test certificate must be provided		
18	Make in India	Item shall be manufactured in India		
19	Compatibility	Battery terminal shall be compatible to existing inter-cell connectors		

1.53. Auto-phase sequence corrector in OMC's

Sl. No	Features and Minimum Specifications	Compliance (Yes/No)	Deviations (Yes/No)

	Make		
	Model		
1	General 80 KVA 3 Phase industrial auto phase sequence corrector		

1.54. Voltage Control Stabilization at OMC

Sl. No	Features	Minimum Specifications		Compliance (Yes/No)	Deviations (Yes/No)
	Make				
	Model				
1		Type	Three Phase		
		Reference Standard	MI		
		Capacity	60 KVA		
		Type of Cooling	OIL Cooled		
		Degree of Protection	IP:20		
2	Rating	Input Voltage Range	300-480 V		
		Output Voltage	415 V ± 1%		
		Rated Supply Frequency	50Hz		
		Reference Ambient	45˚C		
3	Temperature Rise	Temperature Rise Above Ambient	<55˚C		
4	Losses	No Load Losses	<300W		
		Full load under short circuit	<1000W		
		Total losses	1200W		
5	Efficiency	Maximum Efficiency	≥98%(atnominalInputVoltageorsameinoutput voltage)		
6	Regulation	At 0.8 Power Factor	± 1%		
		At Unity Power Factor	± 1%		

Sl. No	Features	Minimum Specifications		Compliance (Yes/No)	Deviations (Yes/No)
7	Metering	VF Meter Input / Output Voltage Frequency	Digital Voltmeter to read the input and output voltage for per phase & Frequency with selectable menu key.		
		Ammeter Output Current	Digital Ammeter to read the output Current for per phase with selectable menu key.		
8	Indications		Lamp Indications: Input On Output On Output Low/High Overload		
9	Protection for input and output control (Optional)	Overload Current Under Voltage / Over Voltage Cut Off Manual Bypass	i) MCCB by 125A – 1Nos at Input side ii) Contactor (Tripping) by 90A – 1No at output side iii) Bypass by 125A – 1No at output side		
11	Fabricated and Painted Enclosure	Powder Coating	Provided		