MINISTRY OF HOME AFFAIRS

(Center State Division, Govt. Of India)

Tender No.: 15011/38/2013-SC/ST-W 26 June 2015

Request for Proposal

for

"Selection of IT Service Provider for Nationwide Emergency Response System"

Section 1
Invitation to Bid

Issued by:

Ministry Of Home Affairs – CS Division, 5th Floor, NDCC-II Building, Jai Singh Road,
New Delhi -110001, India

1. This invitation is to interested eligible bidders for "**Selection of IT Service Provider for Nationwide Emergency Response System".**

2. Bidder(s) refer to the sole bidder who wants to bid for this tender as per the terms and conditions of this RFP.

3. Bidders are advised to study the RFP document carefully. Submission of bid response to this RFP shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications. Bid response prepared in accordance with the procedures enumerated in **Section 2 of this RFP** should be submitted to the Purchaser not later than the date and time laid down in this section of the RFP.

4. Bidders can download the RFP document from eProcurement portal **www.eprocure.gov.in** or MHA website **www.mha.nic.in.** The tender fee in the form of demand draft of Rs 25,000 (Rupees Twenty Five Thousand only) in favor "DDO, Ministry of Home Affairs" payable at New Delhi should be submitted along with the bid response. Tender fee is non-refundable.

5. All bids must be accompanied by Earnest Money Deposit (EMD) of Rs. 10,00,00,000 (Rupees Ten Crore only) in the form of Bank Guarantee. The EMD should be issued from a nationalized/ scheduled bank. The Bank Guarantee shall be valid for the same period as the bid validity mentioned in this section. The Bank Guarantee should be prepared as per the format specified in Section 4 of this RFP.

6. This RFP document is not transferable.

7. Critical information

7.1 Contact Details

Name of the Purchaser	Ministry of Home Affairs
Name of the RFP	Selection of IT Service Provider for Nationwide Emergency Response System
Contact person	Director (SR) Ministry of Home Affairs, Government of India, New Delhi
Contact Address	5th Floor, NDCC-II Building, Jai Singh Road New Delhi – 110001
Contact Number	011-23438133
Contact e-mail ID	nirbhaya-mha@gov.in
Venue of Pre-Bid Meeting, Submission of EMD, Opening of Technical Bid	Conference Room, Ist floor, NDCC-II building, Jai Singh Road, New Delhi – 110001

7.2 Date-sheet

1.	Publication of RFP on eProcurement Portal	26 June 2015
2.	Date and time of pre-bid meeting	1 July 2015 at 11:00 AM
3.	Last date and time to submit pre-bid queries on eProcurement Portal or e-mail ID (nirbhaya-mha@gov.in)	6 July 2015 at 5:00 PM
4.	Date of issue of query responses / Corrigendum (if required)	13 July 2015
5.	Last date and time of submission of EMD and tender fees in a sealed box at contact address of the Purchaser	12 August 2015 at 3:00 PM
6.	Last date and time for submission of online Bid	12 August 2015 at 3:00 PM
7.	Date and time of opening of Technical Bid	12 August 2015 at 3:30 PM
8.	Date of Technical Presentation	Would be communicated later
9.	Date of Financial Bid opening	Would be communicated later
10.	Bid validity	120 days from date of submission of RFP response

8. Bidders must note that **bids, including both online bid submission and hardcopy submission of EMD and tender fees, received after due date and time shall be rejected.** Purchaser would not be responsible for any delay in submission of bids.

9. The Scope of Work, tender procedures and Contract terms are prescribed in this RFP Document. In addition to Section 1, the RFP Document includes:

SECTION	CONTENTS
Section 2	Instruction to Bidders
Section 3	Contract Conditions and Service Levels
Section 4	Bid Submission Formats
Section 5	Scope of Work
Annexure to Section 5	A: Software Requirement Specifications B: Technical Requirement Specifications

10. The Bidder should examine all instructions, forms, terms & conditions, and scope of work in the RFP Document and furnish all information as stipulated therein.

MINISTRY OF HOME AFFAIRS

(Center State Division, Govt. Of India)

Tender No.: 15011/38/2013-SC/ST-W **26 June 2015**

Request for Proposal

for

"Selection of IT Service Provider for Nationwide Emergency Response System"

Section 2
Instruction to Bidders

Issued by:

Ministry Of Home Affairs – CS Division, 5th Floor, NDCC-II Building, Jai Singh Road,
New Delhi -110001, India

Table of Contents

1. Procedure for Submission of Bids

1.1. The last date and time of submission of bids shall be as per Clause 7 of Section 1 of the RFP.

1.2. The bidders are required to submit soft copies of their bids electronically on the Central Public Procurement (CPP) Portal, using valid Digital Signature Certificates. The instructions given below are meant to assist the bidders in registering on the CPP Portal, prepare their bids in accordance with the requirements and submitting their bids online on the CPP Portal.

1.2.1. Registration

1.2.1.1. Bidders are required to enroll on the e-Procurement module of the Central Public Procurement Portal (URL: https://eprocure.gov.in/eprocure/app) by clicking on the link "Online Bidder Enrollment". Enrollment on the CPP Portal is free of charge.

1.2.1.2. As part of the enrolment process, the bidders will be required to choose a unique username and assign a password for their accounts.

1.2.1.3. Bidders are advised to register their valid email address and mobile numbers as part of the registration process. These would be used for any communication from the CPP Portal.

1.2.1.4. Upon enrolment, the bidders will be required to register their valid Digital Signature Certificate (Class II or Class III Certificates with signing key usage) issued by any Certifying Authority recognized by CCA India (e.g. Sify / TCS / nCode / eMudhra etc.), with their profile.

1.2.1.5. Only one valid DSC should be registered by a bidder. Please note that the bidders are responsible to ensure that they do not lend their DSC's to others which may lead to misuse.

1.2.1.6. Bidder then logs in to the site through the secured log-in by entering their user ID / password and the password of the DSC / e-Token.

1.2.2. Preparation of Bids

1.2.2.1. Bidder should take into account any corrigendum published on the tender document before submitting their bids.

1.2.2.2. Please go through the tender document carefully to understand the documents required to be submitted as part of the bid. Please note the number of covers in which the bid documents have to be submitted, the number of documents - including the names and content of each of the document that need to be submitted.

1.2.2.3. Bidder, in advance, should get the bid documents ready to be submitted as indicated in the tender document / schedule and generally, they can be in PDF / XLS / RAR / DWF formats. Bid documents may be scanned with 100 dpi with black and white/ color option.

1.2.3. Submission of bids

1.2.3.1. Bidder should log into the site well in advance for bid submission so that he/she upload the bid in time i.e. on or before the bid submission time. Bidder will be responsible for any delay due to other issues.

1.2.3.2. The bidder has to digitally sign and upload the required bid documents one by one as indicated in the tender document.

1.2.3.3. Bidder has to select the payment option as “offline” to pay the tender fee / EMD as applicable and enter details of the instrument.

1.2.3.4. Bidder should prepare the EMD as per the instructions specified in the tender document. The original should be delivered to Purchaser, latest by the last date and time of bid submission as provided in Section 1 of RFP. The details of the DD/any other accepted instrument, physically sent, should tally with the details available in the scanned copy and the data entered during bid submission time. Otherwise the uploaded bid will be rejected.

1.2.3.5. The server time (which is displayed on the bidders’ dashboard) will be considered as the standard time for referencing the deadlines for submission of the bids by the bidders, opening of bids etc. The bidders should follow this time during bid submission.

1.2.3.6. The uploaded tender documents become readable only after the tender opening by the authorized bid openers.

1.2.3.7. Upon the successful and timely submission of bids, the portal will give a successful bid submission message & a bid summary will be displayed with the bid no. and the date & time of submission of the bid with all other relevant details.

1.2.3.8. The bid summary has to be printed and kept as an acknowledgement of the submission of the bid. This acknowledgement may be used as an entry pass for any bid opening meetings.

1.2.4. Assistance to Bidders

1.2.4.1. Any queries relating to the tender document and the terms and conditions contained therein should be addressed to the Tender Inviting Authority for a tender or the relevant contact person indicated in the tender.

1.2.4.2. Any queries relating to the process of online bid submission or queries relating to CPP Portal in general may be directed to the 24x7 CPP Portal Helpdesk. The contact number for the helpdesk is 1800 233 7315.

1.3. Online bid should be submitted on http://eprocure.gov.in/eprocure/app following the details mentioned below:

1.3.1. **Cover-01:**

1.3.1.1. Scanned copy of Bank Guarantee towards EMD and bank draft towards Tender Fees should be uploaded (PDF format) electronically on http://eprocure.gov.in/eprocure/app. Also, original EMD bank guarantee and original Tender fees bank draft shall be submitted physically at MHA office (address as per Secion1, clause 7) in a sealed envelope in a single sealed envelope clearly marked **“Selection of IT Service Provider for setting up of Nationwide Emergency Response System”**. This envelope is to be super-scribed with RFP Number and Due Date.

1.3.1.2. All documents in Cover – 01 shall be uploaded as below:

Cover No.	Cover type	Description	Document type	Content
Cover 1	Fee/ Technical Bid	Scanned copy of Tender Fee	.pdf	Scanned copy of Tender Fee
		Scanned copy of	.pdf	Scanned copy of EMD

Cover No.	Cover type	Description	Document type	Content
		EMD		
		Technical bid containing all relevant details	.pdf	Technical bid as per bid submission formats
		Blank Financial Bid Template	.pdf	Breakdown of cost components mentioning ONLY bill of material. It should NOT mention cost of any item
		Supporting documents (this may be uploaded along with Technical Bid)	.pdf	All relevant details and documentary proofs including Power of Attorney executed by the Bidder

Cover 02: Cover-2 would consist of the following documents:

Cover No.	Cover type	Description	Document type	Content
Cover 2	Financial Bid	Financial bid letter	.pdf	Signed copy of Financial bid letter
		Price schedule	.pdf	Price break-up as per formats

1.3.3. The bids received after the due date and time (electronically or physical cover of EMD and Tender Fees) shall be summarily rejected and returned to the Bidder declaring as “Late submission” and the same shall not be opened.

2. Cost of Bidding Process

2.1. The Bidder shall bear all costs associated with the preparation and submission of its bid, including cost of presentations etc. for the purposes of clarification of the bid.

3. Clarification on RFP Document

3.1. A prospective Bidder requiring any clarification on the RFP Document may upload queries on the eProcurement portal as per schedule indicated in Clause 7 of Section 1. The queries must be submitted in the following editable format:

BIDDER’S REQUEST FOR CLARIFICATION		
Name and Address of the Organization submitting request	Name and Position of Person submitting request	Contact Details of the Organization / Authorized Representative
		Tel:

BIDDER’S REQUEST FOR CLARIFICATION					
				Fax:	
				Email:	
S. No	RFP Section	RFP Page	RFP Clause	Content of RFP requiring clarification	Points of clarification required
1.					
2.					

3.2. The Purchaser will respond, to any request for clarification to queries on the RFP Document, received not later than the date prescribed by the Purchaser in Section 1 of this RFP document.

4. Amendment of RFP Document

4.1. At any time prior to the last date for receipt of bids, the Purchaser, may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the RFP Document by an amendment. It shall not be mandatory for the Purchaser to disclose the reasons for this change.

4.2. The amendment will be notified on http://eprocure.gov.in/eprocure/app and should be taken into consideration by prospective bidders while preparing their responses. The amendments would be binding on all Bidders.

4.3. The Purchaser may, at its discretion, extend the last date for the receipt of Bids.

5. Language of Bids

5.1. The Bids prepared by the Bidder and all correspondence and documents relating to the bids exchanged by the Bidder and the Purchaser, shall be written in English language, provided that any printed literature furnished by the Bidder may be written in another language so long the same is accompanied by an English translation in which case, for purposes of interpretation of the bid, the English translation shall govern.

6. Bid Prices

6.1. The Bidder shall indicate in the pro-forma prescribed in Section 4 of this RFP, the unit rates of the services, it proposes to provide under the Contract. Prices should be shown separately for each item as detailed in Bid Documents.

6.2. In absence of information as requested in Clause 6.1 above, a bid shall be considered incomplete and summarily rejected.

6.3. 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.

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

7. Firm Prices

7.1. 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. The Bidder shall, therefore, indicate the prices in Clause 2.2 of Section 4 of this RFP enclosed with the Bid. The Bid Prices shall be indicated in Indian Rupees (INR) only.

7.2. 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. No separate taxes should be provided.

7.3. A proposal submitted with an adjustable price quotation or conditional proposal shall be treated as non-responsive and the bid may be rejected.

7.4. Net Present Value would be used to calculate the financial prices as provided in clause 21 of this section of RFP.

8. Discount

8.1. 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.

9. Bidder Qualification

9.1. The “Bidder” as used in the RFP documents shall mean the organization on whose behalf the RFP response has been submitted. The Bidder may be either the Principal Officer (MD/ Company Secretary) or his/her duly Authorized Representative, in which case he/she shall submit a power of attorney.

9.2. It is further clarified that the individual signing the RFP or other documents in connection with the RFP must certify whether he/she signs as :

9.2.1. Constituted attorney of the firm, if it is a company

OR

9.2.2. The principal officer or his/her duly assigned authorized representative of the bidder, in which case he/she shall submit a certificate of authority on behalf of the bidder.

9.3. The authorization shall be indicated by power-of-attorney accompanying the bid.

10. Earnest Money Deposit (EMD)

10.1. The Bidder shall furnish, as part of its bid, EMD of the amount and format as mentioned in Clause 5 of Section 1 of this RFP.

10.2. The EMD is required to protect the Purchaser against the risk of Bidder’s conduct which would warrant the EMD's forfeiture, pursuant to Clause 10.6.

10.3. The EMD (denominated in Indian Rupees) shall be in the form of a bank guarantee issued by a Nationalized / Scheduled Bank, in the proforma provided in Section 4 of this RFP and shall have validity as stated in Section 1 of this RFP.

10.4. Unsuccessful Bidder’s EMD will be discharged/ returned after award of contract to the successful Bidder. No interest will be paid by the Purchaser on the EMD amount.

10.5. The successful Bidder's EMD shall be discharged upon the Bidder executing the Contract, pursuant to Clause 26 and after furnishing the performance security, pursuant to Clause 25.

10.6. The EMD may be forfeited:

10.6.1. if a Bidder withdraws its bid during the period of bid validity specified by the Bidder in the Bid; or

10.6.2. in the case of a successful bid, if the Bidder fails;

i. to furnish performance security in accordance with Clause 25

ii. to sign the Contract in accordance with Clause 26

11. Period of Validity of Bids

11.1. Bids shall remain valid for period as stated in Section 1 of this RFP. A bid valid for a shorter period shall be rejected by the Purchaser as non-responsive and shall not be taken up for evaluation purposes.

11.2. The Purchaser may request the Bidder(s) for an extension of the period of validity. The request and the responses thereto shall be made in writing (or by fax or by e-mail).

12. Terms and Conditions of Bidder

12.1. Printed terms and conditions (General Conditions) of the Bidder will not be considered as forming part of their Bids. In case terms and conditions of the contract applicable to this Invitation of RFP are not acceptable to any Bidder, he should clearly specify deviation in his Technical Bid, Clause 1.6 of Section 4 of this RFP. Similarly in case the Services being offered have deviations from the requirements/specifications laid down in this RFP, the Bidder shall describe in what respects and to what extent the Services being offered differ/deviate from the requirements, even though the deviations may not be very material. The Bidder must state categorically whether or not his offer conforms to RFP requirements / specifications and indicate deviations, if any, in his Technical Bid (Clause 1.6 of Section 4 of this RFP)

12.2. Any deviations / assumptions mentioned elsewhere in the Bid, other than the formats (Clause 1.6 of Section 4 of this RFP) will not be considered by the Purchaser.

12.3. All deviations should be closed before the financial opening by mutual discussion between Purchaser and Bidder. Financial bid would be opened only after closure of all deviations by the technically successful bidders.

13. Local Conditions

13.1. It will be incumbent upon each Bidder to fully acquaint himself with the local conditions and factors at the respective locations, sites and offices which would have any effect on the performance of the contract and / or the cost.

13.2. The Bidder is expected to obtain for himself on his own responsibility all information that may be necessary for preparing the bid and entering into contract. Obtaining such information shall be at Bidder's own cost.

13.3. Failure to obtain the information necessary for preparing the bid and/or failure to perform activities that may be necessary for project will in no way relieve the successful Bidder from performing any work in accordance with the contract entered into.

13.4. It will be imperative for each Bidder to fully inform themselves of all local and legal conditions and factors which may have any effect on the execution of the contract as described in the RFP documents.

13.5. It is the responsibility of the Bidder that such factors have properly been investigated and considered while submitting the bid proposals and that no claim whatsoever including those for financial adjustment to the contract awarded under the bidding documents will be entertained by the Purchaser and that neither any change in the time schedule of the contract nor any financial adjustments arising thereof shall be permitted by the Purchaser on account of failure of the Bidder to appraise themselves of local laws and conditions.

14. Last Date for Receipt of Bids

14.1. Bids will be received by the Purchaser at the address specified under Clause 7 of Section 1. In the event of the specified date for the receipt of Bids being declared a holiday for the Purchaser, the Bids will be received up-to the appointed time on the next working day.

14.2. The Purchaser may, at its discretion, extend the last date for the receipt of bids, in which case all rights and obligations of the Purchaser and Bidder previously subject to the last date will thereafter be subject to the last date as extended.

15. Late Bids

15.1. Any bid received by the Purchaser after the last date and time for receipt of bids prescribed by the Purchaser, pursuant to Clause 7 of Section 1, will be rejected and shall not be considered for opening and/or returned unopened to the Bidder.

16. Modification and Withdrawal of Bids

16.1. No bid may be altered / modified after submission to the Purchaser. Unsolicited correspondences in this regard from Bidder will not be considered.

16.2. 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.

17. Address for Correspondence

17.1. The Bidder shall designate the official mailing/e-mail address, place and fax number to which all correspondence shall be sent by the Purchaser.

18. Contacting the Purchaser

18.1. No Bidder shall contact the Purchaser on any matter relating to its bid, from the time of the bid opening to the time the Contract is awarded.

18.2. Any effort by a Bidder to influence the Purchaser's bid evaluation, bid comparison or contract award decisions shall result in the rejection of the Bidder's bid.

19. Opening of Technical Bids by Purchaser

19.1. The Purchaser will open the Technical Bid, in the presence of the representatives of the Bidders' members who choose to attend, at the time, date and place, as mentioned in Section 1 of this RFP.

19.2. The Bidder's names, modifications, bid withdrawals and the presence or absence of the requisite EMD and such other details as the Purchaser, at its discretion, may consider appropriate will be announced at the bid opening.

20. Consortium Approach

20.1. Bidder is not allowed to form a consortium for any piece of work. If proposed, the purchaser reserves the right to reject the bid.

21. Evaluation of Bids

21.1. The Bidder must possess the requisite experience, strength and capabilities in providing the services necessary to meet the Purchaser’s requirements, as described in the RFP Documents. The Bidder must possess the technical know-how and the financial wherewithal that would be required to successfully provide the services sought by the Purchaser, for the entire period of the contract. The Bidder’s bid must be complete in all respect and covering the entire scope of work as stipulated in the RFP document.

21.2. Preliminary Examination

21.2.1. The Purchaser will examine the bids to determine whether they are complete, whether the bid format confirms to the RFP requirements, whether required Tender fee and EMD has been furnished, and whether the bids are generally in order.

21.2.2. The Purchaser may waive any informality or nonconformity or irregularity in a bid which does not constitute a material deviation according to the Purchaser

21.3. Clarification

21.3.1. When deemed necessary, during the tendering process, the Purchaser may seek clarifications or ask the Bidder to make Technical presentations on any aspect from any or all the Bidders.

21.4. Evaluation of Technical Bids

21.4.1. Only those Bidders who cross the threshold level of Technical Evaluation indicated below and adhere to the Purchaser’s technical requirements shall be considered for next stage i.e. financial evaluation.

21.4.2. Foreign currency Turnover will be converted into Indian Rupees based on RBI reference rate applicable as on the date of opening of RFP without assigning any weightage factor.

21.4.3. In case of no response by the Bidder to any of the requirements with regard to the contents of the Technical Bid, he shall not be assigned any marks for the same.

21.4.4. Technical bid of the Bidder shall be opened and evaluated for acceptability of Techno-functional requirements, deviations and technical suitability. Bidders shall respond to the requirements as explained below for their evaluation with regard to experience and qualification. Also, Bidder shall refer and respond to ALL technical and functional requirements as mentioned in the RFP document

21.4.5. In order to qualify technically, a proposal must secure a minimum of 70% of total marks after summing up. The Bidder would be technically evaluated out of 1000 marks. Bids receiving 700 marks and above would qualify for financial evaluation.

21.4.6. Technical Evaluation shall be based on the following parameters and associated weightages:

S. No.	Evaluation Criteria	Supporting documents required	Marks	Min. Marks
1	Company Profile		100	70
1.A	Bidder should be a company registered for minimum 3 years in India as on 31 March 2015	Incorporation certificate PAN card VAT registration	40	
1.B	Bidder should have an annual turnover of at least Rs. 1000 Crores in each of the last three(3) financial years (ending 31st March 2014) accruing from System Integration	Copy of audited financial statements or declaration from the appointed statutory auditor	30	
1.C	The Bidder should be at least SEI CMM /CMMi maturity Level 5 certification. Additional certification in ISO 9000 and ISO 27001 would be preferred.	Valid certificates	30	
2	Prior Experience		150	75
2.A	The bidder should have experience of handling minimum 2 assignments of value more than Rs. 100 crore in India or abroad as System Integrator / Technology solution implementing agency in last 5 years. Project should have either been completed or ongoing where deliverable or milestone has been successfully met relevant to the experience.	Documentary evidence (Copy of Client certificate / Purchase order / Contract) The date of work order / contract should be at least 6 months before date of release of this RFP	50	
2.B	The proposed contact centre solution of OEM should have been implemented in minimum 2 projects with more than 2500 seats in India or abroad. Projects with Police/ Homeland security/ Medical services would be given more weightage.	Documentary evidence from OEM (Copy of Client certificate / Purchase order / Contract) The date of work order / contract should be atleast 6 months before date of release of this RFP	50	
2.C	The Bidder should have experience in large scale cloud solution deployment and will provide the cloud hardware specification of the proposed solution	Documentary evidence (Copy of Client certificate / Purchase order / Contract)	50	
3	Solution proposed		350	175
3.A	Compliance to Section 5A	Submission of detailed technical solution as per the prescribed formats	50	
3.B	Overall Proposed Solution		70	
3.C	Software Solutions		50	
3.D	Cloud infrastructure solution		30	
3.E	Network Solution		30	
3.F	Project implementation approach / strategy		30	
3.G	Operations and maintenance plan		45	
3.H	Manpower deployment plan		45	
4	Manpower proposed		250	125

S. No.	Evaluation Criteria	Supporting documents required	Marks	Min. Marks
	Manpower would be evaluated on Qualification, Number of years of work experience, relevant projects, and certifications of the proposed individual.	Any certification as mentioned in the CV may be requested by Purchaser for verification purpose		
4.A	Project Director		20	
4.B	Project Manager		20	
4.C	Operations Center Manager		20	
4.D	Solution Architect (Applications)		20	
4.E	Solution Architect (Network)		30	
4.F	Solution Architect (Information Security)		20	
4.G	Database Architect/ Modeler		20	
4.H	Contact Centre Expert (from OEM of the proposed product)		20	
4.I	GIS Expert (from OEM of the proposed product)		10	
4.J	Contact Centre configuration & customization expert		10	
4.K	QA Manager		10	
4.L	BI, Data warehouse expert		20	
4.M	Master Trainer		10	
4.N	Solution Architect (Cloud expert)		20	
5	Technical Presentation		150	75
5.A	Technical presentation by the Bidder	Technical presentation on the appointed day	150	
	TOTAL		**1000**	**700**

21.5. Opening of Financial Bids

21.5.1. The Purchaser will open the Financial Bids of only Technically Qualified Bidders after all deviation has been resolved and accepted by the bidder, in the presence of the representatives of the Bidder who choose to attend, at the time, date and place, as decided by the Purchaser.

21.5.2. Financial evaluation would be undertaken irrespective of number of Bidders qualifying the Technical evaluation.

21.5.3. The Financial bids shall be evaluated by the Purchaser for completeness and accuracy. 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.

21.5.4. No enquiry shall be made by the bidder(s) during the course of evaluation of the tender, after opening of bid, till final decision is conveyed to the successful bidder(s). However, the Committee/its authorized representative and office of Purchaser can make any enquiry/seek clarification from the bidders, which the bidders must furnish within the stipulated time else bid of such defaulting bidders will be rejected.

21.6. Combined Quality- cum- Cost Based System Selection (CQCCBS) will be followed.

21.6.1. The technically qualified bidders shall be ranked as per score achieved by them, from the highest to the lowest Technical Score (ST).

21.6.2. Each Financial Proposal will be assigned a financial score (SF).The lowest financial proposal (FM) will be given a financial score (SF) of 1000 points in which 700 points for technical evaluation and 300 points for financial evaluation. The financial scores of other proposals will be computed as follows:

SF = 1000 x FM/F, where F = amount of Financial Proposal

21.6.3. Thereafter, Combined and Final evaluation will be done on the following basis:
Proposals will finally be ranked according to their combined score (S) based on their technical (ST) and financial (SF) scores as follows:

S = ST x 0.7 + SF x 0.3

The Selected bidder shall be the first ranked bidder (having the highest combined score).The score contains 700 score for technical evaluation and 300 score for financial evaluation.

22. Post Qualification and Award Criteria

22.1. This determination will take into account the Bidder's financial, technical, implementation and post-implementation strengths and capabilities. It will also include examination of the documentary evidence submitted by the Bidder as part of the bid as well as such other information as the Purchaser deems necessary and appropriate.

22.2. An affirmative determination will be a prerequisite for award of the Contract to the Bidder. A negative determination will result in rejection of the Bidder's bid, in which event; the Purchaser will proceed to the next best evaluated bid to make a similar determination of that Bidder's capabilities to perform satisfactorily.

22.3. The Purchaser is not bound to accept the best evaluated bid or any bid and reserves the right to accept any bid, wholly or in part.

23. Purchaser's Right to Accept Any Bid and to Reject Any or All Bids

23.1. The Purchaser reserves the right to accept any bid, and to annul the tender process and reject all bids at any time prior to award of Contract, without thereby incurring any liability to the affected Bidder (s) or any obligation to inform the affected Bidder (s) of the grounds for the Purchaser's action.

24. Notification of Award

24.1. Prior to the expiration of the period of bid validity, pursuant to Clause 11, the Purchaser will notify the successful Bidder in writing that its bid has been accepted. The Bidder shall provide his acceptance within defined time period of such notification.

24.2. The notification of award will constitute the formation of the Contract.

24.3. Upon the successful Bidder's furnishing of performance bank guarantee pursuant to Clause 25, the Purchaser may notify each unsuccessful Bidder and will discharge their EMD, pursuant to Clause 10 of this section.

25. Performance Bank Guarantee

25.1. Within 15 days of the receipt of notification of award from the Purchaser, the successful Bidder shall furnish the performance security of 10% of total contract value in accordance with the Conditions of Contract, in the Performance Bank Guarantee prescribed at Clause 3.1 of Section 4 of this RFP.

25.2. Failure of the successful Bidder to comply with the requirement of the RFP and signing of contract as per Clause 26.1 shall constitute sufficient grounds for the annulment of the award and forfeiture of the EMD, in which event the Purchaser may award the Contract to the next best evaluated bid or call for new bids.

26. Signing of Contract

26.1. The successful Bidder shall sign the contract within 15 days of the receipt of notification of award.

27. Rejection Criteria

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

27.1. General Rejection Criteria
27.1.1. Bids submitted without or improper EMD
27.1.2. Bids received through Telex / Telegraphic / Fax / e-Mail.
27.1.3. Bids which do not confirm validity of the bid as prescribed in the RFP
27.1.4. If the information provided by the Bidder is found to be incorrect / misleading at any stage / time during the tendering Process
27.1.5. Any effort on the part of a Bidder to influence the Purchaser's bid evaluation, bid comparison or contract award decisions
27.1.6. Bids received by the Purchaser after the last date and time for receipt of bids prescribed by the Purchaser, pursuant to Section 1 of the RFP.

27.2. Technical Rejection Criteria
27.2.1. Technical Bid containing financial details.
27.2.2. Revelation of Prices in any form or by any reason before opening the Financial Bid
27.2.3. Failure to furnish all information required by the RFP Document or submission of a bid not substantially responsive to the RFP Document in every respect.
27.2.4. Bidders not responding to the complete scope of Work as indicated in the RFP documents, addendum (if any) and any subsequent information given to the Bidder.
27.2.5. If the bid does not conform to the timelines indicated in the bid.

27.3. Financial Rejection Criteria
27.3.1. If there is an arithmetic discrepancy in the Financial Bid calculations the Purchaser shall rectify the same. If the Bidder does not accept the correction of the errors, bid may be rejected.

MINISTRY OF HOME AFFAIRS

(Center State Division, Govt. Of India)

Tender No.: 15011/38/2013-SC/ST-W 26 June 2015

Request for Proposal

For

“Selection of IT Service Provider for Nationwide Emergency Response System”

Section 3
Contract Conditions and Service Levels

Issued by:

Ministry Of Home Affairs – CS Division, 5th Floor, NDCC-II Building, Jai Singh Road,
New Delhi -110001, India

Table of Contents

A. GENERAL CONDITIONS OF CONTRACT (GCC)

1. Definition of Terms

1.1. **“Acceptance of System”:** means acceptance of the system by the purchaser as per section 5 of the RFP.

1.2. **“Bidder”** shall mean organization submitting the proposal in response to this RFP. Bidder may also be referred as IT Service Provider (ITSP) in the RFP.

1.3. **“Bidder’s Team”** means the successful Bidder who has to provide goods & services to the Purchaser under the scope of this Contract. This definition shall also include any and/or all of the employees of the Bidder, authorized service providers/ partners/ agents and representatives or other personnel employed or engaged either directly or indirectly by the Bidder for the purposes of this Contract.

1.4. **“Bidder’s Representative/Project Coordinator”** means the person or the persons appointed by the Bidder from time to time to act on its behalf for overall co-ordination, supervision and project management.

1.5. **“Contract”** means this agreement and the Appendices / Annexure attached hereto and made a part hereof and any amendments made thereto.

1.6. **“Contract Value”** means the price payable to the Bidder under this Contract for the full and proper performance of its contractual obligations.

1.7. **“Condition Precedent”** means all such conditions that are a pre requisite for the contract to be entered into and shall collectively mean the MHA conditions precedent, the Bidder conditions precedent and the common conditions precedent.

1.8. **“Data Centre (DC)”** means a Cloud Data Centre that would house the Information and Communication Technology (ICT) infrastructure required for carrying out centralized operations of the Purchaser.

1.9. **"Default"** means:

i. a breach, default or violation,

ii. the occurrence of an event that with or without the passage of time or the giving of notice, or both, would constitute a breach, default or violation or

iii. with respect to any Contract, the occurrence of an event that with or without the passage of time or the giving of notice, or both, would give rise to a right of termination, renegotiation or acceleration or a right to receive damages or a payment of penalties.

1.10. **“Document**” means any embodiment of any text or image however recorded and includes any data, text, images, sound, voice, codes or and databases or microfilm or computer generated micro fiche.

1.11. **“Effective Date”** means the date on which this Contract is signed and executed by the parties hereto.

1.12. **“GCC”** means General Conditions of Contract

1.13. **“Goods”** means all of the equipment, sub-systems, hardware, software, products accessories and/or other material / items which the Bidder is required to design, supply, install, configure, re-configure, assemble, commission, de-commission and maintain under the contract.

1.14. **“Intellectual property”** shall mean all intellectual property related to the Assets of either the Purchaser or the bidder and the project, including without limitation:

i. any and all rights, privileges and priorities arising under the laws or treaties of India, any state, territory, any other country, relating to intellectual property, including patents, copyrights, trade names, trademarks, designs, service marks, mask works, trade secrets, inventions, databases, names and logos, trade dress, technology, know-how, and other proprietary information and licenses from third persons granting the right to use any of the foregoing, including all registrations and applications for any of the foregoing that have been issued by or filed with the appropriate authorities, any common-law rights arising from the use of the foregoing, any rights commonly known as "industrial property rights" or the "moral rights" of authors relating to the foregoing, all rights of renewal, continuations, divisions, extensions and the like regarding the foregoing and all claims, causes of action, or other rights arising out of or relating to any actual or threatened Infringement by any person relating to the foregoing;

ii. all computer applications, programs and other software, including without limitation operating software, network software, firmware, middleware, and design software, all design tools, systems documentation and instructions, databases, and related items and physical infrastructure components

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.

1.16. **“MHA”** means Ministry of Home Affairs, Government of India

1.17. **“Notice”** means:

- an information, announcement, message, notification, warning etc. which is in writing; or
- a consent, approval or other communication required to be in writing under this Contract.

1.18. **“OEM”** means the Original Equipment Manufacturer of any equipment / system / software / product whose goods shall be provided by Bidder to the Purchaser under the scope of this Tender / Contract.

1.19. **“Owner”** shall mean Ministry of Home Affairs (MHA) and shall include its successor and assignees.

1.20. **“Owner’s Representative”** means the person designated by MHA and shall include his authorized nominee or agent; provided, however, that the Owner’s representative may be one person for certain aspects of this agreement and another person for other aspects of work covered by this contract.

1.21. **“Purchaser”** shall mean means the President of India acting through the Director (SR), Ministry of Home Affairs, Government of India.

1.22. **“Purchaser’s Representative/Project Coordinator”** means the person or the persons appointed by the Purchaser from time to time to act on its behalf for overall co-ordination, supervision and project management.

1.23. **“Replacement Service Provider”** means the organization replacing the bidder in case of contract termination for any reasons

1.24. “**Sites**” refer to Operations Centre location, State Call Centre locations and Cloud Data Centre locations

1.25. **“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 the Purchaser and the heirs, legal representatives, successors and assignees of such person.

1.26. **“SCC”** means Special Conditions of Contract

1.27. **“Services”** means the work to be performed by the Bidder pursuant to this RFP and to the contract to be signed by the parties in pursuance of any specific assignment awarded by the Purchaser.

1.28. “**System**” means all of the goods under the scope of this contract together as an integrated solution

2. Interpretation

2.1. In this Contract unless a contrary intention is evident:

a. the clause headings are for convenient reference only and do not form part of this Contract;

b. unless otherwise specified a reference to a clause number is a reference to all of its sub-clauses;

c. 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;

d. 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;

e. a word in the singular includes the plural and a word in the plural includes the singular;

f. a word importing a gender includes any other gender;

g. a reference to a person includes a partnership and a body corporate;

h. a reference to any legislation/ regulation having force of law includes legislation/ regulation time to time repealing, replacing, modifying, supplementing or amending that legislation;

i. 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.

j. in the event of an inconsistency between the terms of this Contract and the Tender and the Bid, the terms hereof shall prevail.

k. Any reference to time shall, except where the context otherwise requires and specifies, be construed as a reference to the time in India. Any reference to the Calendar shall be construed as reference to the Gregorian calendar.

l. If the Contract / Service Specification include more than one document, then unless the Purchaser specifies to the contrary, the later in time shall prevail over a document of earlier date to the extent of any inconsistency.

m. In case of reference of same scope of work/contract condition or any clause in the RFP (all sections) drawing different inferences, in that position, any clause in Section-3 would prevail over the other.

3. Conditions Precedent

This Contract is subject to the fulfillment of the following conditions precedent by the Bidder.

3.1. Furnishing by the Bidder, an unconditional, irrevocable and continuing Bank Guarantee towards contract performance for 10% of the total contract value, in a form and manner specified in Clause 3.1, Section 4 of this RFP and acceptable to the Purchaser and which would remain valid until such time as stipulated by the Purchaser.

3.2. Obtaining of all statutory and other approvals required for the performance of the Services under this Contract. This may include approvals/clearances, wherever applicable, that may be required for execution of this contract e.g. clearances from Government authorities for importing equipment, exemption of Tax/Duties/Levies, work permits/clearances for Bidder/Bidder's team, etc.

3.3. Furnish notarized copies of any/all contract(s) duly executed by the Bidder and its OEMs existing at the time of signing of this contract in relation to the Purchaser's project. Failure to do so within stipulated time of signing of contract would attract penalty as defined in clause 39 in this Section.

3.4. Furnishing of such other documents as the Purchaser may specify/ demand.

3.5. The Purchaser reserves the right to waive any or all of the conditions specified in Clause 3 above in writing and no such waiver shall affect or impair any right, power or remedy that the Purchaser may otherwise have.

3.6. In the event that any of the conditions set forth in Clause 3 hereinabove are not fulfilled within 3 months from the date of this Contract, or such later date as may be mutually agreed upon by the parties, the Purchaser may terminate this Contract.

3.7. In case there is a contradiction between the sections, the below hierarchy of sections in order of precedence :

3.7.1. Pre-bid clarification

3.7.2. Section 3 (GCC holds precedence over SCC)

3.7.3. Section 5

3.7.4. Section 5A

3.7.5. Section 5B

3.7.6. Section 2

3.7.7. Section 4

3.7.8. Section 1

4. Scope of work / Contract

4.1. Scope of the Contract shall be as defined in Section 5 of the RFP and Annexes thereto of the tender.

4.2. The Bidder is required to provide such goods, services and support as the Purchaser may deem proper and necessary, during the term of this Contract, and includes all such processes and activities which are consistent with the proposals set forth in the Bid, the Tender and this Contract and are deemed necessary by the Purchaser, in order to meet its requirements (hereinafter 'scope of work').

5. Key Performance Measurements

5.1. Unless specified by the Purchaser to the contrary, the Bidder shall deliver the goods, perform the Services and carry out the scope of work in accordance with the terms of this Contract, Scope of Work and the Service Specifications as laid down under **Service Level Agreement** of this section.

5.2. The Purchaser reserves the right to amend any of the terms and conditions in relation to the Contract and may issue any such directions which are not necessarily stipulated therein if it deems necessary for the fulfillment of the scope of work.

6. Commencement and Progress

6.1. The Bidder shall subject to the fulfillment of the conditions precedent set out in Clause 3 above, commence the performance of its obligations in a manner as per the Scope of Work (Section 5 of the RFP).

6.2. The Bidder shall proceed to carry out the activities / services with diligence and expedition in accordance with any stipulation as to the time, manner, mode, and method of execution contained in this Contract.

6.3. The Bidder shall be responsible for and shall ensure that all activities / services are performed in accordance with the Contract, Scope of Work and Service Specifications and that the Bidder’s Team complies with such Specifications and all other standards, terms and other stipulations/conditions set out hereunder.

6.4. The Bidder shall perform the activities / services and carry out its obligations under the Contract with due diligence, efficiency and economy, in accordance with generally accepted techniques and practices used in the industry and shall observe sound management, engineering and security practices. The Bidder shall always act, in respect of any matter relating to this Contract, as faithful advisors to the Purchaser and shall, at all times, support and safeguard the Purchaser's legitimate interests in any dealings with Third parties.

6.5. The Goods supplied under this Contract shall conform to the standards mentioned in the Technical Specifications, and where no applicable standard is mentioned, to the authoritative standards, such standard shall be the latest issued by the concerned institution. Delivery of the Goods shall be made by the Bidder in accordance with the terms specified by the Purchaser in its Notification of Award / Purchase Order.

6.6. The Services rendered under this Contract shall at all times conform to the service levels specified in Service Level Agreements of this section of RFP.

6.7. The drawings accompanying the RFP document are of indicative nature for general guidance of the bidder to enable him to visualize the type of work and/ or supplies contemplated under the contract and are issued for bidding purpose only. Purpose of these drawing is to enable the bidder to make an offer in line with the requirements of the Purchaser. The overall design of the solution is bidder's responsibility.

7. Approvals and Required Consents

7.1. The Purchaser will extend necessary support to the Bidder to obtain, maintain and observe all relevant and customary regulatory and governmental licenses, clearances and applicable approvals (hereinafter the "Approvals") necessary for the Bidder to provide the Services. The costs of such Approvals shall be borne by the Bidder. Both parties will give each other all co-operation and information reasonably.

8. Bidder's Obligations

8.1. **Scope of Work**: The Bidder's obligations shall include all the activities as specified by the Purchaser in the Scope of Work and other sections of the Tender and Contract and changes thereof to enable Purchaser to meet the objectives and operational requirements. It will be the Bidder's responsibility to ensure the proper and successful implementation, performance and continued operation of the proposed system in accordance with and in strict adherence to the terms of his Bid, the Tender and this Contract.

8.2. **Licenses and OEM support**: All the software licenses that the Bidder proposes should be perpetual software licenses. The software licenses shall not be restricted based on location and the Purchaser should have the flexibility to use the software licenses for other requirements if required.

8.2.1. The Bidder shall ensure that the Annual Maintenance support for the software and hardware components and other devices is provided till the end of the contract period. Annual Maintenance support shall include, but not limited to, patches, support licenses, updates and upgrades of the software, hardware components and other devices. The Bidder shall ensure that there is a comprehensive onsite warranty / support arrangement for the aforementioned period with all the OEMs.

8.2.1.1. The Bidder should provide the latest hardware and specification shall be such that it does not need up gradation during the contract period.

8.2.1.2. All software application updates and upgrades will be provided by the bidder during the contract period at no extra cost to the purchaser.

8.2.2. The Purchaser reserves the right to review the terms of the Warranty and Annual Maintenance agreements entered into between the Bidder and OEMs and no such agreement/contract shall be executed, amended, modified and/or terminated without the prior written consent of the Purchaser. An executed copy of each of such agreements/contracts shall, immediately upon execution be submitted by the Bidder to the Purchaser.

8.2.3. The Bidder shall ensure that none of the hardware and software components and sub-components is declared **end-of-sale** or **end-of-support** by the respective OEM for 12 months from submission of the bid. If, the OEM declares any of the products/solutions end-of-sale subsequently, the Bidder shall ensure that the same is supported by the respective OEM for contract period.

8.2.4. If a product is de-supported by the OEM for any reason whatsoever, from the date of Acceptance of the System till the end of contract, the Bidder should replace the products/solutions with an alternate that is acceptable to the Purchaser at no additional cost to the Purchaser and without causing any performance degradation.

8.2.5. The Bidder shall ensure that the OEMs provide the support and assistance to the Bidder in case of any problems / issues arising due to integration of components supplied by him with any other component(s)/product(s) under the purview of the overall solution. If the same is not resolved for any reason whatsoever, the Bidder shall replace the required component(s) with an equivalent or better substitute that is acceptable to Purchaser without any additional cost to the Purchaser and without impacting the performance of the solution in any manner whatsoever

8.3. The Bidder warrants that the goods supplied under this contract shall be of the high grade and quality and consisted with the established and generally accepted standards for materials of this type. The goods shall be in full conformity with the specifications and shall operate properly and safely. All recent design improvements in goods, unless provided otherwise in the Contract, shall also be made available.

8.4. The Bidder further warrants that the Goods supplied under this Contract shall be free from all encumbrances and defects/faults arising from design, material, manufacture or workmanship

8.5. The Purchaser shall promptly notify the Bidder in writing of any claims arising under this warranty. Upon receipt of such notice, the Bidder shall, with all reasonable speed, repair or replace the defective Goods or parts thereof, without prejudice to any other rights which the Purchaser may have against the Bidder under the Contract.

8.5.1. If the Bidder, having been notified, fails to remedy the defect(s) within a reasonable period, the Purchaser may proceed to take such remedial action as may be necessary, at the Bidder’s risk and expense and without prejudice to any other rights which the Purchaser may have against the Bidder under the Contract.

8.5.2. The Bidder shall ensure that the all the OEMs for hardware/equipment or Bidder's trained engineers conduct the preventive maintenance on a Quarterly basis and break-fix maintenance in accordance with the best practices followed in the industry.

8.5.3. The Bidder shall ensure that the documentation and training services associated with the components shall be provided by the OEMs without any additional cost to the Purchaser.

8.5.4. The Bidder cannot have re-negotiation with the OEM after placing a purchase order. The bidder shall issue the purchase order for OEM within 15 days, as per requirement and timelines of project plan and with approval from the Purchaser. Any delay in issuing the Purchaser Order to the OEM would lead to penalty as detailed in Clause 39 of this section. A copy of the purchase order shall be submitted to the Purchaser and need not include any commercial information. In case, the purchase order is not submitted and is causing delay in the project execution then the Purchaser reserves the right to procure the material at Bidder’s risk and cost from L2 bidder.

8.6. **Bidder’s representative**: Bidder’s representative(s) shall have all the powers requisite for the execution of scope of work and performance of services under this contract. The Bidder’s representative(s) shall liaise with the Purchaser’s representative for the proper coordination and timely completion of the works and on any other matters pertaining to the works. The Bidder will extend full co-operation to Purchaser’s representative in the manner required by them for supervision/inspection/observation of the equipment/goods/material, procedures, performance, progress, 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 compliance of rules, regulations and safety practice.

8.7. The Bidder shall be responsible on an ongoing basis for coordination with other vendors and agencies of the Purchaser in order to resolve issues and oversee implementation of the same. The Bidder shall also be responsible for resolving conflicts between vendors.

8.8. **Access to Sites**

8.8.1. The Purchaser’s representative upon receipt of request from the Bidder intimating commencement of installation at Sites shall give to the Bidder access to as much of the Sites as may be necessary to enable the Bidder to commence and proceed with the installation of the works in accordance with the programme of work. Any reasonable proposal of the Bidder for access to site to proceed with the installation of work in accordance with the programme of work will be considered for approval and shall not be unreasonably withheld by the Purchaser. Such requests shall be made to the Purchaser’s representative in writing at least 7 days prior to start of the work.

8.8.2. At the Sites and Purchaser's locations, the Purchaser's representative shall give to the Bidder access to as much as may be necessary to enable the Bidder to commence and proceed with the installation of the works in accordance with the programme of work or for performance of Facilities Management Services.

8.9. **Start of Installation**

8.9.1. Bidder shall co-ordinate with the Purchaser and stakeholders for the complete setup of the Cloud Data Centre sites before commencement of installation at respective sites. The bidder shall also co-ordinate regarding Network / Bandwidth connectivity in order to prepare the installation plan and detailed design / architectural design documents.

8.9.2. As per TRAI guidelines, resale of bandwidth connectivity is not allowed. In such a case tripartite agreement should be formed between purchaser, selected Bidder and Internet Service Provider (s).

8.9.3. The plan and design documents thus developed shall be submitted by the Bidder for approval by the Purchaser.

8.9.4. After obtaining the approval from the Purchaser, the Bidder shall commence the installation.

8.10. **Reporting Progress**

8.10.1. The Bidder shall monitor progress of all the activities related to the execution of this contract and shall submit to the Purchaser, progress reports including photographs and videos with reference to all related work, milestones and their progress during the implementation phase on weekly and monthly basis. The Bidder should also provide a Pert Chart based on which monitoring may be done also.

8.10.2. Formats for all abovementioned reports and their dissemination mechanism shall be discussed and finalized at the Kick-Off meeting. The Purchaser on mutual agreement between both parties may change the formats, periodicity and dissemination mechanism for such reports.

8.10.3. Periodic meetings shall be held between the representatives of the Purchaser and the Bidder once in every 7 days during the implementation phase to discuss the progress of implementation. After the implementation phase is over, the meeting shall be held as an ongoing basis, as desired by Purchaser, to discuss the performance of the contract.

8.10.4. The Bidder shall ensure that the respective solution teams involved in the execution of work are part of such meetings.

8.10.5. High Level **Committees** involving representative of the Purchaser and senior officials of the Bidder shall be formed for the purpose of this project. These committees shall meet at intervals, as decided by the Purchaser later, to oversee the progress of the implementation. The committees are as under:

8.10.5.1. Empowered Committee: Headed by Additional Secretary (MHA) along with MHA officials

8.10.5.2. Steering Committee: Headed by Joint Secretary along with other MHA officials

8.10.6. All the goods, services and manpower to be provided / deployed by the Bidder under the Contract and the manner and speed of execution and maintenance of the work and services are to be conducted in a manner to the satisfaction of Purchaser's representative in accordance with the Contract.

8.10.7. The Purchaser reserves the right to inspect and monitor/assess the progress/performance of the work / services at any time during the course of the Contract. The Purchaser may demand and upon such demand being made, the Bidder shall provide documents, data, material or any other information which the Purchaser may require, to enable it to assess the progress/performance of the work / service.

8.10.8. At any time during the course of the Contract, the Purchaser shall also have the right to conduct, either itself or through another agency as it may deem fit, an audit to monitor the performance by the Bidder of its obligations/functions in accordance with the standards committed to or required by the Purchaser and the Bidder undertakes to cooperate with and provide to the Purchaser/ any other agency appointed by the Purchaser, all Documents and other details as may be required by them for this purpose. Such audit shall not include Bidder's books of accounts.

8.10.9. The Bidder shall reply to the written notice giving details of the measures proposed to be taken to expedite the progress so as to complete the works by the prescribed time or to ensure compliance to RFP requirements. The Bidder shall not be entitled to any additional payment for taking such steps. If at any time it should appear to the Purchaser or Purchaser's representative that the actual progress of work does not conform to the approved plan, the Bidder shall produce at the request of the Purchaser's representative a revised plan showing the modification to the approved plan necessary to ensure completion of the works within the time for completion or steps initiated to ensure compliance to the stipulated requirements

8.10.10. The submission seeking approval by the Purchaser or Purchaser's representative of such plan shall not relieve the Bidder of any of his duties or responsibilities under the Contract.

8.10.11. In case during execution of works, the progress falls behind schedule or does not meet the Tender requirements, the Bidder shall deploy extra manpower/ resources to make up the progress or to meet the RFP requirements. All cost will be the responsibility of the bidder.

8.11. **Knowledge of Sites' conditions**

8.11.1. The Purchaser shall grant access to the Bidder to the Sites.

8.11.2. The Bidder shall be deemed to have knowledge of the Sites and their surroundings and information available in connection therewith and to have satisfied itself the form and nature thereof including, the data contained in the Bidding Documents, the physical and climatic conditions, the quantities and nature of the works and materials necessary for the completion of the works, the means of access, etc. and in general to have obtained itself all necessary information of all risks, contingencies and circumstances affecting his obligations and responsibilities therewith under the Contract and his ability to perform it. However, if during pre-installation survey / during delivery or installation, the Bidder detects physical conditions and/or obstructions affecting the work, the Bidder shall take all measures to overcome them.

8.12. **Project Plan**

8.12.1. Within 21 calendar days of Effective date of the contract, the Bidder shall submit to the Purchaser for its approval a detailed Project Plan with details of the project showing the sequence, procedure and method in which he proposes to carry out the works. The Plan so submitted by the Bidder shall conform to the requirements and timelines specified in the Contract. The Purchaser and the Bidder shall discuss and agree upon the work procedures to be followed for effective execution of the works, which the Bidder intends to deploy and shall be clearly specified. The Project Plan shall include but not limited to project organization, communication structure, proposed staffing, roles and responsibilities, processes and tool sets to be used for quality assurance, security and confidentiality practices in accordance with industry best practices, project plan and delivery schedule in accordance with the Contract. Approval by the Purchaser's Representative of the Project Plan shall not relieve the Bidder of any of his duties or responsibilities under the Contract.

8.12.2. If the Bidder's work plans necessitate a disruption/ shutdown in Purchaser's operation, the plan shall be mutually discussed and developed so as to keep such disruption/shutdown to the barest unavoidable minimum. Any time and cost arising due to failure of the Bidder to develop/adhere such a work plan shall be to his account.

8.13. **Bidder's Organisation**

8.14. **Staffing and team:** The requirements for Bidder's team and staffing are outlined in Section 5 – Scope of Work. Bidder shall ensure that the Bidder's Team is security vetted as per Purchasers guidelines, competent, professional and possesses the requisite qualifications and experience appropriate to the task they are required to perform under this Contract.

8.14.1. Bidder shall ensure that the Services are performed through the efforts of the Bidder's Team, in accordance with the terms hereof and to the satisfaction of the Purchaser.

8.14.2. Nothing in this Contract relieves the Bidder from its liabilities or obligations under this Contract to provide the Services in accordance with the Purchaser's directions and requirements and as stated in this Contract and the Bid to the extent accepted by the Purchaser and the Bidder 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.

8.14.3. The Bidder shall provide the Purchaser with the resume of the proposed personnel and provide such other information as the Purchaser may reasonably require. The Bidder shall conduct background verification checks of the proposed personnel (Bidder's Team) and share the report with the Purchaser before joining the project.

8.14.4. Purchaser reserves the right to interview the personnel proposed that will be deployed as part of the project team. If found unsuitable, the Purchaser may reject the deployment of the personnel. But ultimate responsibility of the project implementation shall lie with the Bidder.

8.14.5. Purchaser reserves the right to require changes in personnel which shall be communicated to the Bidder. The Bidder with the prior approval of the Purchaser may make additions to the project team.

8.14.6. The Bidder shall ensure that none of the Key Personnel (refer Clause 10.2 of Section 5 of the RFP) proposed, exit from the project during first 18 months of the project. The change of Key Personnel will be accepted only in case of person leaving the organization or medical exigency. It is important that the Bidder submits profiles of only those resources that are available for the project. In case of any change of the Key Personnel during the first 18 months of the project, it would attract a penalty as per clause 39 in this Section irrespective of the reasons. It does not apply in case of change requested by the Purchaser. Every change in any case will require the approval of the Purchaser.

8.14.7. In case of change in its team members, for any reason whatsoever, the Bidder shall ensure that the exiting members are replaced with at least equally qualified and professionally competent members and shall ensure a reasonable amount of time overlap in activities to ensure proper knowledge transfer and handover / takeover of documents and other relevant materials between the outgoing and the new member.

8.14.8. In case of replacement of any manpower resource, the Bidder should ensure efficient knowledge transfer from the outgoing resource to the incoming resource and adequate hand-holding period and training for the incoming resource in order to maintain the continued level of service. There should be at least 30 day overlap period for knowledge transfer.

8.14.9. All manpower resources deployed by the Bidder for execution of this contract must strictly adhere to the attendance reporting procedures and make their services available as agreed upon for the entire reporting time period at the Sites. The resources which have been allocated at 100% for the project, cannot work simultaneously on other projects.

8.14.10. The Bidder shall provide at the respective sites necessary supervision during the execution of work and as long thereafter as the Purchaser may consider necessary for the proper fulfillment of the Bidder’s obligations under the Contract. The Bidder or his competent and authorized representative(s) shall be constantly present at the respective Data Centre Sites during agreed time for supervision. The Bidder shall authorize his representative to receive directions and instructions from the Purchaser’s Representative.

8.14.11. The Bidder shall be responsible for the deployment, transportation, travel, accommodation and other requirements of all its employees required for the execution of the work and provision for all costs/charges in connection thereof.

8.14.12. The Bidder shall provide and deploy at the Sites only those manpower resources who are qualified/skilled and experienced in their respective trades and who are competent to deliver in a proper and timely manner the work they are required to perform or to manage/supervise the work.

8.14.13. The Purchaser’s Representative may at any time object to and require the Bidder to remove forthwith from the Sites; any authorized representative or employee of the Bidder or any person(s) of the Bidder’s team, if, in the opinion of the Purchaser’s Representative the person in question has misconduct or his / her deployment is otherwise considered undesirable by the Purchaser’s representative. The Bidder shall forthwith remove and shall not again deploy the person without the written consent of the Purchaser’s Representative.

8.14.14. The Purchaser’s Representative may at any time object to and request the Bidder to remove from the project, any of Bidder’s authorized representative including any employee of the Bidder or his team or any person(s) deployed by the Bidder or his team for professional incompetence or negligence or for being deployed for work for which he is not suited or for any other reason. The Bidder will have to replace the concern person.

8.15. **Adherence to safety procedures, rules regulations and restriction**

8.15.1. The Bidder’s Team shall comply with the provision of all laws including labour laws, rules, regulations and notifications issued there under from time to time. All safety and labour laws enforced by statutory agencies and by Purchaser shall be applicable in the performance of this Contract and Bidder’s Team shall abide by these laws.

8.15.2. Access to the Cloud Data Centre sites and Operations Centre shall be strictly restricted. No access to any person except the essential members of the Bidder’s Team who are genuinely required for execution of work or for carrying out management/maintenance who have been explicitly authorised by the Purchaser shall be allowed entry to the Data Centre and Operations Centre Sites. Even if allowed, access shall be restricted to the pertaining equipment of the Purchaser only. The Bidder shall maintain a log of all activities carried out by each of its team personnel including entry/exit of the premises.

8.15.3. The Bidder shall take all measures necessary or proper to protect the personnel, work and facilities and shall observe all safety rules and instructions. The Bidder’s Team shall adhere to all security requirement/regulations of the Purchaser during the execution of the work.

8.15.4. The Bidder shall report as soon as possible any evidence, which may indicate or is likely to lead to an abnormal or dangerous situation and shall take all necessary emergency control steps to avoid such abnormal situations.

8.16. **Statutory Requirements**

8.16.1. During the tenure of this Contract nothing shall be done by the Bidder or his team in contravention of any law, act and/ or rules/regulations, there under or any amendment thereof governing inter-alia customs, stowaways, foreign exchange etc. and shall keep Purchaser indemnified in this regard.

9. Purchaser’s Obligations

9.1. Purchaser 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 the Bidder.

9.2. Purchaser shall ensure that timely approval is provided to the Bidder as and when required, which may include approval of project plans, implementation methodology, design documents, specifications, or any other document necessary in fulfillment of this contract.

9.3. The Purchaser’s representative shall interface with the Bidder, to provide the required information, clarifications, and to resolve any issues as may arise during the execution of the Contract. Purchaser shall provide adequate cooperation in providing details, coordinating and obtaining of approvals from various governmental agencies, in cases, where the intervention of the Purchaser is proper and necessary.

9.4. Purchaser may provide on Bidder’s request, particulars/information/ or documentation that may be required by the Bidder for proper planning and execution of work and for providing services covered under this contract and for which the Bidder may have to coordinate with respective vendors.

10. Payments

10.1. Purchaser shall make payments to the Bidder at the times and in the manner set out in the Payment schedule which is described in Clause D - Annexure II in this section .Milestones with timelines and deliverable are specified in clause 15 of section 5 in this RFP. Implementation phase and operation & maintenance phase are defined in clause 4.6.2 and 4.6.3 in section 5 of this RFP. Purchaser will make all efforts to make payments to the Bidder within 30 days of receipt of invoice(s) and all necessary supporting documents.

10.2. All payments agreed to be made by Purchaser to the Bidder in accordance with the Bid shall be inclusive of all statutory levies, duties, taxes and other charges whenever levied/applicable, if any, and Purchaser shall not be liable to pay any such levies/other charges under or in relation to this Contract and/or the Services.

10.3. No invoice for extra work/change order on account of change order will be submitted by the Bidder unless the said extra work /change order has been authorized/approved by the Purchaser in writing in accordance with Change Control process. Change control process would be defined by the Purchaser later.

10.4. In the event of Purchaser noticing at any time that any amount has been disbursed wrongly to the Bidder or any other amount is due from the Bidder to the Purchaser, the Purchaser may without prejudice to its rights recover such amounts by other means after notifying the Bidder or deduct such amount from any payment falling due to the Bidder. The details of such recovery, if any, will be intimated to the Bidder. The Bidder 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 Purchaser or the Bidder.

10.5. All payments to the Bidder shall be subject to the deductions of tax at source under applicable taxes, and deductions as provided for under any law, rule or regulation. All costs, damages or expenses which Purchaser may have paid or incurred, for which under the provisions of the Contract, the Bidder is liable, the same shall be deducted by Purchaser from any dues to the Bidder. All payments to the Bidder shall be made after making necessary deductions as per terms of the Contract and recoveries towards facilities, if any, provided by the Purchaser to the Bidder on chargeable basis.

10.6. In case of change in service taxes under change in law, appropriate parties shall pass the benefit, if any, of the same over and above the contract value to the other party.

10.7. Purchaser- shall be at liberty to deduct such amounts from the invoices raised by the bidder as calculated by application of the provisions for liquidated damages, SLA and any other penalties as specified in this section of the RFP.

10.8. All invoices to be submitted quarterly along with SLA reports.

11. Intellectual Property Rights

11.1. Any / all Intellectual Property Rights owned by the Bidder prior to the execution date and/ or applied for prior to the execution date ("herein after referred to as "pre-existing IPR") shall strictly vest with the Bidder as the case maybe and the Purchaser shall have no right whatsoever on such Intellectual Property Rights.

11.2. Any/ All Intellectual Property Rights modified by the Bidder during the Contract Term, which is not related to work within this contract, shall also exclusively vest with the Bidder.

11.3. Any / all Intellectual Property owned by the Purchaser prior to the execution date and/ or any Intellectual Property Right applied for prior to the execution date ("herein after referred to as "pre-existing IP") shall strictly vest with the Purchaser and the Bidder shall have no right whatsoever on such Intellectual Property.

11.4. After the execution date the Purchaser shall exclusively own/ have rights/ title and have right in perpetuity to use all Intellectual Property that:

11.4.1. are newly created and developed by the Bidder during execution of this Contract and/ or for the exclusive use of the Purchaser or primarily in connection with the Purchaser's Assets;

11.4.2. was developed exclusively or primarily for the conduct of the Purchaser's Project or in connection with the Purchaser's Assets;

11.4.3. arose from funding by the Purchaser, or exclusively or primarily for the benefit of/ the conduct of, the Purchaser's Project or in connection with the Purchaser's Assets.

11.5. The Bidder and/ or 3rd party vendors as the case may be, shall grant non-exclusive, non-transferable, irrevocable licenses, to the Purchaser, for its project at all geographic locations, to use their pre-existing IPRs (relevant to this project) and any foreground IPRs developed by them for this project, but not restricted to the term of this Contract.

11.6. If Purchaser desires, the Bidder 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 Bidder, the same shall be acquired in the name of the Purchaser, prior to termination of this Contract and which may be assigned by the Purchaser to the Bidder for the purpose of execution of any of its obligations under the terms 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 Purchaser.

11.7. Bidder shall ensure that while it uses 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/ third party and Bidder shall keep the Purchaser indemnified against all costs, expenses and liabilities. Howsoever, arising out of any illegal or unauthorized use (piracy) or misuse/ breach of terms of contract 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 Bidder as per the terms of the indemnification clause.

11.8. Information Security

11.8.1. The Bidder / Team/ representatives/ employees etc. shall not carry any written/printed document, layout diagrams, Compact Discs, pen drive, hard disk, storage tapes, and/ or any other storage devices media or any other goods /material either out of Sites without prior written consent and written permission from the Purchaser or the designated authority.

11.8.2. All documentation and media at the respective Sites shall be properly identified, labelled and numbered by the Bidder. Bidder shall keep track of all such items and provide a monthly summary report of these items to the Purchaser.

11.8.3. The Bidder / Team/ representatives/ employees etc. shall follow the Purchaser's Information Security Policy. Access to Purchaser's data and systems, Email and Internet facility by the Bidder / Team/ representatives/ employees etc., at any of the Sites shall strictly be in accordance with the security and access policies set/laid down by the Purchaser.

11.8.4. The Bidder / Team/ representatives/ employees etc. acknowledge that Purchaser's business data and other Purchaser proprietary information or materials, whether developed by Purchaser or being used by the Purchaser pursuant to any license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to the Purchaser; and the Bidder along with its Team/ representatives/ employees etc., agree to use such information with all reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall under no circumstance be less than that used by the Bidder to protect its own proprietary information. The Bidder recognizes that the goodwill of Purchaser depends, among other things, upon the Bidder keeping such proprietary information confidential and that unauthorized disclosure of the same by Bidder/ Team/ representatives/ employees etc. could damage the goodwill of Purchaser and that by reason of the Bidder's duties hereunder. The Bidder may come into possession of such proprietary information, even though the Bidder 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. Bidder shall use such information only for the purpose of performing the services under this contract.

11.8.5. Bidder shall, upon termination of this agreement for any reason, or upon ending of the term of the contract or upon demand by the Purchaser, whichever is earliest, return any and all information provided to Bidder by the Purchaser or by any third party in connection with this Contract, including any copies or reproductions, both hardcopy and electronic.

12. Taxes

12.1. Applicable tax shall be deducted at source by Purchaser from all the payments made to Bidder according to the Indian Acts and Rules, unless valid and complete documents for tax exemption are submitted by the Bidder prior to release of payment. A certificate shall be provided by Purchaser to the Bidder for any tax deducted at source.

12.2. The Bidder shall bear all personnel taxes levied or imposed on its personnel, or any other member of the Bidder's Team, etc. on account of payment received under this Contract. The Bidder shall bear all corporate taxes, levied or imposed on the Bidder on account of payments received by it from the Purchaser for the work done under this Contract.

12.3. The Bidder shall bear all taxes and duties etc. levied or imposed on the Bidder under the Contract including but not limited to Sales Tax, Customs duty, Excise duty, Octroi, Service Tax, VAT, Works Contracts Tax and all Income Tax levied under Indian Income Tax Act – 1961 or any amendment thereof during the entire contract period, i.e., on account of material supplied and services rendered and payments received by him from the Purchaser under the Contract. It shall be the responsibility of the Bidder to submit to the concerned Indian authorities the returns and all other connected documents required for this purpose. The Bidder shall also provide the Purchaser such information, as it may be required in regard to the Bidder's details of payment made by the Purchaser under the Contract for proper assessment of taxes and duties. The amount of tax withheld by the Purchaser shall at all times be in accordance with Indian Tax Law and the Purchaser shall promptly furnish to the Bidder original certificates for tax deduction at source and paid to the Tax Authorities.

12.4. The Bidders shall fully familiarize themselves about the applicable domestic taxes (such as value added or sales tax, service tax, income taxes, duties, fees, levies, etc.) on amounts payable by the Purchaser under the Agreement. All such taxes must be included by Bidders in the financial proposal. (Bidder to find out applicable taxes for the components being proposed.)

12.5. Should the Bidder 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 Bidder shall pay the same. The Bidder shall indemnify Purchaser against any and 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 Purchaser/ Bidder.

13. Representation and warranties

In order to induce the Purchaser to enter into this Contract, the Bidder hereby represents and warrants as of the date hereof. The following representations and warranties shall survive the term and termination hereof:

13.1. The Bidder is a registered company incorporated under the laws of India and has been properly constituted and is in continuous existence since incorporation. The Bidder shall at all point of time, during the term of contract and during such extended period as the Purchaser may approve, maintain a registered office within the territory of INDIA.

13.2. That the Bidder has the power and the authority that would be required to enter into this Contract and the requisite experience, the technical know-how and the financial wherewithal required to successfully execute the terms of this contract and to provide services sought by the Purchaser under this contract.

13.3. That the Bidder is not involved in any litigation or legal proceedings, pending, existing, potential or threatened, that may have an impact of affecting or compromising the performance of its obligations or delivery of Services under this Contract.

13.4. That the representations and warranties made by the Bidder in its Bid, Tender and Contract are and shall continue to remain true and correct throughout the term of this Contract and Bidder shall fulfil all the requirements as are necessary for executing the obligations and responsibilities as laid down in the Contract and the Tender and unless the Purchaser specifies to the contrary, the Bidder shall be bound by all the terms of the Bid/Tender/Contract.

13.5. That the Bidder and its team has the professional skills, personnel, infrastructure and resources/authorizations that are necessary for providing all such services as are necessary to fulfil the scope of work stipulated in the Tender and this Contract.

13.6. That the Bidder shall ensure that all assets/ components including but not limited to equipment, software, licenses, processes, documents, etc. installed, developed, procured, deployed and created during the term of this Contract are duly maintained and suitably updated, upgraded, replaced.

13.7. That the Bidder shall procure all the necessary permissions and adequate approvals and licenses for use of various software and any copyrighted/ patented process/ product, as are specifically mentioned by the Bidder in its Bid or agreed in writing by the Bidder during the Contract term, free from all claims, titles, interests and liens thereon and shall keep the Purchaser indemnified in relation thereto.

13.8. That the execution of the scope of work and the Services herein is and shall be in accordance and in compliance with all applicable laws.

13.9. That Bidder has the corporate power to execute, deliver and perform the terms and provisions of this Contract and has taken all necessary corporate action to authorise the execution, delivery and performance by it of the Contract. That all conditions precedent under the Contract has been satisfied.

13.10. That neither the execution and delivery by the Bidder/ Bidder's Team of the Contract nor the Bidder / Bidder Team's compliance with or performance of the terms and provisions of the Contract (i) shall 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) shall conflict or be inconsistent with or result in any breach of any or 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) shall violate any provision of the Memorandum and Articles of Association of the Bidder.

13.11. That the Bidder certifies that all registrations, recordings, filings and notarisations of the Contract and all payments of any tax or duty, including but not limited to 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.

13.12. That the Bidder confirms that there has not and shall not occur any execution, amendment or modification of any of its agreement/ contract/ sub-contract without the prior written consent/ approval of the Purchaser, which may directly or indirectly have a bearing on the Contract or the project.

13.13. That the Bidder 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.

13.14. That the Bidder 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 performance of the project under this contract and regarding the same the Bidder does not, so far as the Bidder is aware, in carrying on its business and operations, infringe any Intellectual Property Rights of any person. So far as the Bidder is aware, none of the Intellectual Property Rights owned or enjoyed by the Bidder or which the Bidder is licensed to use, which are material in the context of the Bidder’s business and operations for the performance of this contract are being infringed nor, so far as the Bidder is aware, is there any infringement or threatened infringement of those 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) required by the Bidder for the performance of the contract 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 the Bidder shall keep the Purchaser indemnified in relation thereto.

13.15. That the Bidder shall provide adequate and appropriate support and participation, on a continuing basis, in tuning all supplied equipment, hardware and software to meet the requirements of the solution design.

13.16. No sum of money or no Payment in kind has been made or promised to be made or accepted by any person (s) or will be made or accepted by any person (s) or on its/ his/ her behalf by way of fees/ commission or in any other form whatsoever to induce the Purchaser to enter into this Contract or to keep the Contract in continuance or to settle the terms of the agreement/ contract.

13.17. Bidder should not with hold any material information/ document from the Purchaser, the nondisclosure of which would have a material and adverse effect on the evaluation and/ or the acceptance of the terms of this Contract.

14. Indemnity

14.1. The Bidder shall indemnify the Purchaser from and against any costs, loss, damages, expense, claims including those from third parties or liabilities of any kind howsoever suffered, arising or incurred inter alia during and after the Contract period out of:

14.1.1. any negligence or wrongful act or omission by the Bidder or any third party associated with the Bidder in connection with or incidental to this Contract; or

14.1.2. any breach of any of the terms of the Bidder's did as agreed, the RFP and this Contract by the Bidder

14.1.3. any infringement of patent, trademark/copyright or industrial design rights arising from the use of the supplied goods and related services or any part thereof

14.2. The Bidder shall also indemnify the Purchaser against any privilege, claim or assertion made by a third party with respect to right or interest in, ownership, mortgage or disposal of any asset, property etc.

14.3. Regardless of anything contained (except for the Bidder's/OEM's liability for bodily injury and/ or damage to tangible and real property for which it is legally liable and it's liability for patent and copyright infringement in accordance with the terms of this Agreement) the total liability of the Bidder is restricted to the total value of the contract.

15. Term and Extension of the Contract

15.1. The term of this Contract is for 5 years and it shall include the time period for Design, Implementation and O&M services from the effective date of this contract. The contract may be extended by two years on same terms & conditions by the purchaser. If the time period of the project is not extended by the purchaser then there should not be any cost over-run in the event of time over-run for the reasons solely attributed to the Bidder.

15.2. Where the Purchaser is of the view that no further extension of the term be granted to the Bidder, the Purchaser shall notify the Bidder of its decision at least 3 (three) months prior to the expiry of the Term. Upon receipt of such notice, the Bidder shall continue to perform all its obligations hereunder, until such reasonable time beyond the Term of the Contract within which, the Purchaser shall either appoint an alternative agency/Bidder or create its own capability to operate such Services as are provided under this Contract.

16. Dispute Resolution

16.1. During the subsistence of this Contract or thereafter, in the event of any dispute, claim, question, or disagreement arising out of or in relation to this contract, disputes between the Parties shall include, without limitation of 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 shall consult and negotiate with each other, in good faith and, recognizing their mutual interests, 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 thirty (30) days, gives to the other Party a thirty (30) day notice in writing, to refer the dispute to arbitration.

16.2. The Arbitration proceedings shall be governed by the Arbitration and Conciliation Act, 1996

16.3. The Arbitration proceedings shall be held at New Delhi, India.

16.4. The Arbitration proceeding shall be governed by the substantive laws of India.

16.5. The proceedings of Arbitration shall be in English language.

16.6. 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/ 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.

16.7. 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 Chief Justice of the Delhi High Court or any person or institution designated by him shall appoint the Arbitrator/Presiding Arbitrator upon request of one of the parties.

16.8. Any letter, notice or other communications dispatched to the Bidder relating to either arbitration proceeding or otherwise whether through the post or through a representative on the address last notified to the Purchaser by the Bidder shall be deemed to have been received by the Bidder although returned with the remarks, refused 'undelivered' where about not known or words to that effect or for any other reasons whatsoever.

16.9. If the Arbitrator so appointed dies, resigns, incapacitated or withdraws for any reason from the proceedings, it shall be lawful for the Purchaser 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.

16.10. 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.

16.11. 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.

16.12. The Arbitrator shall give reasoned award and the same shall be final, conclusive and binding on the parties.

16.13. The fees of the arbitrator, costs and other expenses incidental to the arbitration proceedings shall be borne equally by the parties.

17. Conflict of interest

17.1. The Bidder shall disclose to the Purchaser in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for the Bidder or the Bidder’s Team) in the course of performing the Services as soon it becomes aware of that conflict.

18. Publicity

18.1. The Bidder / Bidder’s Team shall not make or permit to be made a public announcement or media release about any aspect of this Contract unless the Purchaser first gives the Bidder its written consent.

18.2. Bidder undertakes to take all reasonable steps to ensure that its servants/ employees/ agents/ representatives/ professional advisors and consultants comply with Clause 27 of this Contract

19. Force Majeure

19.1. The Purchaser or the Bidder as the case may be are entitled to suspend or excuse their respective performance of their respective obligations under this agreement to the extent that the Purchaser or the Bidder as the case may be is unable to render such performance by an event of Force Majeure.

19.2. In this agreement Force Majeure means any event or circumstance or a combination of events and circumstances, which satisfy all the following conditions:-

19.2.1. materially and adversely affects the performance of an obligation;

19.2.2. are beyond the reasonable control of the affected party;

19.2.3. such party could not have prevented or reasonably overcome with the exercise of good industry practice or reasonable skill or care;

19.2.4. do not result from the negligence or misconduct of/ from/ by such party/ their representatives/ employees/ agents as the case may be, or the failure of such party to perform its obligation hereunder; and

19.2.5. or any consequence of which have an effect described in Clause 19.1

19.3. Force Majeure includes the following events and/ or circumstances to the extent that they or their consequences satisfy the requirements set forth in Clauses 19.1 and 19.2.

19.3.1. war (whether declared or undeclared), invasion, armed conflict or act of foreign enemy in each case involving or directly affecting India;

19.3.2. revolution, riot, insurrection or other civil commotion, act of terrorism or sabotage in each case within India;

19.3.3. nuclear explosion, radioactive and chemical contamination or ionising radiation, directly affecting the area, unless the source and the cause of explosion, contamination, radiation or hazardous thing is brought to or near the area by the Bidder or anyone affiliated to Bidder or any of their employees or servants or agents

19.3.4. strikes, go- slows and/ or lock outs which are on each case wide spread nationwide or political;

19.3.5. any effect of the natural elements including lighting, fire, earthquake, unprecedented rains, cloud bursts, flash floods, landslides, storms, cyclone, tsunami, typhoon or tornado within India;

19.3.6. epidemics and plague within India;

19.3.7. any fire, which is not the effect of natural element:

19.3.8. any event or circumstances of a nature analogous to any events set forth in paragraphs 19.3.1 to 19.3.9 above within India.

19.4. Procedure for Force Majeure

19.4.1. If a party claims relief on account of or under the Force Majeure event, then such party claiming to be effected by the Force Majeure event, immediately on becoming aware of the Force Majeure event must give notice thereof and describe in detail herein under:

a. the Force Majeure event (s) that have occurred;
b. the obligations affected as described in Clause 19;
c. the date of commencement and estimated cession of such event of Force Majeure; and
d. the manner in which the Force Majeure event(s) affect the party’s obligations under this contract/ agreement

e. No party shall be able to suspend or excuse the non-performance of its obligations herein unless such party has given the notice specified above.

19.4.2. The affected party shall have the right to suspend the performance of obligations affected as described in Clause 19 upon delivery of the notice of the occurrence of Force Majeure event in accordance with sub clause 19.4.1 above

19.4.3. The time for performance by the affected party of any obligation or compliance by the affected party with any time limit affected by Force Majeure, and for the exercise of any right affected thereby, shall be extended by the period during which such Force Majeure continues and by such additional period thereafter as is necessary to enable the affected party to achieve the level of activity prevailing before the event of Force Majeure.

19.4.4. The party receiving the claim and relief under the Force Majeure shall, if it wishes to dispute the claim, give a written notice of dispute to the party making the claim within 60 days of receiving of the notice of claim. If the notice of claim is contested within fifteen days as stated above, all the parties to this agreement shall be deemed to have accepted the validity of the claim. If any party disputes the claim, the parties shall follow that procedure set forth in Clause 16.

19.5. Mitigation: The party claiming to be affected by Force Majeure shall take all reasonable steps to prevent/ reduce to a minimum and mitigate the effect of such Force Majeure.

19.6. Termination due to Force Majeure: If Force Majeure event continues for more than 365 days, either party shall have the right to terminate this agreement by giving a notice of termination in respect thereof.

20. Delivery

20.1. The Bidder shall bear the cost for packing, transport, insurance and delivery of all the goods for “**Selection of IT Service Provider for Nationwide Emergency Response System**” at all locations identified by the Purchaser.

20.2. The Goods supplied under this Contract shall conform to the standards mentioned in the RFP, and, when no applicable standard is mentioned, to the authoritative standards; such standard shall be approved by Purchaser.

20.3. The Bidder shall bear all the statutory levies like customs, insurance, freight, etc. applicable on the goods and also the charges like transportation charges, octroi, etc. that may be applicable till the goods are delivered at the respective site of installation shall also be borne by the Bidder.

21. Insurance

21.1. The Goods supplied under this Contract shall be fully insured by the Bidder at his own cost, against any loss or damage, for the entire period of the contract. The Bidder shall submit to the Purchaser, documentary evidence issued by the insurance company, indicating that such insurance has been taken.

22. Transfer of Ownership

22.1. The Bidder must transfer all titles to the assets or goods procured for the purpose of the project to the Purchaser at the time of Acceptance of System. This includes all licenses, titles, source code, certificates etc. related to the system designed, developed, installed and maintained by the Bidder.

B. SPECIAL CONDITIONS OF CONTRACT (SCC)

23. Performance Security

23.1. The successful Bidder shall furnish Performance Security to the Purchaser at the time of signing the Contract which shall be equal to 10% of the value of the Contract and shall be in the form of a **Bank Guarantee** from a Nationalized / Scheduled Bank in the Proforma given in clause 3.1 of Section 4 of this RFP which would be valid up to a period of six months after the contract period. If the contract is extended beyond 5 years then Bank Guarantee will also be appropriately extended to ensure its validity of 6 months after the revised contract period.

24. Liquidated Damages

24.1. If the Bidder fails to supply and install any or all of the goods as per the contract, within the time period(s) specified in the Contract, the Purchaser without prejudice to its other rights and remedies under the Contract, **deduct from the Contract price, as liquidated damages given in the Clause 39 of this Section.**

24.2. The deduction shall not in any case exceed **20 percent of the contract value**.

24.3. The Purchaser may without prejudice to its right to effect recovery by any other method, deduct the amount of liquidated damages from any money belonging to the Bidder in its hands (which includes the Purchaser’s right to claim such amount against the Bidder’s Bank Guarantee) or which may become due to the Bidder. Any such recovery or liquidated damages shall not in any way relieve the Bidder from any of its obligations to complete the Work or from any other obligations and liabilities under the Contract.

25. Ownership and Retention of Documents

25.1. All documents relating to the Purchasers project shall be owned exclusively by the Purchaser. Forthwith upon expiry or earlier termination of this Contract and at any other time on demand by the Purchaser, the Bidder shall deliver to the Purchaser all documents provided by or originating from the Purchaser and all documents produced by or for the Bidder in the course of performing the Services, unless otherwise directed in writing by the Purchaser at no additional cost. The Bidder shall not, without the prior written consent of the Purchaser store, copy, distribute or retain any such documents.

25.2. **Ownership of Data**: By virtue of this Contract, the Bidder/ Bidder’s Team may have access to personal information of the Purchaser and/or a third party or any citizen The Purchaser shall have the sole ownership of and the right to use, all such data in perpetuity including any data or other information pertaining to the citizen that may be in the possession of the Bidder or Bidder's Team in the course of performing the Services under this Contract.

25.3. The Purchaser retains the ownership of the Data during the execution of this contract and Bidder has to facilitate the control of the Data, Operations and Service delivery at any given point of time to Purchaser.

26. Security and Safety

26.1. The Bidder will comply with the directions issued from time to time by the Purchaser and the standards related to the security and safety, in so far as it applies to the provision of the Services.

26.2. The Bidder shall upon reasonable request by the Purchaser, or its nominee(s) participate in regular meetings when safety and information technology security matters are reviewed.

27. Confidentiality

27.1. Confidential Information

27.1.1. All information (whether written/ tangible or oral/ Intangible) furnished by the Purchaser or any third party to the Bidder or Bidder's Representatives/ employees/ agents, in connection with this Contract, and all analyses, compilations, studies or other information documents or materials prepared by Bidder or Bidder's Representatives/ employees/ agents etc., in relation to information obtained by the Bidder in connection to and under the purview of this Contract shall be considered Confidential Information. The Bidder shall not, either during the term or after expiration of this Contract, disclose any proprietary or confidential information relating to the Services/Contract and/or Purchaser's business/ operations, information, Application/software, hardware, business data, architecture schematics, designs, storage media and other information / documents without the prior written consent of the Purchaser.

27.1.2. All information disclosed in writing or email or other tangible electronic storage medium, shall be considered as "Confidential" by the Purchaser.

27.1.3. The term confidential information does not, however, include any information which:

a. was or became publicly available as a matter of law or otherwise without any disclosure by the Bidder/Bidder's Representatives;
b. was or is developed by the Bidderor Bidder's Representatives without reference to any information received from the Purchaser in connection with this Agreement; and
c. has been approved for release in writing by an authorized representative of the Purchaser.

27.2. Terms of Confidentiality

27.2.1. The Bidder (on behalf of itself and its Representatives/ agents/ employees):

a. acknowledges the confidential and proprietary nature of the information;
b. shall keep the information confidential and will not without the prior written consent of the Purchaser, disclose any information to any person (including, without limitation, any member of the media, or any other individual, corporation, partnership, limited liability company, Government agency, or group) in any manner whatsoever, and
c. will not use any information other than for the purpose contained within the contract terms.

27.2.2. The Bidder may however reveal confidential information:

a. To those of Bidder's Representatives/ employees/ agents:
    i. who need to know the information for performing Bidder's obligations under this Contract;
    ii. who are informed by the Bidder of the confidential nature of the information and this Contract; and
    iii. who are bound by confidentiality obligations in terms of an Agreement.
b. If it is required to be disclosed by any decree or order of a government authority, court or statutory law/regulation, by judicial/ quasi-judicial bodies, statutory bodies, and any other applicable provisions of this Agreement;
c. If it is required for the purposes of audit of the Bidder.

27.2.3. The Bidder shall be responsible for any breach of confidentiality by any of its employees/ agents/ representatives/ vendors/ OEMs/ Subcontractors as approved by MHA

27.2.4. The Bidder shall use all reasonable endeavors to ensure that any government department, Court, Contracting Authority, employee, third party or sub-contractor to whom the Purchaser's Confidential Information is disclosed pursuant to Clause 27.2.2 is made aware of the Bidder's obligations of confidentiality.

27.2.5. Bidder and/ or its agents/ employees/ representatives shall not (unless provided for elsewhere in the contract), without prior written consent from the Purchaser, disclose to any person the fact of this Contract or the information existing therein or which has been made available, that the Bidder is considering the transaction, or that discussions or negotiations are taking place or have taken place concerning the transaction or any term, condition or other fact relating to this contract, the transaction thereof or such discussions or negotiations, including, without limitation, the status thereof.

27.2.6. In the event that Bidder is requested pursuant to, or required by, applicable law, regulation or legal process to disclose any of the confidential information or matters contemplated under Clause 27.2.2 hereinabove, then the Bidder shall furnish only that portion of the confidential information which is legally required. The Bidder will otherwise reasonably cooperate with the Purchaser to preserve the confidentiality of the Information. The Bidder shall however, immediately notify the Purchaser promptly so that the Purchaser may seek a protective order or other appropriate remedy.

27.3. The Bidder& its personal (vendors/OEMS/ subcontractors etc) shall execute a Non-Disclosure Agreement (NDA) as given in Clause 3.2, Section 4 of the RFP, in favor of the Purchaser

27.4. The Bidder shall be liable to fully compensate the Purchaser for any loss of service/revenue arising from breach of confidentiality. The Purchaser reserves the right to adopt legal proceedings, civil or criminal, against the Bidder in relation to a dispute arising out of breach of obligation/ confidentiality by the Bidder under this clause.

28. Modification

28.1. Any modification of this Contract shall be in writing and signed by an authorized representative of each Party.

29. Events of Default by the Bidder

The failure on the part of the Bidder to perform any of its obligations or comply with any of the terms of this Contract shall constitute an Event of Default on the part of the Bidder. The events of default are but not limited to:

29.1. The Bidder/ Bidder's Team has failed to perform any instructions or directives issued by the Purchaser which it deems proper and necessary to execute the scope of work or provide services under the Contract, or

29.2. The Bidder/ Bidder's Team has failed to confirm / adhere to any of the key performance indicators as laid down in the Key Performance Measures / Service Levels, or if the Bidder has fallen short of matching such standards / benchmarks / targets as the Purchaser may have designated with respect to the system or any goods, task or service, necessary for the execution of the scope of work and performance of services under this Contract. The above mentioned failure on the part of the Bidder may be in terms of failure to adhere to performance, quality, timelines, specifications, requirements or any other criteria as defined by the Purchaser;

29.3. There is a proceeding for bankruptcy, insolvency, winding up or there is an appointment of receiver, liquidator, assignee, or similar official against or in relation to the Bidder.

29.4. The Bidder/ Bidder's Team has failed to comply with or is in breach or contravention of any applicable laws.

29.5. The Bidder/ Bidder's Team has failed to comply with or adhere to any of the terms & conditions of this contract

29.6. The Bidder has failed to meet appropriate performance criteria and Liquidated damages/ SLA penalty of 20% has been levied for 2 consecutive quarter.

29.7. Where there has been an occurrence of such defaults inter alia as stated above, the Purchaser shall issue a notice of default to the Bidder, setting out specific defaults / deviances / omissions / non-compliances / non-performances and providing a notice of thirty (30) days to enable such defaulting party to remedy the default committed.

29.8. Where despite the issuance of a default notice to the Bidder by the Purchaser, the Bidder fails to remedy the default to the satisfaction of the Purchaser, the Purchaser may, where it deems fit, proceed to contract termination.

30. Consequences of Event of Default

Where an Event of Default subsists or remains uncured the Purchaser shall be entitled to:

30.1. Impose any such obligations and conditions and / or issue any directions / notifications / clarifications as may be necessary to inter alia ensure smooth continuation of the project and the services which the Bidder shall be obliged to comply with that may include re-determination of the consideration payable to the Bidder as agreed mutually by Purchaser and Bidder or through a third party acceptable to both parties. The Bidder shall in addition take all available steps to minimize loss resulting from such event of default.

30.2. Suspend all payments to the Bidder under the Contract by a written notice of suspension to the Bidder, provided that such notice of suspension:

30.2.1. shall specify the nature of the failure; and

30.2.2. shall request the Bidder to remedy such failure within a specified period from the date of receipt of such notice of suspension by the Bidder.

30.3. Require replacement of any of the Bidder’s Team member(s) with another suitable member(s) where the Purchaser deems necessary. The Bidder shall in such case terminate forthwith all their agreements/ contracts/ other arrangements with such member(s) and find suitable replacement for such outgoing member(s) with another member(s) to the satisfaction of the Purchaser, who shall execute such Contracts with the Purchaser as the Purchaser may require. Failure on the part of the Bidder to find a suitable replacement and/or terminate all agreements/contracts with such member(s), shall amount to a breach of the terms hereof and the Purchaser in addition to all other rights, have the right to claim damages and recover from the Bidder all losses/ or other damages that may have resulted from such failure.

30.4. Retain such amounts from the payment due and payable by the Purchaser to the Bidder as may be required to offset any losses caused to the Purchaser as a result of such event of default and the Bidder shall compensate the Purchaser for any such loss, damages or other costs, incurred by the Purchaser in this regard. Nothing herein shall effect the continued obligation of the Bidder and Bidder's Team to perform all their obligations and responsibilities under this Contract in an identical manner as were being performed before the occurrence of the default.

30.5. Invoke the Performance Bank Guarantee and other Guarantees furnished hereunder, recover such other costs/losses and other amounts from the Bidder as may have resulted from such default and pursue such other rights and/or remedies that may be available to the Purchaser under law.

30.6. Require the Bidder to make all such payments as may be incurred / losses borne by the Purchaser in getting such work done through any third party as a result of any default on the part of the Bidder. Bidder agrees to compensate the Purchaser for all such costs incurred by the Purchaser in this regard.

31. Termination

The Purchaser may, terminate this Contract in whole or in part by giving the Bidder a prior and written notice indicating its intention to terminate the Contract under the following circumstances:

31.1. Where the Purchaser is of the opinion that there has been such Event of Default on the part of the Bidder / Bidder's Team which would make it proper and necessary to terminate this Contract and may include failure on the part of the Bidder to respect any of its commitments with regard to any part of its obligations under its Bid, the RFP or under this Contract.

31.2. The Bidder has failed to meet appropriate performance criteria and Liquidated damages/SLA penalty of 20% has been levied for 2 consecutive quarters.

31.3. Where it comes to the Purchaser's attention that the Bidder (or the Bidder's Team) is in a position of actual conflict of interest with the interests of the Purchaser, in relation to any of terms of the Bidder's Bid, the RFP or this Contract.

31.4. Where the Bidder's ability to survive as an independent corporate entity is threatened or is lost owing to any reason whatsoever, including inter-alia the filing of any bankruptcy proceedings against the Bidder, any failure by the Bidder to pay any of its dues to its creditors, the institution of any winding up proceedings against the Bidder or the happening of any such events that are adverse to the commercial viability of the Bidder. In the event of the happening of any events of the above nature, the Purchaser shall reserve the right to take any steps as are necessary, to ensure the effective transition of the pilot site to a successor agency, and to ensure business continuity

31.5. **Termination for Insolvency**: The Purchaser may at any time terminate the Contract by giving written notice to the Bidder, without compensation to the Bidder, if the Bidder 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 Purchaser.

31.6. Terminate the Contract in part or in full, in case the Bidder has not provided remedial action acceptable to the Purchaser, after notice of default.

32. Consequence of Termination

32.1. In the event of termination of this Contract pursuant to Clause 31, [whether consequent to the stipulated Term of the Contract or otherwise] the Purchaser shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the project which the Bidder shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/ breach, and further allow and provide all such assistance to the Purchaser and/or the successor agency, as may be required, to take over the obligations of the erstwhile Bidder in relation to the execution/continued execution of the scope of this Contract, even where such assistance is required to be rendered for a reasonable period that may extend beyond the contract term/ termination hereof.

32.2. Where the termination of the Contract is prior to its stipulated term on account of a default on the part of the Bidder /Bidder's Team or due to the fact that the survival of the Bidder as an independent corporate entity is threatened/has ceased, or for any other reason, whatsoever, the Purchaser through re-determination of the consideration payable to the Bidder as agreed mutually by Purchaser and Bidder or through a third party acceptable to both parties may pay the Bidder for those goods that have been satisfactorily installed and commissioned and for that part of the Services which have been authorized by the Purchaser and satisfactorily performed by the Bidder up to the date of termination. Without prejudice to any other rights, the Purchaser may retain such amounts from the payment due and payable by the Purchaser to the Bidder as may be required to offset any losses caused to the Purchaser as a result of the Termination or due to any acts/omissions of the Bidder. In case of any loss or damage due to default on the part of the Bidder in performing any of its obligations with regard to executing the scope of work under this Contract, the Bidder shall compensate the Purchaser for any such loss, damages or other costs, incurred by the Purchaser. Additionally, the Bidder's Team and/or all third parties appointed by the Bidder shall continue to perform all their obligations and responsibilities as stipulated under this Contract, and as may be proper and necessary to execute the scope of work under the Contract in terms of the Bidder's Bid, the Tender and this Contract, in an identical manner as were being performed before the collapse of the Bidder as described above in order to execute an effective transition and to maintain business continuity of the Purchaser.

32.3. Nothing herein shall restrict the right of the Purchaser to invoke the Bank Guarantee and other Guarantees furnished hereunder and pursue such other rights and/or remedies that may be available to the Purchaser under law.

32.4. The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of this Contract that are expressly or by implication intended to come into or continue in force on or after such termination.

32.5. In the event that the Purchaser or the Bidder, terminates this Agreement pursuant and depending on the event of default, compensation shall be decided by the purchaser as per the services provided by the Bidder that have been accepted by the Purchaser or his authorized representative(s).

33. Change orders

33.1. The Bidder agrees that the System requirements/ quantities/ licenses/ specifications and Service requirements given in the Tender documents are minimum requirements and are in no way exhaustive and guaranteed by the Purchaser.

33.1.1. Any upward revision and/or additions consequent to errors, omissions, ambiguities, discrepancies in the quantities, specifications, drawings etc. of the Tender documents which the Bidder had not accounted for his Bid shall not constitute a change order and such upward revisions and/or addition shall be carried out by Bidder without any time and cost effect to Purchaser.

33.1.2. It shall be the responsibility of the Bidder to meet all performance and other requirements of the Purchaser as stipulated in the Tender document / Contract. Any upward revisions / additions of quantities, specifications, technical manpower, service requirements to those specified by the Bidder in his Bid documents, that may be required to be made during installation / commissioning of the System or at any time during the currency of the contract in order to meet the conceptual design, objective and performance levels or other requirements as defined in the Tender documents shall not constitute a change order and shall be carried out by the Bidder without any change order and without any time and cost effect to the Purchaser whatsoever.

33.2. The Purchaser may at any time, by a written change order given to the Bidder, make changes within the general scope of the Contract. The Purchaser will have the option to increase or decrease the Quantities, Licenses and/or Specifications of the goods/equipment to be supplied and installed by the Bidder or service requirements, as mentioned in the Contract, at any time during the contract period. Depending on the successful implementation of the project, Agent and MDT may increase by about 50%.

33.3. In case of increase in Quantities/ Licenses / Specifications or Service requirements or in case of additional requirement, the Bidder agrees to carry out / provision for such additional requirement at the rate and terms and conditions as provided in the Contract except for the appropriate extension of time to be allowed for delivery/installation of such extra goods/equipment or for commencement of such services. In case of decrease in Quantities or Specifications of goods/equipment or Service requirements, the Bidder shall give a reduction in price at the rate given in the Contract corresponding to the said decrease.

33.4. In case applicable rates for the increase/decrease in question are not available in the Contract then the rates as may be mutually agreed shall apply. The Bidder shall not be entitled to any claim by way of change of price, damages, losses, etc.

33.5. **Conditions for Change Order**

33.5.1. The change order will be initiated only in case (i) the Purchaser directs in writing the Bidder to incorporate changes to the goods or design requirements already covered in the Contract. (ii) the Purchaser directs in writing to the Bidder to include any addition to the scope of work or services covered under this Contract or delete any part thereof, (iii) Bidder requests to delete any part of the work which will not adversely affect the operational capabilities and functioning of the system and if the deletions proposed are agreed to by the Purchaser and for which cost and time benefits shall be passed on to the Purchaser.

33.5.2. Any technology refresh which has been accepted by the purchaser

33.5.3. Any IT Risk assessment which has been accepted by the purchaser

33.5.4. In case, mutual agreement on whether new requirement constitutes the change order or not, is not reached, then Bidder in the interest of the works, shall take up the enforcement of the change order, if advised in writing to do so by Purchaser's Representative pending settlement between the two parties to the effect whether such requirement constitutes a change order or not as per the terms and conditions of Contract documents. The time and cost effects in such a case shall be mutually verified and recorded. Should it establish that the said work constitutes a change order, the same shall be compensated taking into account the records kept in accordance with the Contract.

33.6. **Procedures for Change Order**

33.6.1. If it is mutually agreed that such Requirement constitutes a "Change Request" the bidder has to submit the time, cost, and manpower effort estimate to the purchaser, with proper documentations for approval.

33.6.2. The procedure for change request approval will be notified by the purchaser.

34. No Claim

34.1. The Bidder shall not be entitled to make any claim, whatsoever against the Purchaser, under or by virtue of or arising out of, this contract, nor shall the Purchaser entertain or consider any such claim.

C. SERVICE LEVELS

35. Purpose

35.1. The purpose is to define the levels of service provided by the Bidder to the Purchaser for the duration of the contract .The benefits of this are:

35.1.1. Start a process that applies to Purchaser and Bidder management attention to some aspect of performance, only when that aspect drops below the threshold defined by the purchaser

35.1.2. Help the Purchaser control the levels and performance of Bidder’s services

35.2. The Service Levels are between the Purchaser and the Bidder

36. Service Level Agreements & Targets

36.1. This section is agreed to by Purchaser and Bidder as the key performance indicator for the project. This may be reviewed and revised according to the procedures detailed in Clause 43, SLA Change Control.

36.2. The following section reflects the measurements to be used to track and report system’s performance on a regular basis. The targets shown in the following tables are for the period of contact.

36.3. The procedures in Clause 42 will be used if there is a dispute between Purchaser and Bidder on what the permanent targets should be.

37. General principles of Service Level Agreements

The Service Level agreements have been logically segregated in the following categories:

37.1. **Liquidated Damages**

The liquidated damages will come into effect once the notification of Award has been issued by the Purchaser. It would be mainly applicable on the implementation phase of the project.

37.2. **Service Level Agreement**

SLA would be applicable in operations and maintenance phase of the project. The penalties will be applicable on the Operations & Maintenance cost of the project calculated quarterly. SLA would be applicable on:

a. Cloud Data Centre Application and Components
b. IT infrastructure at State Call Center and Operations Center
c. Network
d. Manpower Availability
e. Audit
f. Issue Resolution
g. Others

38. Service Levels Monitoring

38.1. **The Service Level parameters defined in Clause 39 shall be monitored on a periodic basis**, as per the individual parameter requirements. The Bidder shall be responsible for providing appropriate web based online SLA measurement and monitoring tools for the same. the Bidder will be expected to take immediate corrective action for any SLA that has been breached. In case issues are not rectified to the complete satisfaction of Purchaser within a reasonable period of time then the Purchaser will have the right to take appropriate penalizing actions, including action as per clause 41 or termination of the contract.

39. Measurements & Targets

39.1. **Liquidated Damages**

#	Measurement	Target	Liquidated damage
1.	Signing of contract and submission of performance bank guarantee after award of notification by Purchaser	a. Within 15 days of receipt of award of notification by Purchaser b. Within 30 days of receipt of award of notification by Purchaser	a. Forfeiture of EMD b. Cancellation of award of notification
2.	Team mobilization and commencement of work	a. 100% of key resources within 7 calendar days from the date of signing of contract	0.1% of the contract value per week of delay
2.A	Team mobilization and commencement of work	b. 90% of resources within 30 calendar days from the date of signing of contract	0.1% of the contract value per week of delay
3.	Furnish notarized copies of any/all contract(s) (all commercial negotiation should be concluded) duly executed by the Bidder and its OEMs existing at the time of signing of this contract in relation to the Purchaser's project.	Within 15 days from the date of signing of contract	0.1% of the contract value per week of delay
4.	For every purchase order issued by Purchaser, Bidder should issue purchase order to the respective OEM	Within 15 days from the date of issue of purchase order by Bidder	0.1% of the contract value per week of delay
5.	Completion of milestone no. 7, 8, 9, 10,12 and 14 as per Clause 15, Section 5	As per timelines	0.1% of the contract value per week of delay
6.	Completion of milestone no. 18 and 22 as per Clause 15, Section 15	As per timelines	1% of CAPEX value of respective State, per week of delay

39.2. Service Level Agreements

a. Cloud Data Centre Application and Components

Cloud Data Centre Application and Components					
S. No.	**Definition**	**Measurement**	**Measurement Interval**	**Target**	**Severity Level**
Availability of Cloud Data Centers Applications And Components					
1	Availability of Enterprise Management System (EMS) / Cloud Management Platform (CMP) at the respective Data Centre sites	Uptime = {1 - [(EMS and CMP downtime-Maintenance Downtime) / (Total Time – Maintenance Downtime)]}	Monthly	Minimum 99% up time measured on a monthly basis	-
				>= 96.0% to <99.0% up time measured on a monthly basis	3
				>= 93.0% to <96.0% up time measured on a monthly basis	5
				<93.0% up time measured on a monthly basis	6
2	Availability of each server and virtual machines at the respective Data Centre sites	Uptime = {1 - [(server/VM downtime-Maintenance Downtime) / (Total Time – Maintenance Downtime)]} Each server violation will be measured separately through EMS/CMP tool for penalty.	Monthly	Minimum 99% up time measured on a monthly basis	-
				>= 96.0% to <99.0% up time measured on a monthly basis	3
				>= 93.0% to <96.0% up time measured on a monthly basis	5
				<93.0% up time measured on a monthly basis	6

Cloud Data Centre Application and Components					
S. No.	**Definition**	**Measurement**	**Measurement Interval**	**Target**	**Severity Level**
3	Availability of the : Contact Centre solution which includes CRM, IVRS, ACD, CTI etc. with databases/ software/ hardware	Uptime = {1 - (Application downtime- maintenance downtime) / (Total Time – maintenance downtime) } Please note that continuous downtime of every 2 hours (from 7am to 12midnight) or every 4 hrs (from midnight to 7am) would raise the severity by one level. e.g. the severity level will raise from 0 to 1 Measurement Tool: Reports from EMS/CMP	Monthly	Minimum 99.5% up time measured on a monthly basis	-
				>= 98.0% to <99.5.0 % up time measured on a monthly basis	4
				< 98% up time measured on a monthly basis	6
4	Availability of the following solutions / applications: - Nirbhaya Portal	Uptime = {1 - (Application downtime- maintenance downtime) / (Total Time – maintenance downtime) } Measurement Tool: Reports from EMS/CMP	Monthly	Minimum 99.5% up time measured on a monthly basis	-

Cloud Data Centre Application and Components					
S. No.	**Definition**	**Measurement**	**Measurement Interval**	**Target**	**Severity Level**
				>= 98.0% to <99.5.0 % up time measured on a monthly basis	2
				>=96% but < 98% up time measured on a monthly basis	4
				<96% uptime measured on the monthly basis	6
5	Availability of the following solutions / applications: - BI Reporting & Analytics	Uptime = {1 - (Application downtime- maintenance downtime) / (Total Time – maintenance downtime) } Measurement Tool: Reports from EMS/CMP	Monthly	Minimum 95% up time measured on a monthly basis	-
				>= 92% to <95% up time measured on a monthly basis	2

Cloud Data Centre Application and Components

S. No.	Definition	Measurement	Measurement Interval	Target	Severity Level
				>=90% but < 92% up time measured on a monthly basis	4
				<90% uptime measured on the monthly basis	5
6	Availability of the following solutions / applications: - Email solution - eLearning - SMS	Uptime = {1 - (Application downtime- maintenance downtime) / (Total Time – maintenance downtime) } Measurement Tool: Reports from EMS/CMP	Monthly	Minimum 95% up time measured on a monthly basis	-
				>= 92% to <95% up time measured on a monthly basis	2
				>=90% but < 92% up time measured on a monthly basis	4

Cloud Data Centre Application and Components

S. No.	Definition	Measurement	Measurement Interval	Target	Severity Level
				<90% uptime measured on the monthly basis	5
7	SMS Delivery	95% Outgoing SMS should be delivered in 15 seconds. Measurement tool : EMS/CMP	Monthly	<=15 Sec.	-
				>15 sec. but <=30 sec.	4
				> 30 Sec.	5
8	SMS Gateway Uptime	Both incoming and outgoing SMS uptime should be >99%	Monthly	>=99%	-
				>=98% to <99%	4
				<98%	5
9	Availability of event Log solution	Uptime = {1 - [(Event Log downtime) / (Total Time – Maintenance Downtime)]} Total Time shall be measured on 24*7 basis. Downtime shall be measured from the time the Event Log becomes unavailable (due to any reasons whatsoever attributable to the Bidder) for the user to the time it becomes fully available. Further any downtime for maintenance during the 24*7 timeframe shall be with prior written intimation to the Purchaser	Monthly	Minimum 98 % up time measured on a monthly basis	-
				>= 97.0% to <98.0% up time measured on a monthly basis	4
				>= 96.0% to <97.0% up time measured on a monthly basis	5
				>= 95.0% to <96.0% up time measured on a monthly basis	6

Cloud Data Centre Application and Components					
S. No.	**Definition**	**Measurement**	**Measurement Interval**	**Target**	**Severity Level**
		Measurement Tool: Reports from EMS/CMP		<95.0% up time measured on a monthly basis	7
10	Replication System	**Metric:** % of Uptime for Replication System **Formula:** Uptime % = {1-[(Total Downtime) / (Total Time – Planned Downtime)]} *100 Replication System is used to maintain synchronous/ asynchronous update between primary data Centres. The service is expected to be available 24 x 7. Availability of Replication System is determined by components of Replication System like Replication Server and Replication Software **Total Downtime -** Total cumulative time the Replication Networks are NOT available. **Planned Downtime** -Total maintenance time as defined and agreed upon by MSP and Purchaser. **Total Time** - 24 X 7 measured over a period of month.	Monthly	>= 99.95 % up time measured on a Monthly basis	0
				>= 98.0% to <99.5.0% up time measured on a monthly basis	4
				>= 96.0% to <98.0% up time measured on a monthly basis	5
				<96% up time measured on a monthly basis	7
11	All Security appliance Uptime like firewall, NIPS, Anti APT and other security equipment's / appliance installed in the respective DCs	Uptime % = {1-[(Total Downtime) / (Total Time – Planned Downtime)]} *100 Measurement Tool: Reports from EMS	Monthly	> = 99.5%	-
				>= 99.4% but < 99.5%	5
				< 99.4 %	6

Cloud Data Centre Application and Components					
S. No.	**Definition**	**Measurement**	**Measurement Interval**	**Target**	**Severity Level**
12	Storage Availability	Any downtime for maintenance shall be with prior written intimation to the Purchaser. Measurement Tool: Reports from EMS/CMP	Monthly	Minimum 99.5% up time	-
				>= 90.0% to<99.5.0 % up time	2
				>=80% but < 90% up time	4
				<80% but more than 50% uptime	5
13	Average CPU Utilization for each server and virtual machine at DCs Sites or states	Average CPU utilization of each server should not be more than 50% is the criteria for default. Measurement Tool: Reports from EMS/CMP	Monthly	<=50%	-
				>50 % to <=60%	4
				>60%	5
14	Routing of voice calls to States	Voice call routing latency should not be more than 200 milliseconds (ms).This should be from caller to call agent. Measurement Tool: Reports from EMS/NMS/CMP	Monthly	<= 200 ms.	-
				>200 but <=250 ms.	4
				>250 ms.	6
15	Voice Calls Drop frequency	Voice calls should not drop more than 1% of overall calls Measurement Tool: Reports from EMS/NMS/CMP	Monthly	<=1%	-
				>1% to <=2%	4

Cloud Data Centre Application and Components					
S. No.	Definition	Measurement	Measurement Interval	Target	Severity Level
				>2%	5

b. IT infrastructure at State Call Center and Operations Center

IT Infrastructure at State Call Centre And Operations Centre					
S. No.	**Measurement**	**Definition**	**Measurement Interval**	**Target**	**Severity Level**
Availability – Uptime					
1	Availability of equipment at State Call Centres and Operations Centre equipment: - Routers - Switches	Uptime = {1 - (Equipment downtime-maintenance downtime) / (Total Time – maintenance downtime) } Measurement Tool: Reports from EMS	Monthly	Minimum 99.5% up time	-
				>= 98.0% to <99.5.0 % up time	5
				<98.0% up time	7
2	Availability of equipment at State call Centres and Operation Centre equipment: - IP Phones - Workstations / Desktops	All equipment's should be available 24*7 and any complaint should be resolved within 2 hrs. Equipment should be replaced or repaired after complaint logging from Purchaser officials with 24X7 support Measurement Tool: System generated incident log at Helpdesk / EMS	Daily	Within 2 hours of logging complaint	-
				>2 to <=8 hours of logging complaint	4
				More than 1 day of logging complaint	6
3	Availability of State call Centres and Operation Centre for service delivery	Uptime = {1 - (Equipment downtime-maintenance downtime) / (Total Time – maintenance downtime) } Measurement Tool: EMS	Daily	Minimum 99.5% up time	-
				>= 98.0% to <99.5.0 % up time	6

IT Infrastructure at State Call Centre And Operations Centre					
S. No.	**Measurement**	**Definition**	**Measurement Interval**	**Target**	**Severity Level**
		Reports		<98.0% up time	8
4	Availability of MDT (including applications on MDT)	All MDTs should be available 24*7 and any complaint should be resolved within 4 hrs. 98% of complaints should be resolved within 4 hours Equipment should be replaced or repaired after complaint logging from Purchaser officials. The MDT should be made available for repair/replacement at State Capital / Zonal level. Measurement Tool: System generated Incident log at Helpdesk / EMS	Monthly	>=98% of complaints resolved within 4 hours	-
				>= 95% and <98% of complaints resolved within 4 hours	5
				<95% of complaints resolved within 4 hours	6
5	Availability of equipment at Operations Centre: - Video Walls - Security equipment (Access control, CCTV etc.)	Measurement Tool: Reports from EMS	Monthly	Minimum 97% up time	-
				>= 95.0% to <97.0 % up time	4
				<95.0% up time	5

IT Infrastructure at State Call Centre And Operations Centre					
S. No.	**Measurement**	**Definition**	**Measurement Interval**	**Target**	**Severity Level**
6	UPS Power supply in each state call center and operation center	Supply of power to all IT equipment and call center , operations center through secondary source (Primary source being supplied by respective authority) Measurement Tool: SLA Monitoring EMS tool	Monthly	>= 30 Minutes	-
				< 30 Minutes	5

c. Network

Network					
S. No.	**Measurement**	**Definition**	**Measurement Interval**	**Target**	**Severity Level**
1	Network Availability between State call Centre, Operations Centre and cloud enabled DCs	Network availability for a month is defined as total time (in minutes) in a month less total down time (in minutes) in a month excluding planned network downtime. The network is considered available when all the services in full capacity are available Network Availability (%) = (Total minutes during the month – Planned downtime - Downtime minutes during the month) *100 / Total minutes during the month	Monthly	>=99.5%	-
				<= 99.5% to >98.0% up time	4
				<= 98.0% to >96.0% up time	5
				<= 96.0% to >95.0% up time	6
				<95.0% up time	7

Network					
S. No.	**Measurement**	**Definition**	**Measurement Interval**	**Target**	**Severity Level**
2	Replication Network between Cloud enabled DCs	**Metric:** % of Uptime for Replication Network **Formula:** Uptime % = {1-[(Total Downtime) / (Total Time – Planned Downtime)]} *100 Replication Network is used to connect DCs and is expected to available 24 x 7. **Total Downtime -** Total cumulative time the Replication Networks are NOT available. **Planned Downtime** -Total maintenance time as defined and agreed upon by ITSP and Purchaser. **Total Time -** 24 X 7 measured over a period of month.	Monthly	>= 99.95 % up time	0
				< 99.95 % up time	4
3	Network Quality of Service	Quality of Service (QoS) refers to the capability of a network to provide traffic engineering to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter, latency and improved loss characteristics. Measurement Tool: Reports from NMS/EMS	Hourly	99% throughput of minimum stipulated bandwidth during 24*7 hours	-
				>=97% and <99% throughput of minimum stipulated bandwidth during 24*7 hours	5
				<97% throughput of minimum stipulated bandwidth during 24*7 hours	6
				Average Packet loss exceeding 0.5% over a month (at Data Centre and WAN level)	4

Network					
S. No.	**Measurement**	**Definition**	**Measurement Interval**	**Target**	**Severity Level**
				Latency Delay > 150 ms (every instance) (at Data Centre and WAN level)	4
4	Network Bandwidth Utilization between two cloud DCs, States, Operations centers sites including internet	Average Network Bandwidth utilization should be less than 60% criteria for default. Measurement Tool: Reports from EMS	Monthly	<=60%	-
				>60 % to <=70%	3
				>70%	6

d. Manpower Availability

Manpower Availability					
#	**Measurement**	**Definition**	**Measurement Interval**	**Target**	**Severity Level**
Manpower Availability					
1	Replacement of key personnel (refer clause 10.2 of section 5)	The Bidder is expected to keep the key personnel for at least 18 months at the respective location.	Quarterly	> 18 Months for each key resource personnel	Penalty = 3* Monthly Unit Rate (for each replacement)
2	Availability of all Manpower resources at designated location as per requirement defined in section 5 of the RFP	[(Actual number of man-days deployed for a month) / (Agreed Total number of man-days in a month)] *100	Monthly	>= 95%	-
				>=90 % to < 95%	2

Manpower Availability					
#	**Measurement**	**Definition**	**Measurement Interval**	**Target**	**Severity Level**
				< 90 %	4

e. Audit

Audit					
#	**Measurement**	**Definition**	**Measurement Interval**	**Target**	**Severity Level**
Audit					
1	Implementation of recommendations of audit and Risk Assessment	Implementation of recommendations given by the auditor/ Assessor and which have been agreed upon to be implemented by the Bidder and Purchaser	Monthly	100% on time, for the recommendations agreed upon with the Purchaser, to be implemented in the said Month	5
2	Outcome of Security Audit	The third party auditor shall rate the performance of the Bidder on Security implementation. The three ratings for the performance shall be: Major NC, Minor NC and Requires Improvement(or similar categories)	Yearly	Major NC	8
				Minor NC	7
				Requires Improvement	4
4	Adherence to Backup Policy agreed by Purchaser	Based on the backup policy agreed by Purchaser	Monthly	< 99% backups taken on time at the Data Centre Sites as per the Purchasers backup policy	5
				< 99% backup restoration testing on time in accordance to the Purchasers backup policy	3

f. Issue Resolution

Issue Resolution					
#	Definition	Measurement	Measurement Interval	Target	Severity Level
1	“Resolution Time” means time taken (after the trouble call has been logged on the IT helpdesk), in resolving (diagnosing, troubleshooting and fixing) or escalating to the second level to respective Vendors, getting the confirmatory details about the same.	**Severity: Critical**	Daily	>= 98% of Issues to be analysed and resolved in 2 hours	-
				>=95 % to < 98% of issues to be analysed and resolved in 2 hours	4
		Show stoppers involving major functional failure in the application. There are no usable workarounds available to troubleshoot the problem. Affects majority of the users (more than 25%).		>=90 % to < 95% of issues to be analysed and resolved in 2 hours	5
				< 90 % of issues to be analysed and resolved in 2 hours	6
2	“Resolution Time” means time taken (after the trouble call has been logged on the IT helpdesk), in resolving (diagnosing, troubleshooting and fixing) or escalating to the second level to respective Vendors, getting the confirmatory details about the same.	**Severity: High**	Daily	>= 98% of issues to be analysed and resolved in 4 hours	-
		Users face severe functional restrictions in the application irrespective of the cause. Workarounds are time consuming. Affects majority of the users (more than 25%).		>=95 % to < 98% of issues to be analysed and resolved in 4 hours	3
				>=90 % to < 95% of issues to be analysed and resolved in 4 hours	4
				< 90 % of issues to be analysed and resolved in 4 hours	5
3	“Resolution Time” means	**Severity: Moderate**	Daily	>= 98% of issues to be analysed and	-

Issue Resolution

#	Definition	Measurement	Measurement Interval	Target	Severity Level
	time taken (after the trouble call has been logged on the IT helpdesk), in resolving (diagnosing, troubleshooting and fixing) or escalating to the second level to respective Vendors, getting the confirmatory details about the same.			resolved in 6 hours	
				>=95 % to < 98% of issues to be analysed and resolved in 6 hours	2
		Moderate functional restrictions in the application irrespective of the cause. Has a convenient and readily available workaround. Affects a few users		>=90 % to < 95% of issues to be analysed and resolved in 6 hours	3
				< 90 % of issues to be analysed and resolved in 6 hours	4
4	“Resolution Time” means time taken (after the trouble call has been logged on the IT helpdesk), in resolving (diagnosing, troubleshooting and fixing) or escalating to the second level to respective Vendors, getting the confirmatory details about the same.	**Severity: Low**	Daily	>= 98% of issues to be analysed and resolved in 8 hours	-
		Requiring cosmetic functional changes. Does not require any workaround. It may include user query / suggestions but has no business impact.		>=95 % to < 98% of issues to be analysed and resolved in 8 hours	1
				>=90 % to < 95% of issues to be analysed and resolved in 8 hours	2
				< 90 % of issues to be analysed and resolved in 8 hours	3

g. Others

Issue Resolution					
#	Definition	Measurement	Measurement Interval	Target	Severity Level
1	Generation of SLA reports from EMS system	All reports should be generated from EMS. No manual reports would be acceptable to the Purchaser.	Weekly	100% from EMS.	-
				<100%	3
2	Submission of technology refresh report and annual security audit	Technology refresh and security audit report should be submitted timely as per Clause 13 of Section 5	As per Clause 13 of Section 5	On time submission as per Clause 13 of section 5	-
				Delay of every week	2

39.3. Operations Centre

All events must be monitored and all incidents should be analyzed/reported and resolved on a 24x7 basis.
Security event management should be covered completely but not limited to:

1. Virus/Malware outbreak
2. Phishing attacks
3. Reconnaissance attacks
4. Application/Website monitoring
5. Data Leak/Loss incidents
6. Customer account related incidents
7. Customer inquiries.

Validate the incident with the guidelines provided and exclude if it is a false positive. Priority is the level of response time identified when the incident ticket is created or updated based on the degree of the impact.

No.	Measurement	Definition	Target	Severity Level

No.	Measurement	Definition	Target	Severity Level
1	**Incident Reporting**	Any failure/incident on any part of the solution shall be communicated immediately to MHA as an incident report giving details of impact, if any. Monthly measurement.	100% incidents to be reported to MHA within 1 hour with action for the incident.	No Penalty
			Delay beyond every hour a cumulative penalty to be imposed on an hourly basis subject to a maximum value of severity 8 per incident.	6
			100% incident log to be submitted to MHA that comprises exceptional & normal reportable activities by 5th of every Quarter for the previous quarter.	No Penalty
			Delay beyond the date of submission	6
2	**Change Management**	Measurement of quality and timeliness of changes to the solution. Monthly measurement	100% of changes should follow formal change control procedures. All changes need to be approved by MHA.	No Penalty
			For every instance of change management policy violation.	6
3	**DR Drill**	Bidder shall adhere to the DR Policy agreed by Purchaser and conduct DR Drills. Half yearly measurement.	100% of the time the drill should happen as per schedule and as per request of MHA.	No Penalty
			For any violation of the DR policy.	6
4.	Vulnerability Assessment	Authenticated Mode Assessment should be done for all assets on a monthly basis. The	100% coverage of assets.	No Penalty.

No.	Measurement	Definition	Target	Severity Level
		report to be submitted to MHA by 5th of next month	For any non-compliance with the SLA target.	7
		High severity issues to be closed within 7 days of issue of report.	100% coverage of assets as per respective VA report for that month.	No Penalty.
			For any non-compliance with the SLA target.	7
		Medium severity issues to be closed within the same month of issue of report.	100% coverage of assets as per respective VA report for that month.	No Penalty.
			For any non-compliance with the SLA target.	7
5.	Penetration testing	The Penetration Testing of all the public facing assets and services has to be done by the bidder 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 MHA by 5th of the month following the quarter.	100% coverage of assets as per respective PT report for that month.	No Penalty.
			For any non-compliance with the SLA target.	7
		High severity issues to be closed within 7 days of issue of report.	100% coverage of assets as per respective PT report for that month.	No Penalty.
			For any non-compliance with the SLA target.	7
		Medium severity issues to be closed within the same month of issue of report.	100% coverage of assets as per respective PT report for that month.	No Penalty.
			For any non-compliance with the SLA target.	7

No.	Measurement	Definition	Target	Severity Level
6.	**Patch management**	The patches to be installed on the systems in case a patch is released by the OEM or a flaw is identified due to an internal or external assessment by bidder or MHA. High severity patches to be tested and installed within 7 days of issue of patch.	100% coverage of assets	No Penalty.
			For any non-compliance with the SLA target.	7
		Medium severity patches to be installed within 30 days of issue of patch.	100% coverage of assets	No Penalty.
			For any non-compliance with the SLA target.	7
7.	**Event Source Coverage**	The events of all the ICT assets have to be captured by the event logger. Weekly measurement.	100% coverage of assets	No Penalty.
			For any non-compliance with the SLA target.	7

39.4. **Footnotes**

39.4.1. Working days = All days including Sundays and Public Holidays are working days.

39.4.2. 24*7 means three shifts of 8 hours every day, for all seven days of the week, without any Non-working days

39.4.3. If the measurement interval is not defined then measurement interval should be taken as monthly.

40. Reporting Procedures

40.1. The Bidder representative will prepare and distribute Service level performance reports generated from EMS in a mutually agreed format by the **5th working day of subsequent month**. The reports will include **"actual versus target"** Service Level Performance, a variance analysis and discussion of appropriate issues or significant events. Performance reports will be distributed to Purchaser management personnel as directed by Purchaser.

40.2. Also, the Bidder may be required to get the Service Level performance report audited by a third-party Auditor appointed by the Purchaser.

41. Penalties

41.1. **General**

41.1.1. A maximum level of performance penalties is established and described below.

41.1.2. The framework for performance penalties as a result of not meeting the Service Level Targets are detailed below:

41.1.3. Penalty calculation would be calculated on VALUE1 + VALUE2.

CAPEX – All cost related to applications at center and hardware at states

VALUE1 – The actual quarterly manpower + Annual Maintenance cost + Cloud Services (Virtual machine and storage and contact center) + Network cost

VALUE2 - 25% of the all CAPEX POs issued in the applicable quarter divided by number of remaining quarter + VALUE2 from previous quarter

For third quarter only (i.e. First quarter in which SLA penalty will be levied), VALUE2 will be defined as follows.

VALUE2 = 25% of all CAPEX POs issued till the end of the third quarter divided by 17.

41.1.4. No SLA/ penalty would be levied on Bidder for first 6 months

41.1.5. Performance penalties shall be levied for not meeting each of the severity levels of performance as per the following table:

Severity Level	Penalty as a percentage of Quarterly value applicable (Refer clause 41.1.3)
9	Event of default and termination as per Clause 29 and 31 of this section of RFP respectively and the consequences as provided in Clause 32 of this section of RFP
8	6.0 %
7	4.0 %
6	2.0 %
5	1.0 %
4	0.5 %
3	0.4 %
2	0.3 %
1	0.2 %

41.2. If a measurement parameter is not met in more than one month in a quarter, the penalty percentage will be aggregated for these months.

41.3. Performance Penalty Percentage for not meeting a measurement parameter for two consecutive quarters shall result in twice the aggregated penalty percentage of that respective measurement parameter in the applicable quarter.

41.4. Maximum Penalty Percentage applicable in a quarter shall not exceed 20%.

41.5. Two consecutive quarterly penalty of 20 % will be deemed to be an event of default and termination as per Clause 29 and 31 of this Section of RFP respectively and the consequences as provided in Clause 32 of this section of RFP shall follow.

42. Issue Management Procedures

42.1. **General**

42.1.1. 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 Purchaser and Bidder.

42.1.2. 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.

42.2. **Issue Management Process**

42.2.1. Either Purchaser or the Bidder may raise an issue by documenting the business or technical problem, which presents a reasonably objective summary of both points of view and identifies specific points of disagreement with possible solutions.

42.2.2. Any unresolved issues/disputes concerning the Project/Contract between the Parties will first be referred in writing to the Project Manager for his consideration and resolution. If the Project Manager is unable to resolve any issue/dispute within 5 days of reference to them, the Project Manager will refer the matter to the Program Management Committee. If the Program Management Committee is unable to resolve the issues/disputes referred to them within 15 days the unresolved issue/dispute will be referred to Steering Committee for resolution. The Steering Committee within 30 days of reference to them shall try to resolve the issue/dispute.

42.2.3. If the steering committee failed to resolve the issue as per above clause, the same shall be referred to empowered committee.

42.2.4. If the Empowered Committee fails to resolve a dispute as per the above clause, the same shall be referred to arbitration. The arbitration proceedings shall be carried out as per the Arbitration procedures mentioned in Clause 16 of this section of RFP.

43. Service Level Change Control

43.1. **General**

It is acknowledged that this **Service levels may change as Purchaser's business needs evolve over the course of the contract period**. As such, this document also defines the following management procedures:

43.1.1. A process for negotiating changes to the Service Levels

43.1.2. An issue management process for documenting and resolving particularly difficult issues.

43.1.3. Purchaser and Bidder 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.

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. All SLA changes have to be approved by the purchaser authorized committee to be notified later.

43.2. **Maturity of SLA**: The service levels should mature as the project stabilizes and matures. Annual review of SLA should be taken up by the Bidder and suggest new SLA based on improved system. Maturity of SLA would be governed by Steering Committee and would be updated mutually by Purchaser and Bidder.

43.3. **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 Bidder's representative will maintain and distribute current copies of the Service Level document as directed by Purchaser. Additional copies of the current Service Levels will be available at all times to authorized parties.

43.4. **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.

44. Exit Management Plan

44.1. An Exit Management plan shall be furnished by Bidder in writing to the Purchaser before 180 days from the end of the 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 Pilot site Implementation, and Service Level monitoring.

44.1.1. 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;

44.1.2. Plans for provision of contingent support to Project and Replacement Service Provider for a reasonable period after transfer.

44.1.3. Exit Management plan in case of normal termination of Contract period

44.1.4. Exit Management plan in case of any eventuality due to which Project is terminated before the contract period.

44.1.5. Exit Management plan in case of termination of the Bidder

44.2. Exit Management plan at the minimum adhere to the following:

44.2.1. Three (3) months of the support to Replacement Service Provider post termination of the Contract

44.2.2. Complete handover of the sources codes, reports, documents and other relevant items to the Replacement Service Provider

44.2.3. Certificate of Acceptance from authorized representative of Replacement Service Provider issued to the Bidder on successful completion of handover and knowledge transfer

44.3. During the exit management period, the Bidder shall use its best efforts to deliver the services.

D. ANNEXURES

Annex I: Form of Agreement

THIS Agreement made the …………date of…………2015.., between…………….(hereinafter…….referred to as the “Bidder”) of the one part and …Ministry of Home Affairs (Hereinafter called the “Purchaser”) of the other part.

WHEREAS the Bidder is about to perform services as specified in this RFP …………………..(hereinafter called “works”) mentioned, enumerated or referred to in certain Contract conditions, specification, scope of work, other sections of the RFP, covering letter and schedule of prices which, for the purpose of identification, have been signed by ………………. on behalf of the ………….. Bidder and ……….(the Purchaser) on behalf of the Purchaser and all of which are deemed to form part of the Contract as though separately set out herein and are included in the expression “Contract” whenever herein used.

NOW, THEREFORE, IT IS HEREBY AGREED between the parties as follows:

a. The Purchaser has accepted the tender of the 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 Purchaser, 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	*Section 1,2,3,4,5, 5A and5B of the RFP*
Pre Bid Clarification	*To be Issued later by the Purchaser*
Break-up of cost components	*Bidder’s Commercial Proposal*
The Purchaser’s Letter of Intent dated <<>>	*To be issued later by the Purchaser*
The Bidder’s Letter of acceptance dated <<>>	*To be issued later by the Purchaser*
Bid submitted by the Bidder as per file No. <<>>	

d. The mutual rights and obligations of the “Purchaser” and the Bidder shall be as set forth in the Agreement, in particular:

- the Bidder shall carry out and complete the Services in accordance with the provisions of the Agreement; and
- the “Purchaser” shall make payments to the Bidder in accordance with the provisions of the 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 Bidder by the Purchaser as hereinafter mentioned, the 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 Purchaser will pay to the Bidder the said sum of ……………………or such other sums as may become payable to the 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	:

Annex II: Payment Milestones

The payment milestones have been divided in 3 parts. The detail of each part is provided below. It should be noted that MHA reserves the right to issue Purchase Order of lesser value than provided in the RFP. All payments would be made on quarterly basis and would be based on actual utilization of cloud services, network cost by the Purchaser, irrespective of value mentioned in RFP or Purchase Order.

1. Software at Cloud Data Centre and Hardware at Operations Centre

   Capital expenditure (CAPEX1) made in setting up of Software at Data center and hardware at Operations Centre would be paid under this category. The cost of all the components required for Data Centre and Operations Centre should be provided by the Bidder in Section 4. For each PO issued by the Purchaser following payment plan would apply.

S. No.	Milestone	Payment
1.	Supply, commissioning and testing of hardware and asset entry in the Asset Manager	15% of CAPEX1
2.	Functional and Integration testing of entire system including hardware, software, network and other components	10% of CAPEX1
3.	Go-Live at cloud DC1, DC2, Operations Centre and 2 States	50% of CAPEX1
4.	Go-Live + 6 months	25% of CAPEX1

2. State Call Centre

   Capital expenditure (CAPEX2) made in setting up of State Call Centre would be paid under this category. It should be noted that the demand of hardware, application licenses would depend on the State requirement. Payments under this category would be made on the basis of actual procurement made by the States.

S. No.	Milestone	Payment
1.	Supply, commissioning and testing of hardware including MDT and asset entry in the Asset Manager	20% of CAPEX2
2.	Go-Live of the State	40% of CAPEX2
3.	Stabilization Period (Go-Live + 6 months)	15% of CAPEX2
4.	After Go-Live + 6 Months - Equated quarterly for remaining quarters	25% of CAPEX2

3. Manpower + AMC + Cloud Services + Network Costs

   This would include Manpower cost + AMC of actual deployed hardware & application as well as cost for Cloud Services and Network Costs for all connected sites. Annual maintenance payment, license & support cost for any hardware/ application component would start after one year of deployment. (First year would be provided free)

S. No.	Milestone	Payment
1.	Manpower, license and annual maintenance of operations centre, state call centre and MDT	Quarterly payment of the actual operational cost calculated on basis of per unit cost of actual deployment.
2.	Maintenance of Network bandwidth between all sites (DC, operations centre, State Call Centre)	Quarterly payment of the actual bandwidth charges
3.	Utilization of cloud services	Quarterly payment of actual cloud services usage

MINISTRY OF HOME AFFAIRS

(Center State Division, Govt. Of India)

Tender No.: 15011/38/2013-SC/ST-W **26 June 2015**

Request for Proposal

For

“Selection of IT Service Provider for Nationwide Emergency Response System”

Section 4
Bid submission formats

Issued by:

Ministry Of Home Affairs – CS Division, 5th Floor, NDCC-II Building, Jai Singh Road,
New Delhi -110001, India

Table of Contents

1 Technical Formats

1.1 Technical Bid Letter

To
The Director - SR
Ministry Of Home Affairs
5 Floor, NDCC – II building
Jai Singh Road, New Delhi - 110001

Sir,

Sub **Selection of IT Service Provider for Nationwide Emergency Response System**
Ref: RFP No. **<<>> dated << 2015>>**

We, <<name of the undersigned Bidder >>, having read and examined in detail all the bidding documents in respect of selection of IT Service Provider for Nationwide Emergency Response System 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 Purchaser are 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 declare that :

a. We are not currently blacklisted by any government organization in India (Central / State Government or PSU or Local Urban Body - municipalities etc).
b. We have never been declared to be a willful defaulter by any Bank
c. We are applying for the selection in the capacity of an individual firm as the Bidder
d. We or any person on our behalf will not engage in any corrupt, fraudulent or coercive practices to influence the Bidding Process.
e. We hereby acknowledge and unconditionally accept that the Purchaser can at its absolute discretion apply whatever criteria it deems appropriate, not just limiting to those criteria set out in the RFP and related documents, in short listing of IT service provider for providing services.
f. We have enclosed a **Bank Guarantee for Rs. 10,00,00,000 (Rs. Ten crores only) and Demand Draft of Rs 25,000/- (Rs. Twenty five thousand only)** in favour of **'DDO, Ministry of Home Affairs" payable at New Delhi'**.

g. We hereby declare that all information and details furnished by us in the Proposal are true and correct, and all documents accompanying such application are true copies of their respective originals.
h. We have carefully read and understood the terms and conditions of the RFP and the conditions of the contract applicable to the RFP. We do hereby undertake to provision as per these terms and conditions.
i. In the event of acceptance of our bid, we do hereby undertake-
    i. To supply the products and commence services as stipulated in the schedule of delivery forming a part of the attached proposal.
    ii. To undertake the project services for a period of 5 years from the date of signing of the contract.
    iii. We affirm that the prices quoted are inclusive of delivery, installation, commissioning, training and providing facility management, and inclusive of all out of pocket expenses, taxes, levies discounts etc.
    iv. We shall submit the contract Performance bank guarantee in the form prescribed at Clause 3.1 of Section 4 of the RFP
j. We do hereby undertake, that, until a formal contract is prepared and executed, this proposal, together with your written acceptance thereof and notification of award of contract, shall constitute a binding contract between us.
k. We understand that the bank guarantee furnished by us as Earnest Money Deposit may be encashed under conditions enumerated in Section 2 of the RFP

We understand that the Purchaser may cancel the bidding process at any time and that Purchaser is not bound to accept any bid that it may receive without incurring any liability towards the bidder.

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.

This proposal is valid for 120 days from the date of submission of bid. We shall extend the validity of the bid if required by MHA.

Thanking you,

Yours sincerely,

(Signature of the authorized signatory of the Bidder)

Printed Name
Designation
Seal
Date:
Place:
Business Address:

1.2 Company Profile

A. Brief company profile

SN	Particulars	Description/ 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
Provide the Certificate of Incorporation of the company.

C. Financial Turnover
The financial turnover of the company is provided as follows:

	2011 – 12	2012 – 13	2013 – 14
Annual Turnover			
Networth	[redacted]	[redacted]	

Copy of audited financial statements or declaration from the appointed statutory auditor to be provided as proof of the financial turnover

D. Certifications
Provide copy of valid certification for SEI CMM /CMMi maturity Level 5, ISO 27001 or ISO 9001.

1.3 Prior Experience

1.3.1 Credential Summary

#	Project Name	Client Name and type*	Project Value (in INR)	Project Components**
1				
2				
3				
4				
5				
6				
7				

* Client type – Indicate whether the client is Government / PSU / Private

** Project Components – Indicate the major project components like, setting up of Case record management application, contact centre., Application development, Maintenance, Hardware procurement and deployment, DC setup and maintenance, Facility management services, IT support and maintenance

Please provide documentary evidence as required.

1.3.2 Credential Format

Bidders are requested to furnish the credentials in the following format. All credentials should be followed by relevant documentary proof.

Name of the Work & Location	
Client's Name and Complete Address	
Scope of work carried out by the Applicant	
Contract Value for the bidder (in INR) (mandatory)	
Contract value of whole project (in INR) (mandatory)	
Date of Start (mandatory)	
Date of Completion (for ongoing project, provide the last completed deliverable)	
Details of the project as per the below mentioned header **A. Operations Center Setup** **B. Call center setup**	

C. CRM **D. GIS** **E. Location based service software (LBS)** **F. Cloud Data Center** **G. MDT devices installation** **H. Other details**	

1.4 Overview of Proposed Solution

1.4.1 Structure of proposed solution

Please provide approach & methodology to execute the entire project as per the following illustrative headers. Bidders are advised to comply with the scope of work mentioned in Section 5 and below provided header while detailing out their solution.

S. No.	Item
1.	**Overall solution** • Overall solution architecture of the Nationwide Emergency Response System • Integration with other systems, roll out plan etc. • Enhancement of solution • Options for centralized v/s state level PRI lines
2.	**Operation Centre and State Call Centre** • Setting up of Operations Centre and States Call Centres • Gateway, router, PoE switches and Leased line etc. • Provisioning software like Reporting, Anti-Virus, Outbound dialler, Operating System, CRM, Supervisor application, voice recording software, CLI, ACD etc. • Provisioning hardware at Operations Centre and States Call Centre like desktop, laser printers, IP phone and mobile data terminal etc. • Network connectivity • At Operations Centre, solution for space for NOC/ SOC, video wall, Furniture and furnishing, Visitor's gallery and Support Manpower • Integration with other applications, existing Dial 100 etc. • PRI lines (Can be at center or state as per SI designs)
3.	**Cloud Data Centre** • Overall solution • Application (IP PBX, Media gateway, voice recording, CRM, ACD, CTI, Identity Management, EMS, Location based service etc.) • GIS (Map data and POI data) • PRI lines (Can be at center or state as per SI designs) • Network connectivity
4.	**Network** • Overall solution • Setting up network switches, routers, gateways in Operations Centre, State Call Centre and Data Centre • Providing redundant connectivity through reliable media to DC sites, Operations Center and State Call Centre
5.	**Field** • Mobile data terminals for the vehicles • Applications, data input and output form MDT devices
6.	**Manpower Deployment** • Detailed plan of the resources to be deployed

S. No.	Item
7.	**Project implementation plan** • Understanding of Project Requirements • Project Plan: Completeness of the proposed project plan with proper Timelines, Responsibility Matrix etc. • Project Management Methodology for Implementation Phase: o Quality of Project Management Methodology o Strategy to meet implementation timelines o Solution deployment strategy • Operations and maintenance plan: o Strategy to maintain and improve all the SLAs o Approach and Plan for issue resolution, helpdesk etc. o Strategy for Disaster management • Technology refresh plan o Plan for technology refresh and reducing total cost of ownership during the contract period

1.4.2 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							
S. No.	**Item of Activity**	**Month wise Program**					
		1	2	3	4	5	…n
	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 & phase wise timelines for executing the project with details of deliverables & milestones as per their understanding of project and project proposal							

1.4.3 Manpower Plan

Manpower distribution							
S. No.	**Manpower**	**Week wise time to be spent by each personnel (full time/ part time to be highlighted with actual time spent)**					
		1	2	3	4	5	…n
1.	Project Director						
2.	Project Manager						
3.	Solution Architect (Cloud expert)						
4.	Solution Architect (Applications)						
5.	Solution Architect (Network)						
6.	Solution Architect (Information Security)						
7.	Database Architect/ Modeller						
8.	Database Administrator						
9.	System Administrator						
10.	Network Administrator						
11.	GIS Expert (from OEM)						
12.	CRM Centre specialist (from OEM)						
13.	Master Trainer						
14.	Others (as per RFP and bidder plan)						
Note: Above representation is illustrative. Bidders are requested to provide detailed manpower distribution with clearly stating part time/ full time deployment and other details as per their proposal. Bidder should refer to Manpower of section 5 and ensure all resource/requirement are met.Bidder may add more rows for adding more resources.							

1.4.4 Software Requirement specification

In addition to the above requirements, provide filled in Software Requirement Specification (Section 5A) as part of the overall solution details.

1.4.5 Technical Requirement specification

Bidder should provide filled in Technical Requirement Specification (Section 5B) as part of the overall solution details.

1.5 Details of Manpower Resource

Note: For all proposed resources (refer Caluse 10, Section 5), it is mandatory to provide name of proposed key personnel along with details desired as per format given below. It is also informed that the Purchaser would interview the resources suggested by the bidders before their deployment on board.

S.No.	Name of the Resource	Proposed Role	Higher Qualification	Basic Qualification (E.g. B.E./ B.Tech/ MBA etc.)	Certifications (e.g. PMI/ ITIL/ TOGAF)	Number of projects in Emergency Response System/ CAD / CRM/ Contact Centre etc.	Total Experience (in years)
1.							
2.							
3.							

<table>
<tr><th>1</th><th colspan="2">Name:</th></tr>
<tr><td>1.</td><td><b>Proposed position / role</b></td><td><i>(only one candidate shall be nominated for each position)</i></td></tr>
<tr><td>2.</td><td><b>Date of Birth</b></td><td>DD-MM-YYYY | <b>Nationality</b> |</td></tr>
<tr><td>3.</td><td><b>Education</b></td><td>
<table>
<tr><th>Qualification</th><th>Name of School/College/University</th><th>Degree Obtained</th><th>Date Attended</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>
</table>
</td></tr>
<tr><td>4.</td><td><b>Years of experience</b></td><td></td></tr>
<tr><td>5.</td><td><b>Areas of Expertise and no. of years of experience in this area</b></td><td><i>(as required for the Profile)</i>
▶</td></tr>
<tr><td>6.</td><td><b>Certifications and Trainings attended</b></td><td>▶</td></tr>
<tr><td>7.</td><td><b>Employment Record</b></td><td>
<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>
[<i>Starting with present position, list in reverse order, giving for each employment: dates of employment, name of employing organization, positions held.</i>]
</td></tr>
<tr><td>8.</td><td><b>Detailed Tasks Assigned</b></td><td><i>(List all tasks to be performed under this project</i>)
▶</td></tr>
<tr><td>9.</td><td colspan="2"><b>Relevant Work Undertaken that Best Illustrates the experience as required for the Role</b><i>)</i></td></tr>
<tr><td colspan="3">
<table>
<tr><th colspan="2">Project No:</th></tr>
<tr><td>Name of assignment</td><td></td></tr>
<tr><td>Year</td><td></td></tr>
<tr><td>Location</td><td></td></tr>
<tr><td>Employer</td><td></td></tr>
<tr><td>Main project features</td><td></td></tr>
<tr><td>Position held</td><td></td></tr>
<tr><td>Activities performed</td><td></td></tr>
</table>
</td></tr>
</table>

1.6 Statement Of Deviations From Schedule Of Requirements

Date: DD MONTH 2015

To
The Director - SR
Ministry Of Home Affairs
5 Floor, NDCC – II building
Jai Singh Road, New Delhi - 110001

Sir,

We are providng the the deviations from the requirements of RFP document **No <<>> dated <<2015>>.** 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.

Deviations in Scope of Work

S. No.	Reference of RFP Volume Number, Clause No. & Page. No	Deviation in the Proposal	Brief Reasons

Deviation in Terms and Conditions

S. No.	Reference of RFP Volume Number, Clause No. & Page. No	Deviation in the Proposal	Brief Reasons

Yours sincerely,

(Signature of the Auhtorized Representative)

Printed Name
Designation

Seal

Place:
Business Address:

1.7 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***.** *Key products for which MAF is required are:*

1. *Core switch, routers and gateways*
2. *Contact Centre application*
3. *CRM*
4. *GIS*
5. *IP phones*
6. *Mobile data terminals*

To,
The Director - SR
Ministry Of Home Affairs
5 Floor, NDCC – II building
Jai Singh Road, New Delhi - 110001

Subject: Manufacturer's Authorization Form

Reference: RFP No: ___________________ Dated: _____________ for Selection of IT service provider for Nationwide Emergency Response System

.

We_________ (Name of the OEM) who are established and reputable manufacturers of ________ (List of Goods) having factories/product development centers at the locations __________/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/developed by us.

We hereby extend, our warranty for the hardware goods supplied by the bidder and/or the maintenance/support services for software products against this invitation for bid by _______________________ (Name of the Bidder)

Thanking you,
Yours faithfully,

(Signature)

For and on behalf of: _________(Name of the OEM)

Authorised Signatory

Name:

Designation:

Place:

Date:

1.8 Declaration of office in India

The declaration should be provided on company letter head signed by duly authorized repsrentative of the company.

To
The Director - SR
Ministry Of Home Affairs
5 Floor, NDCC – II building
Jai Singh Road, New Delhi - 110001

Sir,

This is to certify that we, M/s <Company name>, have our own office in India. Address of our office is <Company office address>. The office was set up in the year <year of office set up>.

Yours sincerely,

(Signature of the Authorized Representative)

Printed Name
Designation

Seal

Date:
Place:
Business Address:

1.9 Declaration of Non-Blacklisting

The declaration should be provided on company letter head signed by duly authorized repsretative of the company.

To
The Director - SR
Ministry Of Home Affairs
5 Floor, NDCC – II building
Jai Singh Road, New Delhi - 110001

Sir,

This is to certify that M/s <Bidder company name> is not currently blacklisted by any Central / State Government (Central/State Government) or under a declaration of ineligibility for corrupt or fraudulent practices as of 31 March 2015.

Yours sincerely,

(Signature of the Authorized Representative)

Printed Name
Designation

Seal

Date:
Place:
Business Address:

1.10 Earnest Money Deposit Form

To
The Director - SR
Ministry Of Home Affairs
5 Floor, NDCC – II building
Jai Singh Road, New Delhi - 110001

Whereas M/s <<Name of Bidder>>, a company incorporated under the <<Act>>, its registered office at …………………………./ (hereinafter called 'the Bidder') has submitted its Proposal dated -------------- for **Selection of IT service provider for Nationwide Emergency Response System** (hereinafter called "the Bid") to **Ministry of Home Affairs (MHA).**

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 MHA (hereinafter called "the Client") in the sum of Rs. 10,00,00,000 (Rupees Ten Crore only) 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 --------------------------2015

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 notification of award of contract

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 <<Date of validity>> and its validity should be extensible to 180 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)

2 Financial Proposal Formats

2.1 Financial Bid Letter

To
The Director - SR
Ministry Of Home Affairs
5 Floor, NDCC – II building
Jai Singh Road, New Delhi - 110001

Sir,

Sub: Selection of IT service provider for Nationwide Emergency Response System

Ref: RFP No. **<<>> dated << 2015>>**

i. We, <<name of the undersigned Bidder >>, having read and examined in detail all the bidding documents in respect to above mentioned RFP do hereby propose to provide our services as specified in the bidding proposal submitted by us.

ii. 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 days from the date of submission of RFP response.

iii. 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 / decrease from the scope of work under the contract.

iv. We declare that our bid prices are for the entire scope of the work as specified in the Scope of Work and bid documents.

v. 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 RFP within 15 days of notification of award.

vi. 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.

vii. 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.

viii. We confirm that no deviations are attached here with this commercial offer.

Thanking you,

Yours sincerely,

(Signature of the authorized signatory of the Bidder)

Printed Name
Designation

Seal

Date:
Place:
Business Address:

2.2 Breakdown of Cost Components

Note:

- Bidder should provide all prices, quantities as per the prescribed format under this Clause. Bidder should not leave any field blank. In case the field is not applicable, Bidder must indicate “0” (Zero) in all such fields.
- Bidder should include all Taxes, Duties and Levies wherever applicable and/or payable in the cost. No separate tax should be mentioned.
- Purchaser reserves the right to ask the Agency to submit proof of payment against any of the taxes, duties, levies indicated.

2.2.1 Summary – Total Project Value

#	Item	Table	Total Value
1	Operation Center and AMC	A	Total – A
2	Software and AMC	B	Total – B
3	State Call Centre and AMC	C	Total – C
4	Manpower	D	Total – D
5	Network	E	Total – E
6	Cloud Services	F	Total - F
7	Others	G	Total - G
	Total Project Value		X

The total project value in numbers is Rupees____

The total project value in words is Rupees____

2.2.2 Table A – Operation Center and AMC

Sr. No.	Description	Unit Rate	No. of Units	Total (Unit Rate * No. of Units) A1	AMC for Year 2 to Year 5 A2	Total (A1+A2)
	Hardware					
1.	Managed Access Switch					
2.	Desktop					
3.	UPS					
4.	Router/MPLS CPE					
5.	Laser Jet Printer					
6.	IP Phones					
7.	Desktops (Thin Clients)					
	Security Operations Center/Network operations center					
8.	Video Wall					
9.	LED TV for Conference Room					
	Physical Infrastructure					
10.	Operations centre space on rental for 2400 Sq ft of space					
11.	Electrical works: * UPS- (N+N)- 10 kVA * I/P and O/P DB, earthing * Lighting,point wiring * Electrical distribution board/panel * HVAC DB					
12.	HVAC - Comfort split air-conditioning system					
13.	Safety and Security * Access Control System * Fire Alarm System * Fire Suppression System * CCTV					
	Others					
	Table A Total					**Total – A**

2.2.3 Table B –Software and AMC

Sr. No.	Description	Unit Rate	No. of Units	Total (Unit rate * No. of Units) B1	AMC for Year 2 to Year 5 B2	Total (B1+B2)
	Software					
1.	Proposed Operating System support					
2.	Linux support for CAD					
3.	E-Learning					
4.	Webinar Software License (At Least 50 resource conference)					
5.	BI, Reporting and Analytics					
6.	Location Detection interface					
7.	Nirbhaya Portal and Intranet Web Portal					
8.	Directory Services License					
9.	Database - Postgre Advanced server 9.4 (64 bit version for Linux) for CAD service provider					
10.	Database license for ITSP					
11.	Enterprise Management Software					
12.	Identity Management (IDM) license					
13.	Email Solution (base License)					
14.	Anti Virus					
15.	SMS Gateway					
16.	GIS Map (Map Data and POI)					
17.	Database Activity Monitoring					
18.	Other software to be deployed..					
19.	VPN User License					
20.	Public IP Address					
	Others			**Total Cost for year1**	**Total cost for Year 2 to Year 5**	
21.	Incoming SMS Charges*		1 crore /year			
22.	Outgoing SMS charges*		2 crore /year			
23.	Outbound calls*		5 crore Minutes /year			
24.	USSD					
	Table B Total					**Total – B**

2.2.4 Table C – State Call Centre and AMC

Sr. No.	Description	Unit Rate	No. of Units	Total (Unit Rate * No. of Units) C1	AMC Rate for Year 2 to Year 5 C2	Total (C1+C2)
	Hardware					
1.	Desktop with 3 monitor (Dispatcher, Supervisor) with wireless headset					
2.	Desktop with Single Monitor (Voice Agent and Non Voice Agent) with wireless headset					
3.	IP phones for each agent desk					
4.	Router/ MPLS CPE					
4.1	10 mbps router					
4.2	50 mbps router					
4.3	200 mbps router					
5.	Managed Access Switch					
5.1	48 Port					
5.2	24 Port					
5.3	16 Port					
6.	UPS for					
6.1	Tier-I states (small)					
6.2	Tier-II states (medium)					
6.3	Tier-III states (large)					
	Software					
7	CRM License					
8	Email Solution web Based client License					
	Mobile Data Terminal					
9	8” Rugged MDT – Vendor 1*		20000			
10	8” Non Rugged MDT – Vendor 1*		20000			
11	8” Non-Rugged MDT – Vendor 2*		20000			
12	5.5’ Non-Rugged MDT – Vendor 1*		20000			
13	5.5’ Non-Rugged MDT – Vendor 2*		20000			

Sr. No.	Description	Unit Rate	No. of Units	Total (Unit Rate * No. of Units) C1	AMC Rate for Year 2 to Year 5 C2	Total (C1+C2)
	Table C Total					**Total – C**

2.2.5 Table D – Manpower

Manpower									
Sr. No.	**Description**	**Unit Rate**	**No. of Units**	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Total**
1.	Project Director								
2.	Project Manager								
3.	Solution Architect (Cloud expert /Virtual Machine expert)								
4.	Solution Architect (Applications)								
5.	Solution Architect (Network)								
6.	Solution Architect (Information Security)								
7.	Database Architect/ Modeler								
8.	Database Administrator for ITSP								
9	Database Administrator for CAD service provider								
10.	System Administrator								
11.	Network Administrator								
12.	GIS Expert (from OEM of the proposed product)								
13.	Case Record Management Expert (from OEM of the proposed product)								
14.	Contact Centre expert								
15.	Application Developers								
16.	BI/Data warehouse specialist								
17.	QA Manager								
18.	Test Analysts								
19.	Master Trainer								
20.	Operaiton Center Manager								
21.	Business Analyst								
22	IT Helpdesk Staff								
23	FMS Staff (India-wide)**								

Manpower									
Sr. No.	Description	Unit Rate	No. of Units	Year 1	Year 2	Year 3	Year 4	Year 5	Total
24	Documentation Specialist								
25	Project Coordinator								
26	Process and Compliance Manager								
27	SOC Analyst								
28	Forensics and RCA Analyst								
29	VAPT Analyst								
30	Geo fencig expert								
31	Media/ Communication manager (Content Manager)								
32	UI/UX designer								
33	Project coordinator								
34	Application developer								
35	Build and Release Manager								
	Others								
36	Any other proposed manpower								
	Table – D								**Total D**

2.2.6 Table E – Network

Table E- Network

#	Location	Description	Bandwidth Requirement (in Mbps)	Yr 1	Yr 2	Yr 3	Yr 4	Yr 5	Total
1	DC1 & DC2 Connectivity	Primary Connectivity							
		Secondary Connectivity							
2	Andaman and Nicobar Islands	Primary Connectivity							
		Secondary Connectivity							
3	Andhra Pradesh	Primary Connectivity							
		Secondary Connectivity							
4	Arunachal Pradesh	Primary Connectivity							
		Secondary Connectivity							
5	Assam	Primary Connectivity							

#	Location	Description	Bandwidth Requirement (in Mbps)	Yr 1	Yr 2	Yr 3	Yr 4	Yr 5	Total
		Secondary Connectivity							
6	Bihar	Primary Connectivity							
		Secondary Connectivity							
7	Chandigarh	Primary Connectivity							
		Secondary Connectivity							
8	Chhattisgarh	Primary Connectivity							
		Secondary Connectivity							
9	Dadra and Nagar Haveli	Primary Connectivity							
		Secondary Connectivity							
10	Daman and Diu	Primary Connectivity							
		Secondary Connectivity							
11	Delhi	Primary Connectivity							
		Secondary Connectivity							
12	Goa	Primary Connectivity							
		Secondary Connectivity							
13	Gujarat	Primary Connectivity							
		Secondary Connectivity							
14	Haryana	Primary Connectivity							
		Secondary Connectivity							
15	Himachal Pradesh	Primary Connectivity							
		Secondary Connectivity							
16	Jammu and Kashmir	Primary Connectivity							
		Secondary Connectivity							
17	Jharkhand	Primary Connectivity							
		Secondary Connectivity							
18	Karnataka	Primary Connectivity							
		Secondary Connectivity							
19	Kerala	Primary Connectivity							
		Secondary Connectivity							
20	Lakshadweep	Primary Connectivity							

#	Location	Description	Bandwidth Requirement (in Mbps)	Yr 1	Yr 2	Yr 3	Yr 4	Yr 5	Total
		Secondary Connectivity							
21	Maharashtra	Primary Connectivity							
		Secondary Connectivity							
22	Manipur	Primary Connectivity							
		Secondary Connectivity							
23	Meghalaya	Primary Connectivity							
		Secondary Connectivity							
24	Mizoram	Primary Connectivity							
		Secondary Connectivity							
25	Madhya Pradesh	Primary Connectivity							
		Secondary Connectivity							
26	Nagaland	Primary Connectivity							
		Secondary Connectivity							
27	Odisha	Primary Connectivity							
		Secondary Connectivity							
28	Puducherry	Primary Connectivity							
		Secondary Connectivity							
29	Punjab	Primary Connectivity							
		Secondary Connectivity							
30	Rajasthan	Primary Connectivity							
		Secondary Connectivity							
31	Sikkim	Primary Connectivity							
		Secondary Connectivity							
32	Tamil Nadu	Primary Connectivity							
		Secondary Connectivity							
33	Tripura	Primary Connectivity							
		Secondary Connectivity							
34	Uttar Pradesh	Primary Connectivity							
		Secondary Connectivity							
35	Uttarakhand	Primary Connectivity							

#	Location	Description	Bandwidth Requirement (in Mbps)	Yr 1	Yr 2	Yr 3	Yr 4	Yr 5	Total
		Secondary Connectivity							
36	West Bengal	Primary Connectivity							
		Secondary Connectivity							
37	Telngana	Primary Connectivity							
		Secondary Connectivity							
38	2 Purchaser office location	Primary Connectivity							
39	Connectivity to GMLC database	Primary connectivity							
		Secondary connectivity							
Table E TOTAL									Total – E

2.2.7 Table F - Cloud Services

Table F1 - Cloud Services for Virtual Machine

Cloud Services for Virtual Machine									
Sr. No.	**Description**	**Unit Rate**	**No. of Units**	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**TOTAL**
1	**Virtual Machine**								
1.A	Grade 1								
1.B	Grade 2								
1.C	Grade 3								
1.D	Grade 4								
1.E	Grade 5 for CAD*		**16**						
1.F	Grade 6 for CAD*		**16**						
1.G	Grade 7 for CAD*		**8**						
Table F1	**TOTAL**								**Total- F1**

Table F2 - Cloud services for storage

Cloud Storage for Services								
Sr. No.	Description	Per TB Cost (A)	Year 1 Total Storage in TB (B)	Year 2 Total Storage in TB (C)	Year 3 Total Storage in TB (D)	Year 4 Total Storage in TB (E)	Year 5 Total Storage in TB (F)	TOTAL A*(B+C+D+E+F)
1	Storage							
2	Backup							
Table F2	TOTAL							Total- F2

Table F3 - Cloud services for Contact Center

Cloud Services for Contact Center				
Sr. No.	Description	Per Agent Rate	No. of Agents	TOTAL
1	Contact center solution*		3350	
Table F3	TOTAL			Total- F3

Table F4 - Cloud services for IVRS

Cloud Services for IVRS				
Sr. No.	Description	Per Port Rate	No. of Ports	TOTAL
1	Cloud services for IVRS		1000	
Table F4	TOTAL			Total- F4

Cloud Data Center Services and Network		
Sr. No.	Description	Total cost
1	Cloud Services for virtual machine	F1
2	Cloud Services for Storage	F2
3	Cloud Services for contact center	F3
4	Cloud Services for IVRS	F4

	Table E Total	**Total F = F1+F2+F3+F4**

2.2.8 Table G - Others

Others									
Sr. No.	**Description**	**Unit Rate**	**No. of Units**	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**TOTAL**
1	PRI Lines Primary and Secondary								
2	Voice Gateway								
Table G	**TOTAL**								**Total- G**

***** No. of Units wherever mentioned in tables above is for evaluation purpose only and Purchaser does not guarantee them. Purchaser reserves the right to issue a PO for a lesser amount based on actual usage.

Foot Note:

1. Virtual machine cost should include all network, hardware, security devices, load balancer,cloud SOC, NOC and other services including any hardware required for connecting to GMLC
2. Volume of voice recording storage requirement should be incorporated in cloud storage services
3. Voice recording software license should be incorporated in cloud contact center cost
4. IP phone per agent licnese cost should be incorporated in the contact center cloud solution services.
5. Cloud services cost should include the unit rate for updates also for hardware, network, security devices, load balancer etc.
6. T&D and staging VM count should be included in cloud services

3 Proformas

3.1 Performance Bank Guarantee

Ref: _________________ Date _________________

Bank Guarantee No. ______________________

To
The Director - SR
Ministry Of Home Affairs
5 Floor, NDCC – II building
Jai Singh Road, New Delhi - 110001

1. Against contract vide Advance Acceptance of the Tender No. _________________ dated _________________ covering __________________________________ (hereinafter called the said "Contract") entered into between the Ministry of Home Affairs. (hereinafter called "MHA") and _________________ (hereinafter called the "Bidder"), this is to certify that at the request of the Bidder we ------------- Bank Ltd., are holding in trust in favour of MHA, the amount of ___________________________ (write the sum here in words) to indemnify and keep indemnified MHA against any loss or damage that may be caused to or suffered by MHA by reason of any breach by the Bidder of any of the terms and conditions of the said contract and/or in the performance thereof. We agree that the decision of MHA, whether any breach of any of the terms and conditions of the said contract and/or in the performance thereof has been committed by the Bidder and the amount of loss or damage that has been caused or suffered by MHA shall be final and binding on us and the amount of the said loss or damage shall be paid by us forthwith on demand and without demur to MHA.

2. We __________________________________ Bank Ltd, further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for satisfactory performance and fulfillment in all respects of the said contract by the Bidder i.e. till _________________ hereinafter called the said date and that if any claim accrues or arises against us _________________ Bank Ltd, by virtue of this guarantee before the said date, the same shall be enforceable against us ____ Bank Ltd, notwithstanding the fact that the same is enforced within six months after the said date, provided that notice of any such claim has been given to us _________________ Bank Ltd, by MHA before the said date. Payment under this letter of guarantee shall be made promptly upon our receipt of notice to that effect from MHA.

3. It is fully understood that this guarantee is effective from the date of the said contract and that we _________________ Bank Ltd, undertake not to revoke this guarantee during its currency without the consent in writing of MHA.

4. We undertake to pay to MHA any money so demanded notwithstanding any dispute or disputes raised by the Bidder in any suit or proceeding pending before any court or Tribunal relating thereto our liability under this present bond 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 Bidder shall have no claim against us for making such payment.

5. We ________________________________ Bank Ltd, further agree that MHA shall have the fullest liberty, 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 Tendered from time to time or to postpone for any time of from time to time any of the powers exercisable by MHA against the said Bidder and to forebear or enforce any of the terms and conditions relating to the said contract and we, ________________ Bank Ltd., shall not be released from our liability under this guarantee by reason of any such variation or extension being granted to the said Bidder or for any forbearance by MHA to the said Bidder or for any forbearance and or omission on the part of MHA or any other matter or thing whatsoever, which under the law relating to sureties, would, but for this provision have the effect of so releasing us from our liability under this guarantee.

6. This guarantee will not be discharged due to the change in the constitution of the Bank or the Bidder.

Date ________________

Place ________________ Signature ________________

Witness ________________ Printed name ________________

(Bank's seal)

3.2 Non-Disclosure Agreement

WHEREAS, we the undersigned Bidder, ________________________________, having our principal place of business/ registered office at ________________, are desirous of bidding for RFP No. <<>> dated <<DD-MM-2015>> "**Selection of IT service provider for Nationwide Emergency Response System**" (hereinafter called the said 'RFP') to the MHA, GoI hereinafter referred to as 'Purchaser'

and,

WHEREAS, the Bidder is aware and confirms that the Purchaser's business/ operations, information, application/software, hardware, business data, architecture schematics, designs, storage media and other information / documents made available by the Purchaser in the RFP documents during the bidding process and thereafter, or otherwise (confidential information for short) is privileged and strictly confidential and/or proprietary to the Purchaser,

NOW THEREFORE, in consideration of disclosure of confidential information, and in order to ensure the Purchaser's grant to the Bidder of specific access to Purchaser's 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 Purchaser 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 & 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 Purchaser.

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 Purchaser.

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 Purchaser 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, agents, 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 Purchaser 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 Purchaser or may require the Bidder’s personnel to have access to software, hardware, computer networks, databases, documents and storage media of the Purchaser while on or off premises of the Purchaser. It is understood that it would be impractical for the Purchaser 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/expiry of this Agreement or at any time during its currency, at the request of the Purchaser, the Bidder shall promptly deliver to the Purchaser 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 Purchaser. Upon completion of the Tendering process and/or termination of the contract or at

any time during its currency, at the request of the Purchaser, the Bidder shall promptly deliver to the Purchaser 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 Purchaser. Without prejudice to the above the Bidder shall promptly certify to the Purchaser, due and complete destruction and return. Nothing contained herein shall in any manner impair rights of the Purchaser 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 Purchaser to enable the Purchaser 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 Purchaser. 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 :

MINISTRY OF HOME AFFAIRS

(Center State Division, Govt. Of India)

Tender No.: 15011/38/2013-SC/ST-W **26 June 2015**

Request for Proposal

For

“Selection of Implementation Agency for Nationwide Emergency Response System”

Section 5

Scope of Work

Issued by:

Ministry Of Home Affairs – CS Division, 5th Floor, NDCC-II Building, Jai Singh Road,
New Delhi -110001, India

Table of Contents

1 Intent

The intent of this document is to provide the detailed scope of work for Bidder who shall be engaged to supply, install, commission and maintain Nationwide Emergency Response System and provide related services to the Purchaser.

This section is part of the RFP document and it details out the Scope of Work for Bidder.

This section should be read together with Annexure 5A and 5B to get detailed overview of scope of work.

2 Introduction

2.1 Project Background

2.1.1 In India historically we have had different phone numbers to call police, fire and ambulance services namely 100, 102, 103. This system was designed at the time of a regulated telecom sector with only one telecom provider across India and one in each metro. Hence any call to these emergency numbers were routed to a call agent/ dispatcher of that particular emergency service and handled by the emergency personal themselves. The system was not designed for emergency response initially but as an emergency contact.

2.1.2 Over time, in response to changing environment, the three services have tried to evolve the emergency contact into an emergency response system with mixed results. A number of cities have provided additional numbers for specific emergency situations which are not routed to a central emergency response dispatcher. This leads to confusion in the public about emergency contact number.

2.1.3 After the incident of 16 December 2012 in Delhi, a Committee headed by Justice J.S. Verma, former Chief Justice of Supreme Court, with Justice (retired) Leila Seth, and Shri Gopal Subramanian was set up on 23 December, 2012 to give recommendations on amending laws to provide for speedy justice and enhanced punishment for criminals in sexual assault cases of extreme nature. The Committee had recommended the setting up of a public emergency response system which will have the ability to dispatch an Emergency Response (ER) unit to respond and close the ER call.

2.1.4 On the same, the Ministry of Home Affairs, as per the recommendation of the Justice Verma received the project approval for Computer Aided Dispatch System for Emergency Response. With the current challenges being faced by major Police forces in the Country for an immediate emergency response system specifically inclined towards Women issues, the project is conceived to bridge the gap.

2.1.5 The system should be designed to be scalable in future. Scalability of the system would mean:

- States may join the system at different points
- Integration of new applications
- Increase in number of seats at State Call Centers
- Multiple cities within a State to have Call Centers
- Increase in type of cases to be handled by emergency response
- Increase in dispatch vehicles
- Inclusion of Fire and Medical emergency services and any other feature which would make the Emergency Response more comprehensive

The scalability would be increased in phases. Bidder would procure the system based on the need of Purchaser.

2.1.6 In this aspect, Ministry of Home Affairs is inviting IT Service Providers to design, configure, customize, implement and maintain envisaged Nationwide Emergency

Response System to be implemented across India. Bidder will have to integrate with purchasers CAD software provider

2.2 Objectives and Scope of the project

2.2.1 Providing single emergency response number across the country for women safety

2.2.2 Integration with non-emergency number for counselling, answering to complaints, taking feedbacks etc. Purchaser may choose to opt for its own non-emergency number.

2.2.3 Providing 24 Hours and 7 Days (24x7) efficient and effective response system which can receive input from various voice and data services such as call, SMS, email, Internet of Things etc. to attend to women in distress

2.2.4 Identification of location of person in distress connecting through voice or data with the system

2.2.5 Timely dispatch of field resources (police) to the location of incidence using the system

2.2.6 To locate and dispatch nearest GPS enabled vehicles

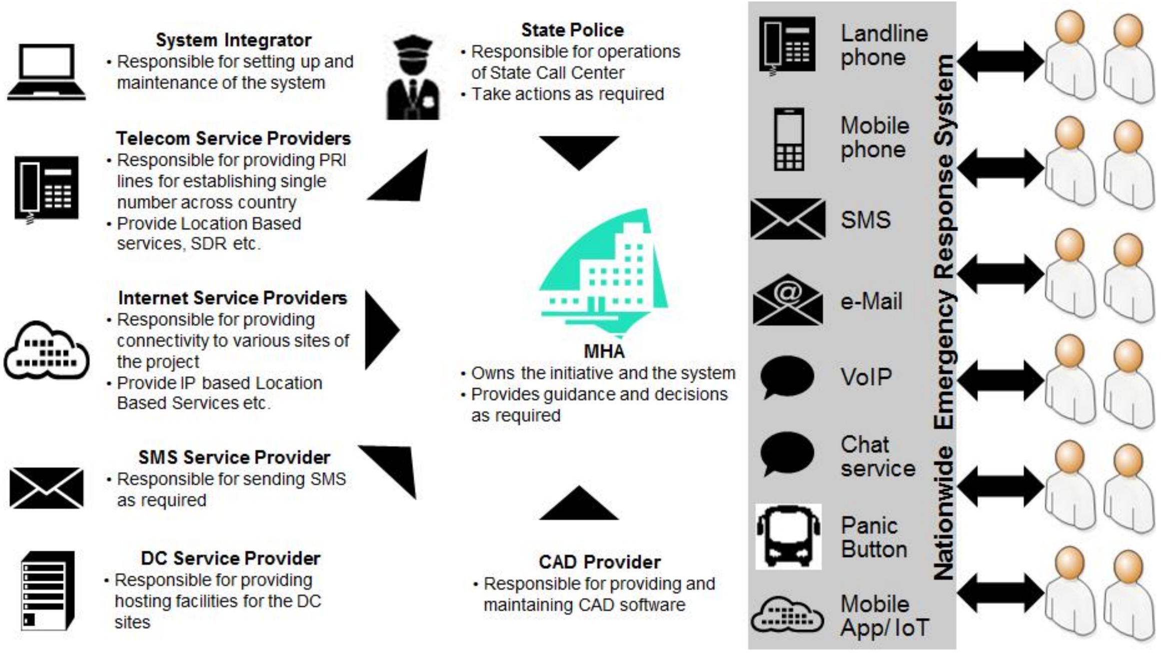
2.2.7 To acquire ability to analyze trends and station GPS- fitted 4 and 2 Wheelers at strategic locations.

2.2.8 Integration with Government applications such as App store, Himmat, mysecurity.gov.in and also an open platform to register and interface any mobile application made by individuals, companies, NGO, students etc.

2.2.9 Integration with existing Dial 100, Dial 108, Dial 181 and other emergency response system

2.3 Ecosystem for service delivery

2.3.1 Envisaged system would require interactions amongst various stakeholders in the ecosystem.


System Integrator
• Responsible for setting up and maintenance of the system
Telecom Service Providers
• Responsible for providing PRI lines for establishing single number across country
• Provide Location Based services, SDR etc.
Internet Service Providers
• Responsible for providing connectivity to various sites of the project
• Provide IP based Location Based Services etc.
SMS Service Provider
• Responsible for sending SMS as required
DC Service Provider
• Responsible for providing hosting facilities for the DC sites
State Police
• Responsible for operations of State Call Center
• Take actions as required
MHA
• Owns the initiative and the system
• Provides guidance and decisions as required
CAD Provider
• Responsible for providing and maintaining CAD software
Landline phone
Mobile phone
SMS
e-Mail
VoIP
Chat service
Panic Button
Mobile App/ IoT
Nationwide Emergency Response System

#	Stakeholder	Broad roles & responsibilities
1.	Purchaser	▶ Provide requirements related to the project ▶ To provide overall guidance and approach for implementation & execution of the project ▶ To approve deliverables as listed in this RFP of the IT Service Provider (ITSP) ▶ Acceptance of the system which has been deployed ▶ To provide any other approval required for the implementation
2.	State Government	▶ Civil infrastructure preparation and interiors, support and maintenance of the State Call Centre ▶ Manpower provision at the call center ▶ Handling operations of State call and field officers ▶ Assisting the Bidder for implementation of the project
3.	IT Service Provider (ITSP)	▶ Cloud enabled DC sites services ▶ Procurement, software development, testing, installation, commission and operation & maintenance of the emergency response system (including hardware, manpower, network, application and operation center) ▶ Installation of MDTs at the state/district locations ▶ Training of the personnel on the solution ▶ Manage CAD service providers contracts
4.	CAD provider	▶ Provide CAD software ▶ Train ITSP personnel on the CAD software
5.	Telecom Service Provider	▶ Provision of PRI lines ▶ Provision of system for identifying the location of caller ▶ Providing mapping of centralized short code number ▶ Providing required databases such as SDR etc.
6.	SMS service provider	▶ Providing SMS service through which messages can be sent and received by the central system to the required personnel based on requirement
7.	Network service provider	▶ Connecting all sites i.e. Operations Center, State/City call center, DC-DC through primary and secondary network link as required ▶ Providing internet services

3 Functional overview of the system

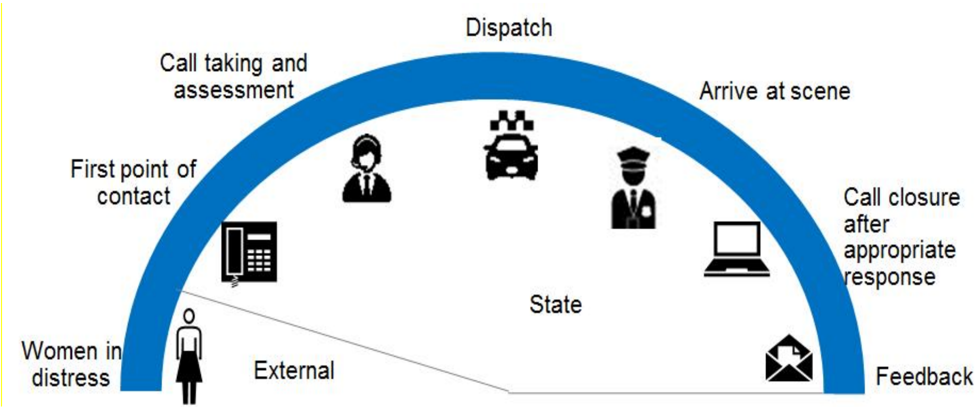
3.1 Geographical overview

3.1.1 The project would be undertaken nationwide, with a centralized Operations Centre at Delhi and State Call Centres at the identified locations in the State capitals.

3.2 Process overview

3.2.1 A centralized system leveraging input from various sources such as voice call, SMS, email, mobile application etc. is envisaged by the Purchaser.

3.2.2 Overview of the process is captured in the steps below.



3.3 First point of contact

3.3.1 A state public safety answering point (**PSAP**) is a state call center responsible for answering calls to an emergency telephone number for police, firefighting and ambulance services. A **PSAP** facility will run 24 hours a day, dispatching emergency services or passing 112 calls on to public or approved private safety agencies. Trained agents are responsible for dispatching the emergency services.

3.3.2 Citizen can contact the emergency number through various communication channels.

3.3.3 Also the non-emergency number can be contacted through various channels for counselling, feedback, complaints etc.

3.3.4 Bidder should ensure all calls originating in one state and are routed to the same states.

3.3.5 The input communication channels include:

- Fixed landline phone
  SDR would be provided to identify the details and location of the caller. A caller location address database will be created by the bidder with web interface to access this database. This database will be created based on CD provided by the TSP

- Mobile phone
  Bidder should correctly identify the state from where the call is originating and ensure to the extent possible that Mobile number portability and roaming issues are addressed. Bidder should integrate with CLI and GMLC databases to be made available by TSP.A caller location address database will be created by the bidder

with web interface to access this database. This database will be created based on CD provided by the TSP

- SMS
  SMS should be routed to correct State Call Centre by identifying location of sender

- Email
  Each State should have a separate email id so that email is sent to chosen State. Email can also be sent through the Nirbhaya portal where in State is selected through a drop down menu of States. Information of all email IDs should be available on Nirbhaya Portal.

- Chat
  Each State should have separate chat ID so that chat is directed to chosen State. Chat can also be initiated through Nirbhaya portal where in State is selected through a drop down menu of States. Information of all chat IDs should be available on Nirbhaya Portal.

- Panic button in public transport
  Integration with the Nirbhaya project of Ministry of Road Transport and Highways wherein panic buttons are installed in public transport. Bidder should define a protocol based on open standards to interface with all such devices.

- VoIP
  VoIP calls to be made to State VoIP ID. Each State would have multiple IDs. In case of increasing usage, State may have more than one ID for VoIP. VoIP can be initiated from Nirbhaya portal as well. Information of all VoIP IDs should be available on Nirbhaya Portal.

- Mobile application
  Mobile application would send GPS coordinate to the system. The alert should be directed to respective State based on the coordinates. Mobile application would also have a call button which should directly call the emergency response system. User of mobile application would be registered on the Nirbhaya Portal first and then the application would be used.

- Internet of Things (IoT)
  IoT are future devices such as wrist bands, buttons etc. that can send GPS coordinate to the system. The alert should be directed to respective State based on the coordinates. User and IoT device would be registered on the Nirbhaya Portal first to use the services. Bidder would provide a generic interface definition like xml signature etc. to receive the data from IOTs.

3.4 Call/ data message taking and assessment

3.4.1 Call/ data message would be distributed through the system to the available agent and the system would display the pre-populated fields like location, name of the caller etc. from the information available in the database.

3.4.2 Agent will create case file in the system and based on pre-defined rules would grade the call

3.4.3 Information about the emergency case would be passed on to dispatcher for further action

3.5 Dispatch

3.5.1 Dispatcher would have information about the case from agent and availability of emergency vehicles on the GIS map

3.5.2 Dispatcher would compile all information and dispatch the nearest emergency vehicle to the incident location

3.5.3 Also, information would be sent to the nearest police station

3.6 Arrive at Scene and call closure

3.7 Feedback

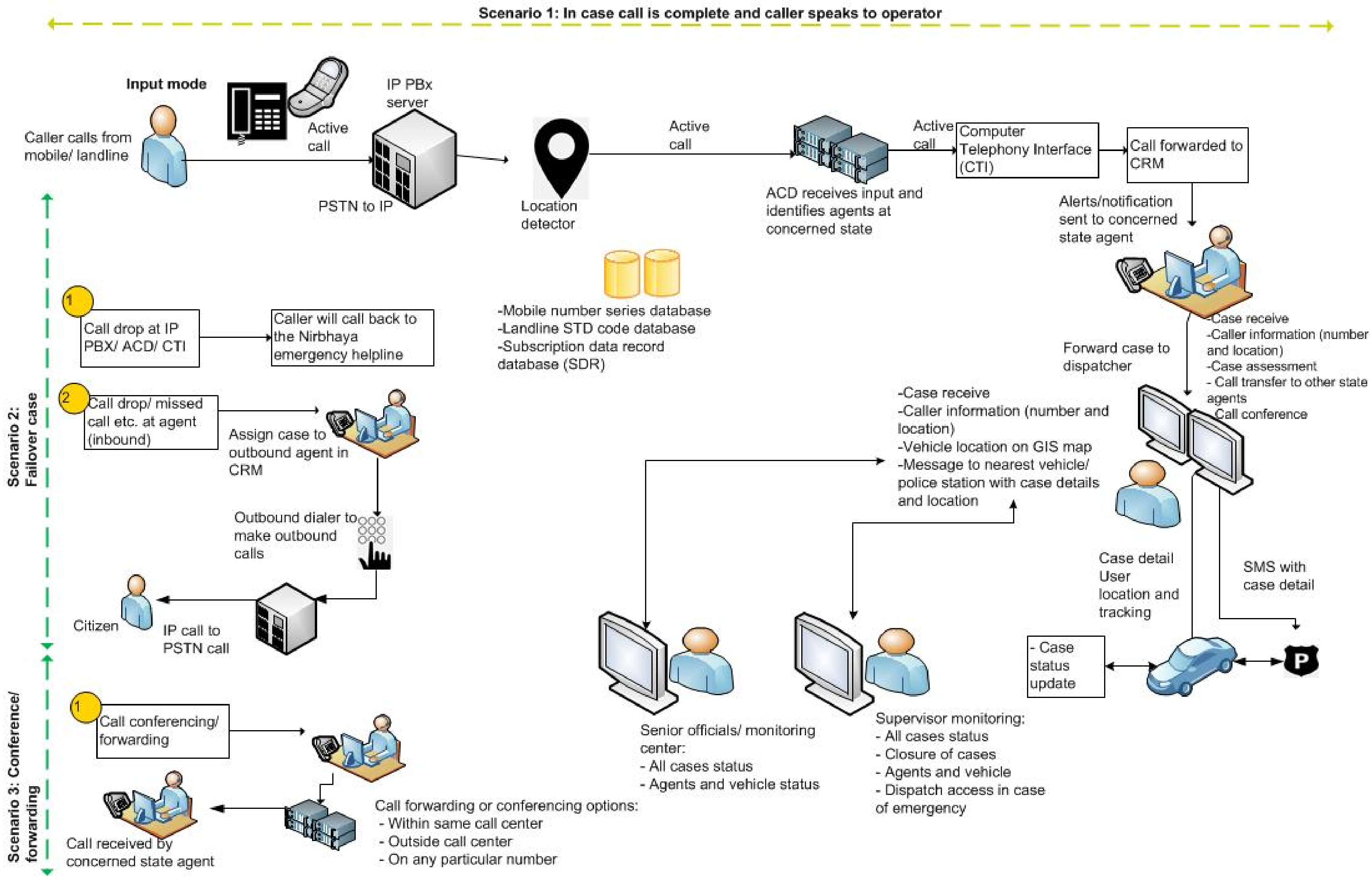
3.7.1 Post the event, either caller or call center agent can connect (through call/ message/ email/ mobile application) to receive feedback on the services

3.7.2 Feedback would help in improving the efficiency and effectiveness of the system.

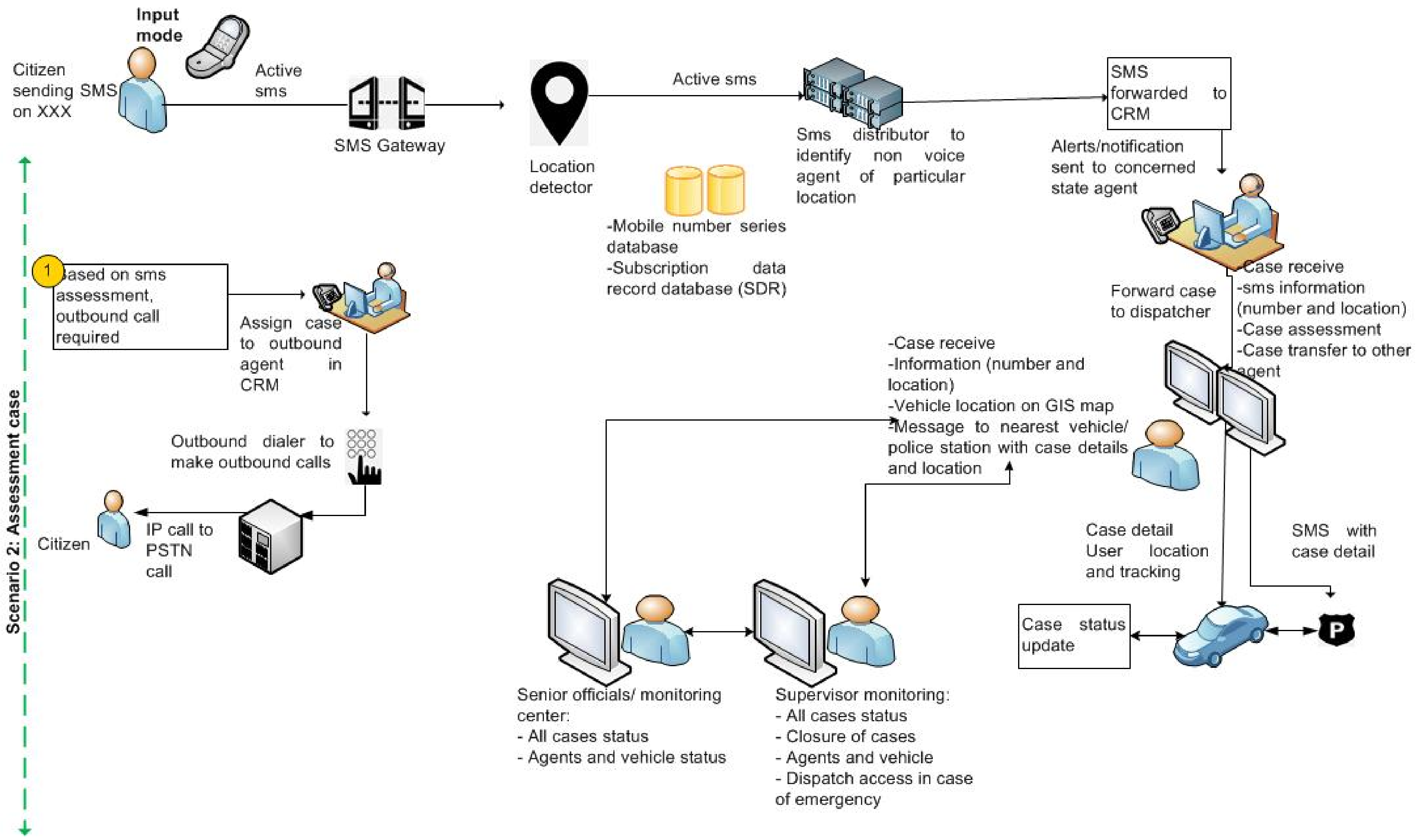
3.8 Case handling scenarios

3.8.1 Case handling scenarios are provided below to facilitate Bidder’s understanding of the process.

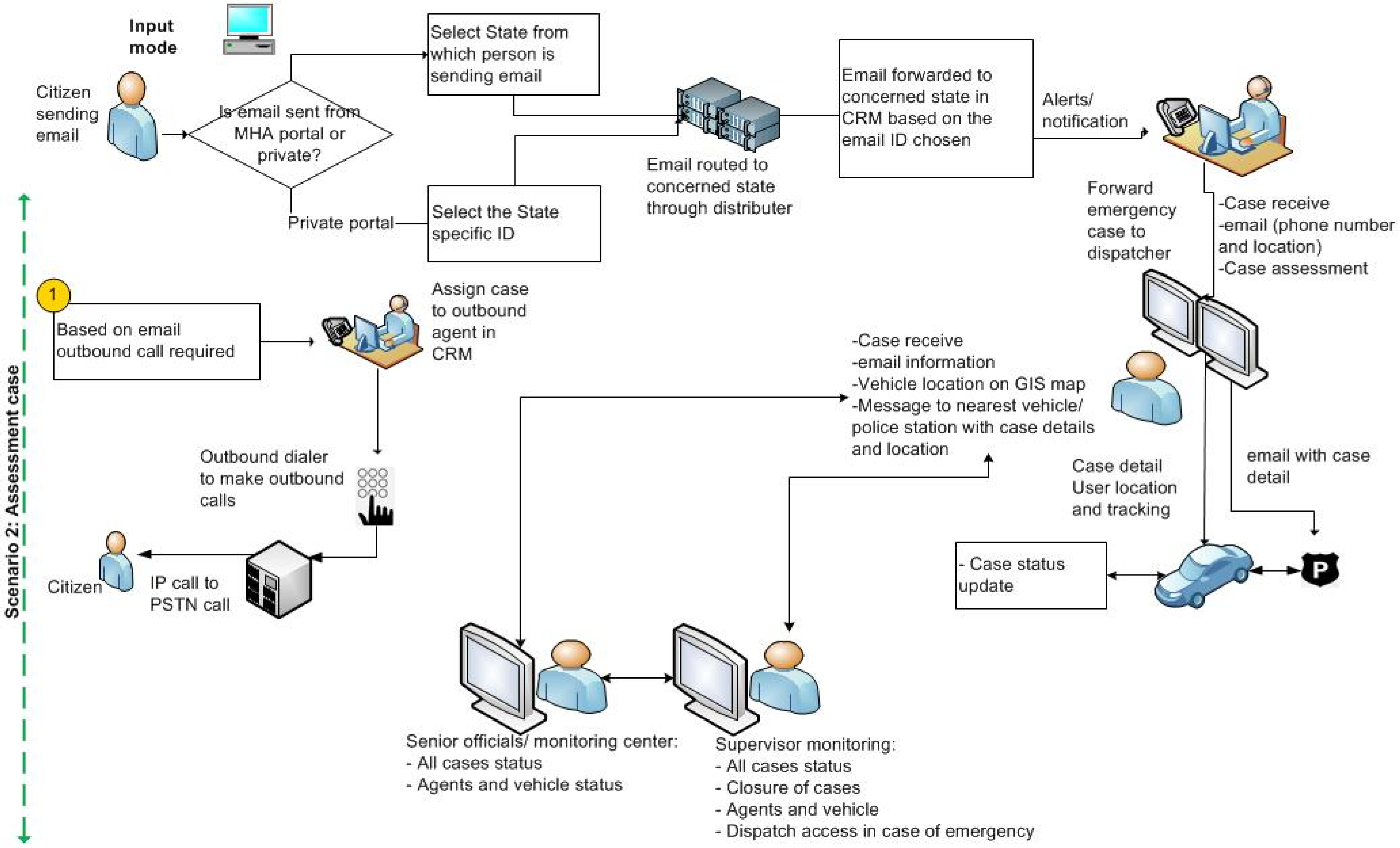
Case 1: Caller calling from Mobile/ landline


Scenario 1: In case call is complete and caller speaks to operator
Input mode
Caller calls from mobile/ landline
Active call
IP PBx server
PSTN to IP
Location detector
Active call
ACD receives input and identifies agents at concerned state
Active call
Computer Telephony Interface (CTI)
Call forwarded to CRM
Alerts/notification sent to concerned state agent
-Mobile number series database
-Landline STD code database
-Subscription data record database (SDR)
-Case receive
-Caller information (number and location)
-Case assessment
- Call transfer to other state agents
- Call conference
Forward case to dispatcher
-Case receive
-Caller information (number and location)
-Vehicle location on GIS map
-Message to nearest vehicle/ police station with case details and location
Case detail User location and tracking
SMS with case detail
- Case status update
P
Senior officials/ monitoring center:
- All cases status
- Agents and vehicle status
Supervisor monitoring:
- All cases status
- Closure of cases
- Agents and vehicle
- Dispatch access in case of emergency
Scenario 2: Failover case
1
Call drop at IP PBX/ ACD/ CTI
Caller will call back to the Nirbhaya emergency helpline
2
Call drop/ missed call etc. at agent (inbound)
Assign case to outbound agent in CRM
Outbound dialer to make outbound calls
Citizen
IP call to PSTN call
Scenario 3: Conference/ forwarding
1
Call conferencing/ forwarding
Call received by concerned state agent
Call forwarding or conferencing options:
- Within same call center
- Outside call center
- On any particular number

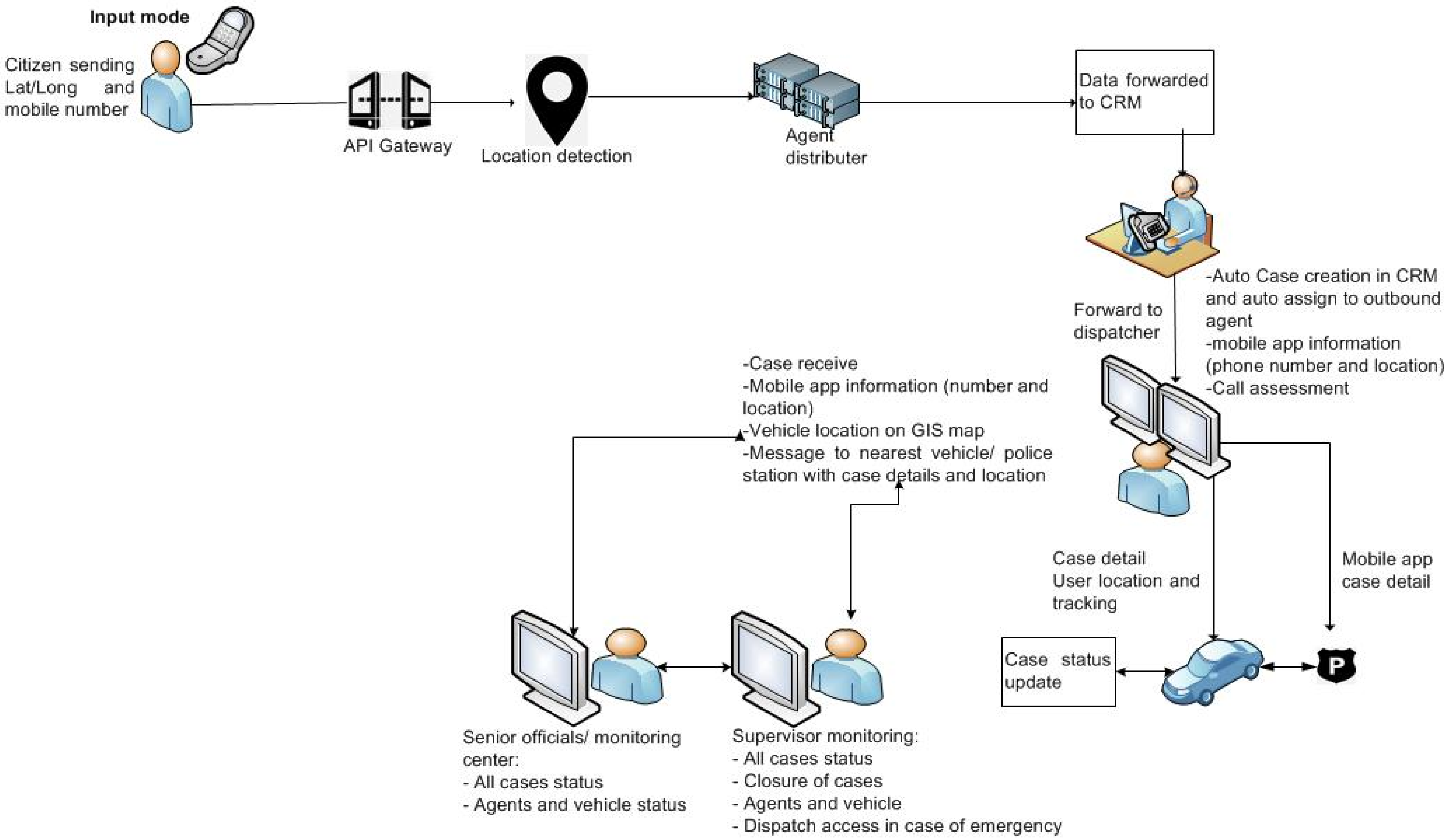
Case 2: SMS


Input mode
Citizen sending SMS on XXX
Active sms
SMS Gateway
Location detector
Active sms
-Mobile number series database
-Subscription data record database (SDR)
Sms distributor to identify non voice agent of particular location
SMS forwarded to CRM
Alerts/notification sent to concerned state agent
Case receive
-sms information (number and location)
-Case assessment
-Case transfer to other agent
Forward case to dispatcher
Scenario 2: Assessment case
1
Based on sms assessment, outbound call required
Assign case to outbound agent in CRM
Outbound dialer to make outbound calls
Citizen
IP call to PSTN call
-Case receive
-Information (number and location)
-Vehicle location on GIS map
-Message to nearest vehicle/ police station with case details and location
Case detail User location and tracking
SMS with case detail
Case status update
P
Senior officials/ monitoring center:
- All cases status
- Agents and vehicle status
Supervisor monitoring:
- All cases status
- Closure of cases
- Agents and vehicle
- Dispatch access in case of emergency

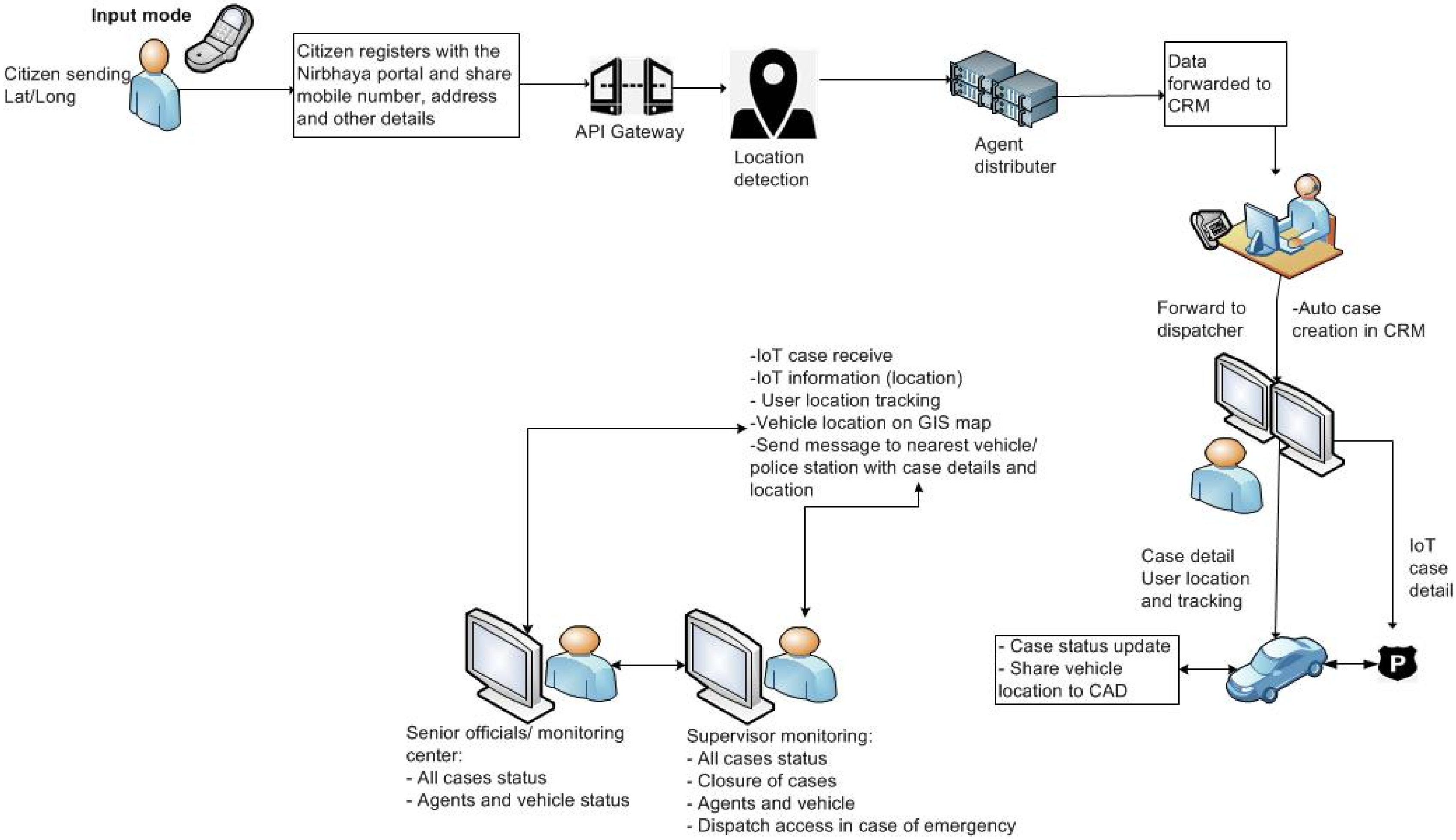
Case 3: Email


Input mode
Citizen sending email
Is email sent from MHA portal or private?
Select State from which person is sending email
Private portal
Select the State specific ID
Email routed to concerned state through distributer
Email forwarded to concerned state in CRM based on the email ID chosen
Alerts/ notification
Forward emergency case to dispatcher
-Case receive
-email (phone number and location)
-Case assessment
Scenario 2: Assessment case
1
Based on email outbound call required
Assign case to outbound agent in CRM
Outbound dialer to make outbound calls
Citizen
IP call to PSTN call
-Case receive
-email information
-Vehicle location on GIS map
-Message to nearest vehicle/ police station with case details and location
Case detail User location and tracking
email with case detail
- Case status update
P
Senior officials/ monitoring center:
- All cases status
- Agents and vehicle status
Supervisor monitoring:
- All cases status
- Closure of cases
- Agents and vehicle
- Dispatch access in case of emergency

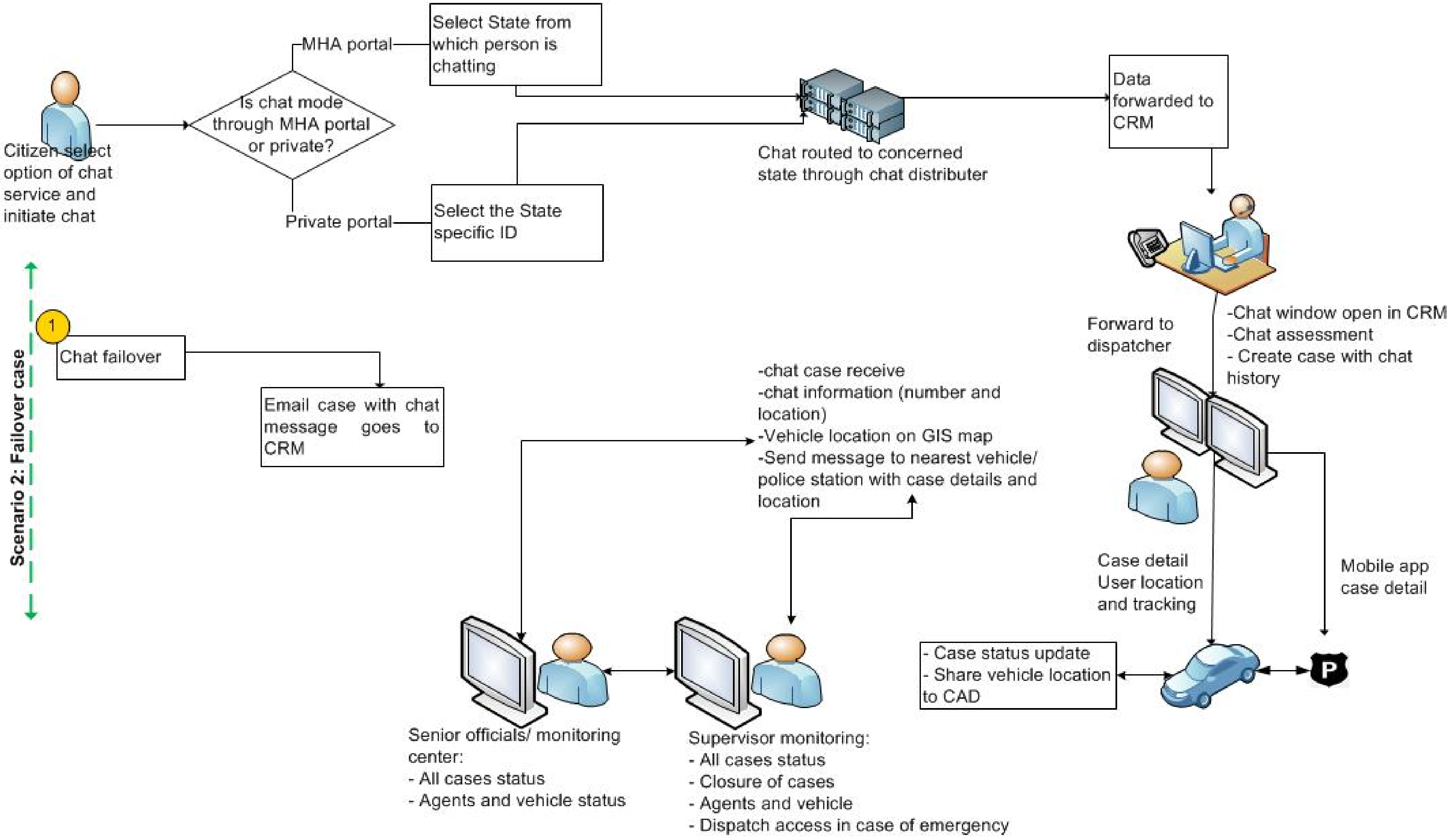
Case 4: Mobile apps


Input mode
Citizen sending Lat/Long and mobile number
API Gateway
Location detection
Agent distributer
Data forwarded to CRM
-Auto Case creation in CRM and auto assign to outbound agent
-mobile app information (phone number and location)
-Call assessment
Forward to dispatcher
-Case receive
-Mobile app information (number and location)
-Vehicle location on GIS map
-Message to nearest vehicle/ police station with case details and location
Case detail
User location and tracking
Mobile app case detail
Case status update
P
Senior officials/ monitoring center:
- All cases status
- Agents and vehicle status
Supervisor monitoring:
- All cases status
- Closure of cases
- Agents and vehicle
- Dispatch access in case of emergency

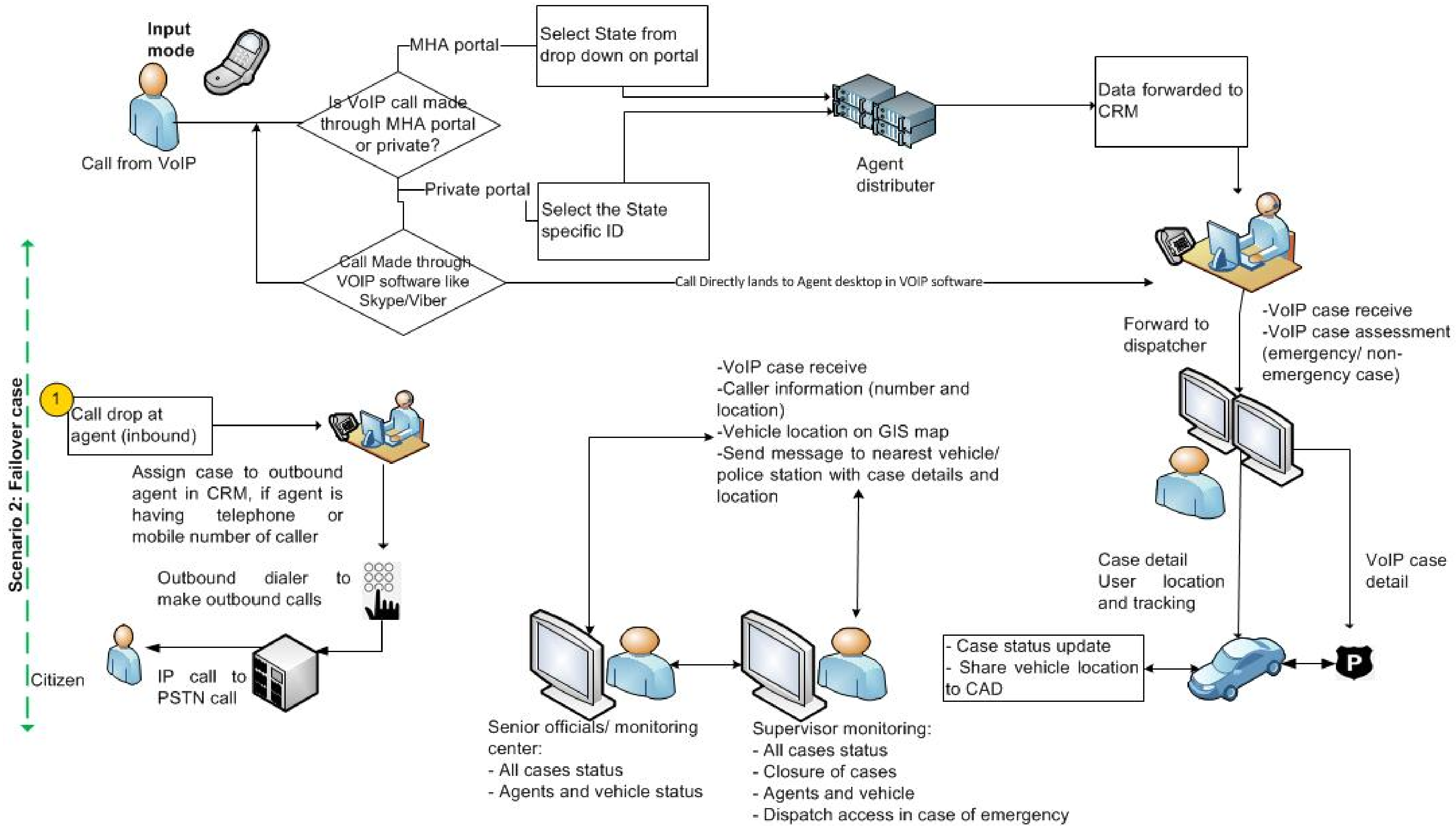
Case 5: Contact through Internet of Things (IoT) devices


Input mode
Citizen sending Lat/Long
Citizen registers with the Nirbhaya portal and share mobile number, address and other details
API Gateway
Location detection
Agent distributer
Data forwarded to CRM
Forward to dispatcher
-Auto case creation in CRM
-IoT case receive
-IoT information (location)
- User location tracking
-Vehicle location on GIS map
-Send message to nearest vehicle/ police station with case details and location
Case detail User location and tracking
IoT case detail
- Case status update
- Share vehicle location to CAD
Senior officials/ monitoring center:
- All cases status
- Agents and vehicle status
Supervisor monitoring:
- All cases status
- Closure of cases
- Agents and vehicle
- Dispatch access in case of emergency

Case 6: Contact through portal chat/ chat messenger


Citizen select option of chat service and initiate chat
Is chat mode through MHA portal or private?
MHA portal
Private portal
Select State from which person is chatting
Select the State specific ID
Chat routed to concerned state through chat distributer
Data forwarded to CRM
-Chat window open in CRM
-Chat assessment
- Create case with chat history
Forward to dispatcher
Case detail
User location and tracking
Mobile app case detail
P
- Case status update
- Share vehicle location to CAD
-chat case receive
-chat information (number and location)
-Vehicle location on GIS map
-Send message to nearest vehicle/ police station with case details and location
Senior officials/ monitoring center:
- All cases status
- Agents and vehicle status
Supervisor monitoring:
- All cases status
- Closure of cases
- Agents and vehicle
- Dispatch access in case of emergency
Scenario 2: Failover case
1
Chat failover
Email case with chat message goes to CRM

Case 7: Contact through VoIP


Input mode
Call from VoIP
MHA portal
Is VoIP call made through MHA portal or private?
Select State from drop down on portal
Private portal
Select the State specific ID
Call Made through VOIP software like Skype/Viber
Call Directly lands to Agent desktop in VOIP software
Agent distributer
Data forwarded to CRM
Forward to dispatcher
-VoIP case receive
-VoIP case assessment (emergency/ non-emergency case)
-VoIP case receive
-Caller information (number and location)
-Vehicle location on GIS map
-Send message to nearest vehicle/ police station with case details and location
Case detail User location and tracking
VoIP case detail
- Case status update
- Share vehicle location to CAD
P
Senior officials/ monitoring center:
- All cases status
- Agents and vehicle status
Supervisor monitoring:
- All cases status
- Closure of cases
- Agents and vehicle
- Dispatch access in case of emergency
Scenario 2: Failover case
1
Call drop at agent (inbound)
Assign case to outbound agent in CRM, if agent is having telephone or mobile number of caller
Outbound dialer to make outbound calls
IP call to PSTN call
Citizen

4 Technical solution

4.1 Architectural principles

4.1.1 Service Oriented Architecture that defines integration architectures based on the concept of a service becomes relevant especially when there are multiple applications in an enterprise and point-to-point integration between them involves complexity. When multiple applications are involved services shall be able to communicate with each other which shall be achieved by implementation of SOA through web services where the services are exposed for other applications. Bidder shall propose SOA based architecture while designing the solution.

4.1.2 The system should be highly available to avoid missing any emergency situation in the country

4.1.3 The Principle of Architecture should have Active-Active between the sites, servers and services across the solution.

4.1.4 The architecture should be cloud based, with interoperable.

4.1.5 The Proposed solution should have Business Continuity and Disaster recovery by taking the RTO and RPO as objective to achieve.

4.1.6 Each input should be formed as unique case in the system

4.1.7 There should be no single point of failure in the system

4.1.8 The bidder has to maintain the principal of less manual intervention and full automation.

4.1.9 The system must be highly performant in order to achieve timely Emergency response to the person in need across country. It should be possible to scale quickly to meet the incoming calls/ inputs from various sources.

4.1.10 All calls/ other inputs should be recorded for future purpose for defined period. In case of any judicial proceedings, the records should be maintained as long as the proceedings.

4.1.11 The system must be reliable against hardware and software failures and Disasters. Integrity of data and availability must be assured.

4.1.12 The underlying technology needs to be user friendly. By having easy use-of-use principle, training can be kept to a minimum thereby aiding IT change management and the risk of using a system improperly can be minimized.

4.1.13 N-Tier model is the framework in which application user interface, logic, data, and their associated processing and repair are separated from each other in logical manner is more flexible in response to changes in internal logic, platforms, and structures; this isolates/minimizes the impact of change. Considering requirements of ease of support, scalability and interoperability, N-tier model shall be proposed.

4.1.14 Vendor lock-in should be avoided.

4.1.15 The bidder should minimize integration effort for the proposed solution.

4.1.16 The infrastructure management should be Directory services driven with Domain Schema

4.2 Security Principles

4.2.1 The bidder should follow security principles such as “defense in depth”; for numerous defense mechanisms (“layers”) in place, designed so that an attacker has to defeat multiple mechanisms to perform a successful attack. Multi-layer security must be employed starting with networks, perimeter, DMZ, Cloud enabled Data Center, applications, databases, End User machines and Mobile computing devices.

4.2.2 Bidder has to ensure the cloud security architecture model to facilitate effective incident response resolution, forensic investigation during incident analysis with best practices like real time internal network defense, etc.

4.2.3 Bidder has to be aware of threat and its mitigation for cloud application which include spoofing, tempering, repudiation, information disclosure, denied of service and elevation of privilege along with OWASP (Open web application security project) testing guidelines.

4.2.4 Bidder has to ensure hyperwiser architecture security concern like virtual machine guest hardening, hyverwiser security, inter VM attack blind spot, operation complexity from VM sprawam, virtual machine encryption, datacominglingue, VM data destruction, VM image tampering.

4.2.5 All the Applications and Infra changes has to be by secure SMLC and Change Management principle driven respectively.

4.2.6 The bidder should follow the principle of “least privilege”. Each user and program should operate using the fewest privileges possible. This principle limits the damage from an accident, error, or attack. It also reduces 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. The bidder will have to design its solution utilizing similar industry recognized security principles.

4.2.7 All IT and IS operations will be governed by the IT and IS Policy which will be provided to the successful bidder. The bidder will have to prepare detailed procedures for the same and implement accordingly. All project documentation should be prepared by the bidder as per the policy and related regulations.

4.2.8 The privacy of data has to be ensured by the bidder at all times. The bidder has to ensure that data sharing is done as per the policy.

4.2.9 Bidder has to adopt technical, physical and administrative measure in order to protect personal data from loss, misuse or alteration based on global best practices for privacy and security like OECD, APAC, IT act, Indian act compliance, NIST cloud computing reference model, CSA security guidance, ISO 27000 standards

4.2.10 The system must follow a role based access control at all levels. The bidder should implement logical access control based on policy prepared by Purchaser for application, subsystem, or group of systems. All the access logs needs to be captured and monitored.

4.2.11 Infrastructure and Application Access should follow 2 Factor Authentication

4.2.12 All the Databases and Data stores must be encrypted.

4.2.13 Bidder has to ensure data security life cycle as a principle in securing data while creating, storing, sharing, archiving or destroy.

4.2.14 Bidder has to ensure database protection with database activity monitoring and file activity monitoring

4.2.15 The proposed MPLS should be a private and dedicated network

4.2.16 Security in Design would encompass security risk assessment on user specifications, secure information architecture, proper role and based access design and secure application and database design.

4.2.17 The bidder has to ensure that their Application Development must follow Secured SDLC process development and deployment by taking OWASP Top 10 and SANS top 25 into consideration. Similarly, Application maintenance should follow Secured SMLC.

4.2.18 The system must be secure at all user touch points by using suitable security protocols and data protection methods

4.2.19 All types of network attacks must be identified and counter measures must be put in place.

4.2.20 All the ICT assets(virtual and physical) and non Digital Assets must also be secured throughout their life cycle as they may contain sensitive data with hardening, Asset disposal, data disposal principles.

4.2.21 The Network layer must have in depth packet inspection and intelligence in blocking attacks.

4.2.22 The bidder should provision for DDOS Free Bandwidth as a part of its solution.

4.2.23 The bidder has to conduct internal Audits annually with Cloud Security Alliance Cloud Controls Matrix (latest version) and ISO 27001/27017 as the reference and submit the audit report and action plan to purchaser.

4.2.24 For areas where Physical access controls have been implemented by the bidder as a part of the Scope of Work , the controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media, and any other elements required for the system's operation. The bidder should review the effectiveness of physical access controls in each area, both during normal business hours and at other times, particularly when an area may be unoccupied.

4.2.25 The bidder will ensure that the Critical data stores are minimized, and stored data has to be encrypted at all times.

4.2.26 The bidder has to ensure that access to data is given through application layer (via an application) at all times.

4.2.27 As a part of Service delivery process, the bidder has to ensure segregation of services and segregation of duties.

4.2.28 For operations phase security activities such as performing backups, holding training classes, managing cryptographic keys, keeping up with user administration and access privileges, and updating security software are some examples that have to be done by the bidder.

4.2.29 VPN and VLNS should be the principle of operations for remote access and isolation of internal traffic.

4.2.30 Service provider has to adopt metrics to measure risk management performance. E.g. Cyber security information exchange framework, security content automation protocol in cloud deployment.

4.2.31 The bidder to propose for a temporary alternate workplace for operations Center and Application management arrangement to manage the operations of the project in an event of loss of location in an event of a disaster.

4.2.32 The bidder should embed a security incident response plan within the Business continuity and disaster recovery plan to response in an efficient and effective manner in case of a disaster.

4.3 Management Principles

4.3.1 The management of system shall be SLA based.

4.3.2 System should have an Enterprise Management Solution that provides end-to-end, comprehensive, modular and integrated management of IT infrastructure components to maximize the availability of IT services and SLA performance

4.3.3 System Management shall follow all processes as per to ITIL standards. This includes Asset Management, Vendor Management, Configuration Management, Incident Management, Performance Management and Capacity Management.

4.3.4 Management to have minimal overhead on the system

4.3.5 Management of ICT should be automated.

4.3.6 Extensive reporting to help management and administrators to take quick decisions

4.3.7 System should track all the assets in use or acquired for use in real time.

4.3.8 Real-time status of the system should be available at all times.

4.3.9 System Management should intelligently perform root-cause analysis to rapidly bring the system back to normal working conditions

4.3.10 The system should be upgradeable without affecting the production

4.3.11 It should be possible to proactively manage all the system hardware and software components maintenance and licenses throughout their life cycle.

4.4 Technology Principles

4.4.1 The system should be built from best of breed components with no obsolescence and with futuristic designs.

4.4.2 The technology adopted should be periodically refreshed to achieve significant improvements in TCO.

4.4.3 All the system components must follow open standards and open source technologies. All application development should be in Java technology.

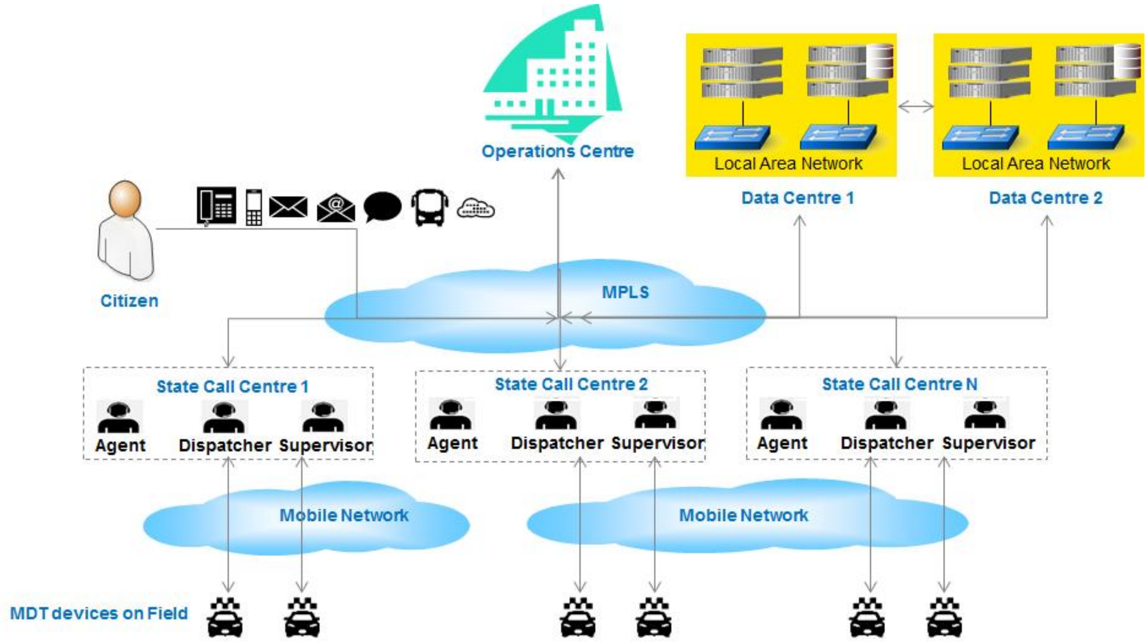
4.4.4 Interoperability of servers from different vendors is required at all levels.

4.4.5 Scalability, manageability to handle huge data volumes

4.4.6 Efficient Resource Utilization by separation of Compute and Storage resources and by distribution of load among all sites.

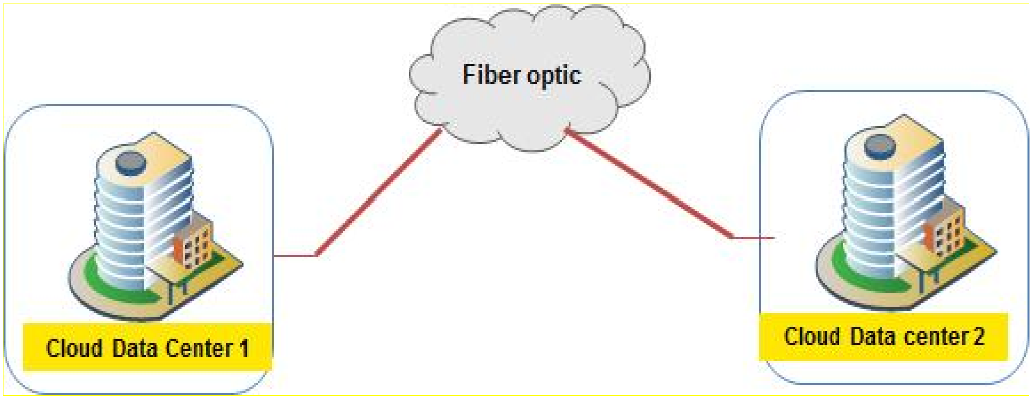
4.5 Solution overview

The simplistic overview of the components of the solution is shown below and explained later in this clause.



4.5.1 Cloud enabled Data Center sites

The indicative representation for the DC infrastructure and its connectivity is presented below



4.5.1.1 Both DC sites should be cloud enabled.

4.5.1.2 Bidder to provide primary and secondary connectivity for each site by the respective TSP.

4.5.1.3 The bidder will be responsible for all the technology, infrastructure at its DC sites over the period of the contract. The bidder will be required to procure, commission the required IT infrastructure as presented in the Clause 17.4 in this section of RFP.

4.5.1.4 The proposed applications shall be centrally hosted at the cloud enabled Data Center sites and access provided as online service to users across the country.

4.5.1.5 Cloud enabled DC1 and DC2 shall operate in active -active mode. The connectivity between both the data center should ensure the replication works seamless with no data loss.

4.5.1.6 The Infrastructure provisioned in both DC shall be capable to handle the 100% load at any point in time. The replication between both the data centers would ensure that there are no data inconsistencies on both application as well as storage level.

4.5.1.7 The cloud infrastructure by the bidder must be designed to avoid a “single point of failure” with redundant core components and other required elements to eliminate system outage.

4.5.1.8 The proposed cloud infrastructure should have high availability i.e. there should be no disruption in services on account of routine maintenance procedures, troubleshooting, loading hardware and software revisions, patches, etc.

4.5.1.9 The bidder should deliver cloud services from Tier III data centers facilities within India and DC cannot be located outside India.

4.5.1.10 Cloud infrastructure should be on industry proven standards

4.5.1.11 Services shall be available with at least 99.5% availability on the Infrastructure

4.5.1.12 Cloud should be hosted on Enterprise class server and storage system

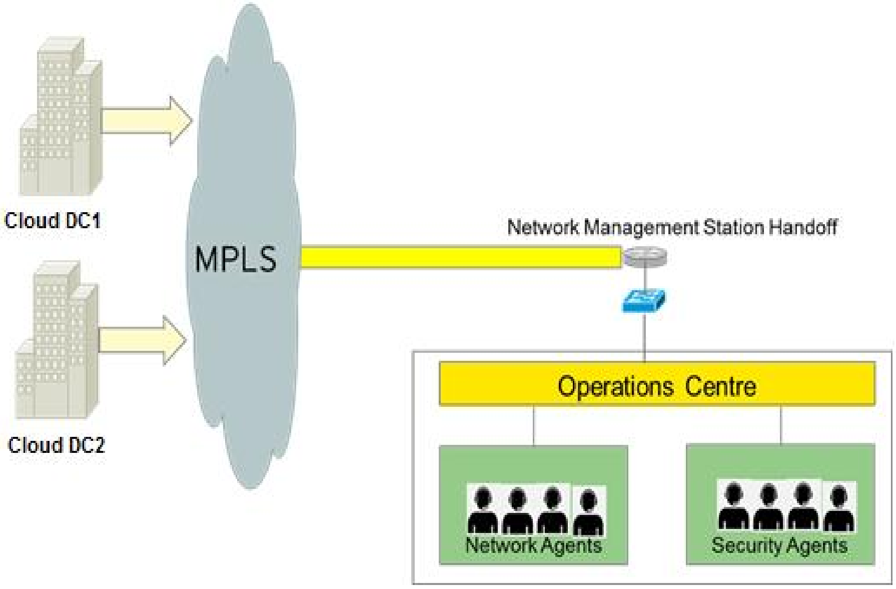
4.5.1.13 The proposed orchestration layer in the cloud infrastructure should give state wise / department usage statistics of the cloud / dedicated infrastructure resources.

4.5.1.14 Network Infrastructure and security infrastructure should be complaint with technology and security principles as mentioned in this section of RFP.

4.5.1.15 The bidder should adhere to best practices like ITIL, ISO: 20000, ISO 27001, etc.

4.5.2 **Operations Center**

4.5.2.1 Operations center is the hub of viewing and monitoring of performance of the emergency response system.



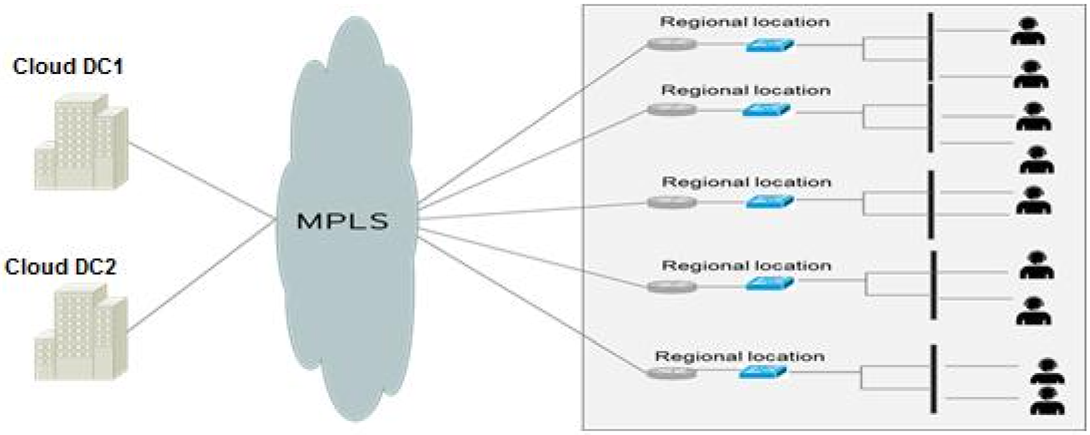
4.5.2.2 It houses NOC, SOC, Visitor gallery and monitoring for the system

4.5.2.3 MIS reports, BI reports and other analysis would also be performed at Operations Centre

4.5.2.4 Operations Center would run 24 * 7 * 365 days and can only be located at either of Delhi, Gurgaon and Noida

4.5.3 State Call Centre/PSAP

4.5.3.1 State Call Centre would be developed as a PSAP and would run 24 * 7 * 365 days



4.5.3.2 All calls/ data messages would mature at the State Call Centre, after identification of correct State

4.5.3.3 Voice/ data message is assessed by the agents and appropriate action is taken through the dispatcher.

4.5.3.4 Emergency vehicles would be dispatched based on the GIS maps used by the system.

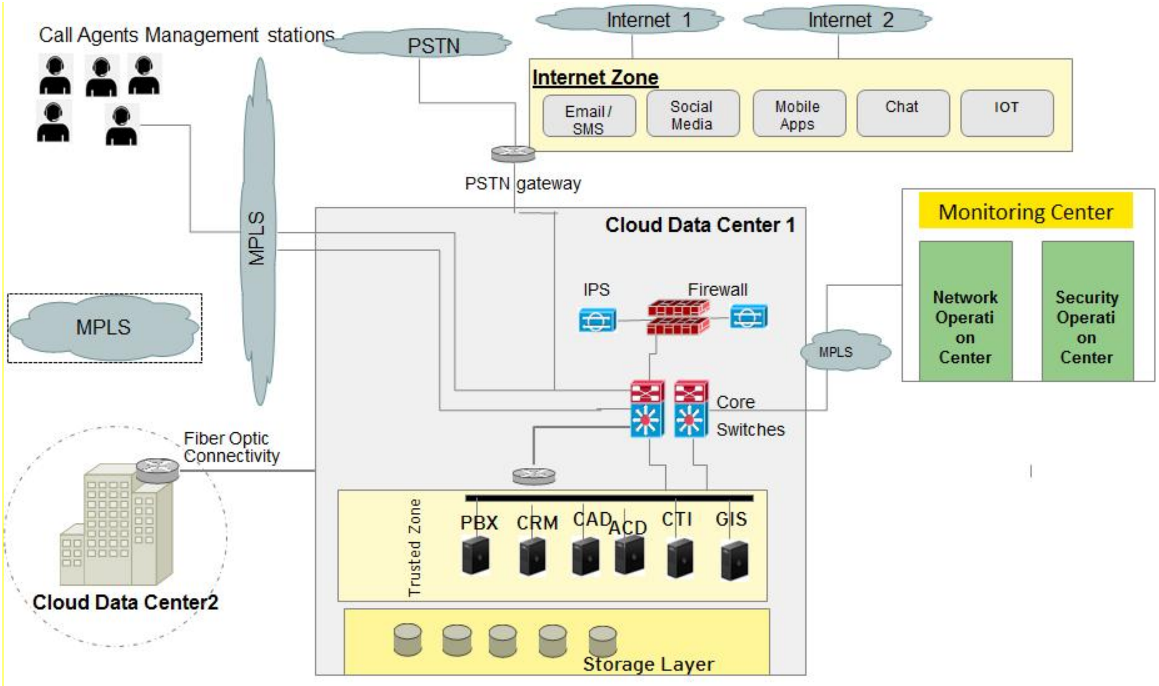
4.5.3.5 Feedback, complaints, comments etc. are also to be managed by State Call Center.

4.5.3.6 States would be given an option to set Call Centre in more than one city in future. The solution proposed by Bidder should be scalable to accommodate increasing State Call Centers.

4.5.4 Cloud enabled Data Center Technology Architecture

Both cloud data center should be enabled on public cloud infrastructure. Bidder should ensure that both cloud data center should are located in India. Bidder can opt for cloud data center services from 2 different service providers.

Bidder should ensure that the contact center software and Virtual machine should be hosted together in DC. The indicative representation for the Cloud enabled DC technology architecture is presented below for reference purpose only. PRI lines can be terminated either at Center or State. It is Bidders responsibility to ensure the proposed solution meets all purchaser's requirements.



4.5.4.1 The Cloud enabled Data Centre shall consist of key elements in terms of providing the connectivity to servers and network devices. The internet and intranet zones shall ensure that public and private traffic are handled properly with equipped security.

4.5.4.2 The classification of zones on the firewall shall play an important role to diverge the public traffic by the means of setting up of DMZ zones. The DMZ zone shall receive traffic request from all external users which shall need to access the web services for respective applications

4.5.4.3 The trusted zone on firewall carries all key critical applications and to ensures the critical applications are protected from external attacks.

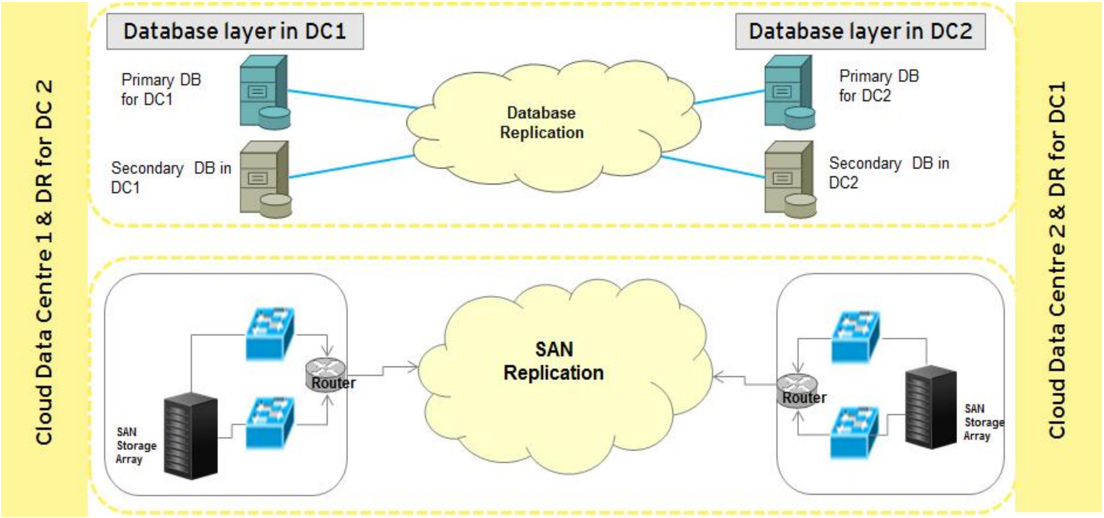
4.5.4.4 The security device has been proposed to ensure the traffic is filtered for all deep packet malicious activity which passes through the firewall.

4.5.4.5 A zone shall be defined on internet router to divert trusted, DMZ, Network management zone respectively. The intranet zone connects directly to MPLS with separate provisioning of IPS, firewall which intercepts all internal traffic which comes from local states.

4.5.4.6 The DCs should have exclusive VPN management system for 20000 users.

4.5.5 Replication Technique

The indicative representation for the replication technique infrastructure and its connectivity is presented below.



4.5.5.1 All data should be replicated between Cloud enabled DC1 and DC2 There shall be no data inconsistencies issues with either cloud enabled data centre sites.

4.5.5.2 The expected RTO from the proposed design would be 0 and RPO to be about 100ms

4.5.6 Field (MDT)

4.5.6.1 MDT devices would be provided to the police vehicles which would be tracked using GSM/GPRS/GPS at data center.

4.5.6.2 Information about the incident would be sent to the field officers through MDT devices in terms of messages, mails and calls

4.5.7 Network

4.5.7.1 Network would form the key component of the entire solution.

4.5.7.2 Network connectivity would be required between Cloud enabled DC sites, Operation Centre and State Call Centers

4.5.7.3 MDT will be connected using GSM/GPRS network

4.5.7.4 The network bandwidth required may be calculated based on the number of users in each state call center location. In this regard the bidder needs to arrive at the bandwidth required by each user / operator. Based on this, bandwidth needs to be provisioned at each of the locations on clause no. 17.3 of this section

4.5.7.5 Bidder needs to size the bandwidth for the following, the below mentioned details may be considered for network estimation

a) DC sites should be connected to the MPLS backbone on an Optical Fibre Channel (OFC) based last mile link from two different service providers.

b) State Call Centres to Data Centre sites should be connected to the MPLS backbone on an Optical Fibre Channel (OFC) based last mile link wherever applicable

c) Operations Centre to Data Centre sites should be connected to the MPLS backbone on an Optical Fibre Channel (OFC) based last mile link wherever applicable

4.5.7.6 The bidder should adequately size the bandwidth requirements between Cloud enabled DC sites considering that the link can adequately take care of backup/ replication traffic between DC sites.

4.5.7.7 The bidder should ensure that the bandwidth estimated and proposed should meet the locations requirements duly meeting the expected performance level. In case of degradation in performance due to bandwidth inadequacy is observed, the bidder shall need to upgrade the bandwidth to the required level at bidders own cost.

4.5.7.8 To meet the requirement for a stable core solution in the future, the network should be scalable. It should also facilitate upgrades to the existing network and networking components, leased line bandwidths and should accommodate additional links. The bidder should determine this scalability which is to be achieved either through the upgrade of hardware modules on the existing routers/switches as per the free slots available.

4.6 Scope of work

4.6.1 The whole project is divided into two phases: implementation phase and operations & maintenance phase

4.6.2 **Implementation phase:** In this phase, Bidder shall provide services for design, customization, installation, commissioning, integration and rollout of the emergency response system. 18 months from the date of signing of contract would be considered as implementation phase. The following services shall be provided by Bidder:

4.6.2.1 Project Planning

4.6.2.2 Supply, installation, configuration, testing and commissioning of compute infrastructure (hardware & software) such as Servers, Operating systems and Databases, Storage at the proposed Cloud enabled Data Center sites, Operations Centre and State Call Centres etc.

4.6.2.3 Testing and commissioning of Network infrastructure at DC sites, Operations Centre and State Call Centres etc.

4.6.2.4 Supply, installation, configuration, testing and commissioning of Security infrastructure like Firewalls, Network Intrusion Prevention Systems etc.

4.6.2.5 Supply, installation, configuration, testing and commissioning of all field hardware including desktops, MDT, printers and IP phones etc

4.6.2.6 Providing PRI lines from TSP which can be dialed from across the nation

4.6.2.7 Providing Network bandwidth at all locations (DC sites, Operations Centre, State Call Centres)

4.6.2.8 Providing TSP connectivity at DC sites and other locations as required

4.6.2.9 Setting up of Operations Centre and State Call Centres

4.6.2.10 Provide Training to agents, dispatchers, supervisors, police officials and other identified staff.

4.6.3 **Operations & Maintenance (O&M) Phase**: In this phase, Bidder would be responsible of operations and maintenance of the entire solution for the contract period. This will be applicable after one state Go-Live. The following services should be provided by Bidder:

4.6.3.1 O&M phase planning and Monitoring

4.6.3.2 Ongoing Administration and Maintenance requirements

- Operation of Operations Centre (including Help Desk)
- Support at DC sites
- Support for NOC and SOC sites
- Maintenance of Solution (hardware, applications, network)

- AMC Applicable after One year of the deployment
- MDT support and state call center support

4.6.3.3 Facility Management Services at States

4.6.3.4 MIS Reports and Incident Reporting

5 Applications

5.1 General Requirements

5.1.1 Bidder should provide redundancy for all applications to avoid single point of failure in the system.

5.1.2 Bidder will be responsible for the generation and submission of necessary documentation required in both phases. Review and approval of Purchaser is required on all such documentation before commencement of activity.

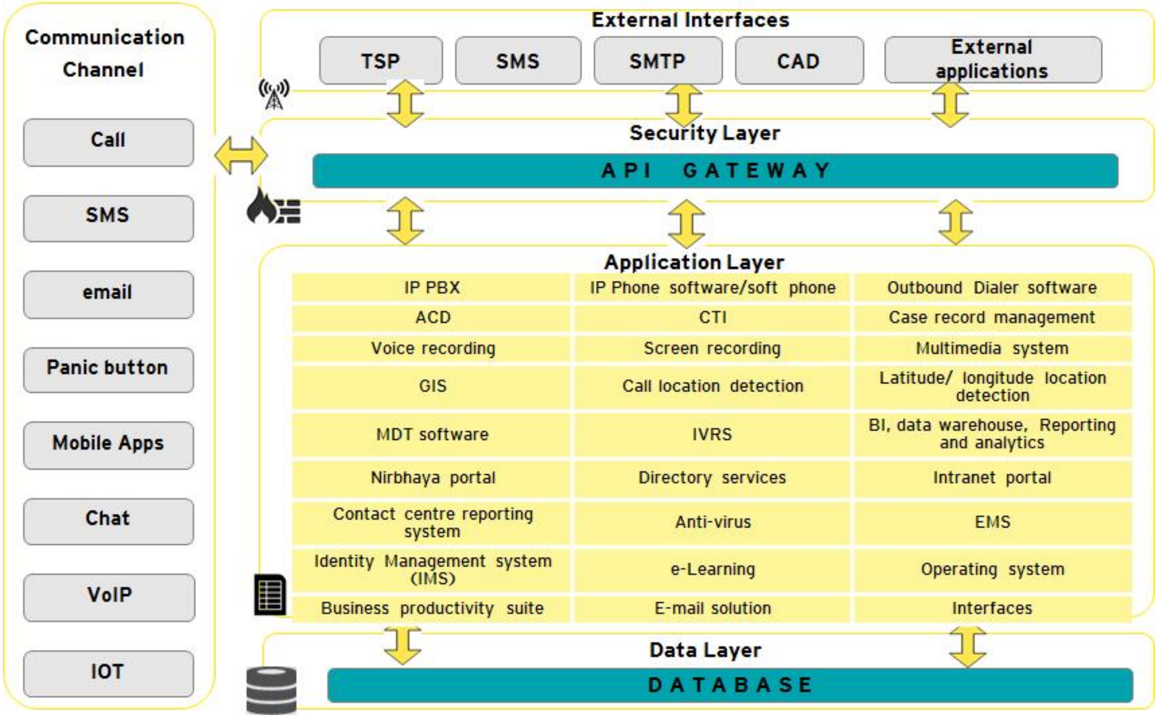
5.1.3 Bidder shall document the baseline configurations for all application equipment & facilities and get it approved from Purchaser prior to commencement of installation. Bidder shall develop and implement a system to maintain these configurations and ensure adequate controls for change management process on an ongoing basis.

5.1.4 Bidder should provide development environment license in the name of the Purchaser for the various tools used by the bidder during the development phase of respective solutions. These tools would typically include Application Development Framework / Environment for custom built and COTS based products, Database Schema Designer, Help authoring tool etc.

5.1.5 Any additional components, sub-components, assemblies, sub-assemblies that would be required to meet the desired performance requirements will have to be provisioned by the bidder at no additional cost to the Purchaser and without any project delays.

5.1.6 Bidder should arrange for necessary tools for bug tracking, defect logging, application performance monitoring, automatic testing etc. to deliver the complete software development and maintenance services.

5.1.7 Indicative application block diagram is provided below.



IP PBX	IP Phone software/soft phone	Outbound Dialer software
ACD	CTI	Case record management
Voice recording	Screen recording	Multimedia system
GIS	Call location detection	Latitude/ longitude location detection
MDT software	IVRS	BI, data warehouse, Reporting and analytics
Nirbhaya portal	Directory services	Intranet portal
Contact centre reporting system	Anti-virus	EMS
Identity Management system (IMS)	e-Learning	Operating system
Business productivity suite	E-mail solution	Interfaces

Contact center cloud should have the following components:

5.2 IP PBX

5.2.1 Bidder is required to deploy IP PBX software to transfer calls received on PRI lines to the IP network.

5.2.2 The software should identify the correct location and automatically route the calls to the respective state call center/ agents.

5.2.3 All outbound calls from the State call center would be routed to PRI lines through IP PBX system

5.2.4 IP PBX system should be scalable in future to receive calls

5.2.5 Redundancy should be built for IP PBX system to avoid single point of failure

5.2.6 IP PBX should ring the IP phone of the identified agent.

5.2.7 Provision to broadcast “Greeting Message” whenever a call is received on the system.

5.3 Outbound Dialer software

5.3.1 The software will be used for the making outbound calls from the Agents to return missed calls, call in case of SMS, email or other input sources.

5.3.2 Automatic Call back: The automatic call back function would enable calling back the missed calls which may be received on the system. It has to work in conjunction with the ACD as well.

5.3.3 Feedback calls: The outbound dialer software should also have a feature to make calls to the caller whose complaints as per system have been closed. The feedback calls will be connected through the ACD with the available agent

5.3.4 Conference facility: This facility would be required in situations wherein the agent makes a conference call with the caller and the field officer from police to connect both on same call for more clarification.

5.4 Automatic Call Distribution (ACD)

5.4.1 Routing of the calls to required State and available agent would be done by ACD.

5.4.2 ACD would employ a rule based routing strategy

5.4.3 ACD should be able to identify available agents and transfer the call accordingly

5.4.4 In event of all agents are engaged, critical calls can be diverted to agent of nearby State based on the rule engine

5.4.5 Call routing to the agents based on the “longest idle basis”

5.4.6 ACD shall seamlessly integrate with IP PBX system

5.4.7 When a call is transferred to the IP phone then the call details should also be simultaneously transferred to CAD software in a pre-defined format.

5.5 Call Telephony Integration (CTI)

5.5.1 CTI will allow interaction between telephone and a computer to be integrated or coordinated.

5.5.2 CTI would run on a server and act as a common interface for integration of all the software applications deployed.

5.5.3 CTI functionality shall support relevant screen pop-ups on the agents’ screen on the basis of call location detection

5.5.4 CTI shall pass events & information of agents’ status & changes in agent status as well as incoming calls to the computer applications

5.5.5 When a call is transferred to the IP phone then the call details should also be simultaneously transferred to CAD software in a pre-defined format.

5.6 Voice recording

5.6.1 The voice recording will happen for all calls.

5.6.2 System should store voice recording of entire conversation between caller and agent both for incoming call and outgoing call even when calls are transferred from one state to another state.

5.6.3 Recording should be stored for 3 months and then recordings should be archived on storage media. This would help in post event analysis and if required for judicial purposes.

5.6.4 System should be designed such that unauthorized person cannot modify/ move/ delete any voice recordings.

5.6.5 Authorized personnel from States should be able to access the recordings as required by them.

5.6.6 System should prepare a case for each voice recording as per a nomenclature to be decided in consultation with the bidder and the Purchaser.

5.6.7 System shall be able to search for the voice recordings through various fields & filters such as date, time, caller name, location, case file number, agent etc.

5.6.8 Voice recording should be accessible in real time.

5.7 Screen recording

5.7.1 The screen capture of flow of screen shared between agent and dispatcher would be recorded with the case file for dispatch cases only.

5.7.2 Recording should be stored for 3 months and then recordings should be archived on storage media. This would help in post event analysis and if required for judicial purposes.

5.7.3 System should prepare a case for each screen recording as per a nomenclature to be decided in consultation with the bidder and the Purchaser.

5.7.4 Authorized personnel from States should be able to access the recordings as required by them.

5.7.5 System shall be able to search for the screen recordings through various fields & filters such as date, time, caller name, location, case file number, agent etc.

5.7.6 System should be deigned such that unauthorized person cannot modify/ move/ delete any screen recordings.

5.7.7 Screen recording should be accessible in real time.

5.8 Multimedia System

5.8.1 Multimedia System would act as an interface to receive the input from various sources such as SMS, email, chats etc. and convert the input to Case Record Management format

5.8.2 It would send notification to the screen of the identified Case Record Management agent.

5.9 Contact Centre Reporting System

5.9.1 Reporting system should have a provision to provide the contact center reports like call handling, Average handle time of the call etc.

5.9.2 System should be able to export the report the report in different kind of format like pdf, text, Xls etc.

5.9.3 This system should be integrated with Business intelligence and Analytics reporting system to analyses the contact center data for purchaser on requirement basis

5.9.4 Search mechanism should be built to index the files and search the available structured and unstructured data.

Non-Contact center solution requirements are as follows:

5.10 IP Phone software / Soft phone

5.10.1 System should allow the agents to log into the IP phone through the software

5.10.2 IP PBX would terminate the call at the IP phone

5.10.3 Incoming call should be flashed on the screen of Case Record Management agent as well, from where it can be attended

5.10.4 IPhone software or soft phone software should be having a feature of echo cancelling.

5.11 Case Record Management

5.11.1 All incoming non-emergency calls/ data messages would be attended by Case Record Management agent and should be reflected in Case Record Management system.

5.11.2 Case Record Management will 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/ IP/ latitude-longitude) or subscription details.

5.11.3 Case Record Management should open pop up window on the screen of agent receiving the call from IP-PBX

5.11.4 After entering the details from the input source (call/ SMS/ email/ mobile application/ chat/ other), agent will create case with unique id and pass on cases as per the standard operating procedure.

5.11.5 Overall the screen of the Case Record Management system will be a user friendly screen and can be customized as per requirement for each state. The customization of the screen would include language/ linguistic changes, personalization etc.

5.11.6 All forms/ information should be available in English, Hindi and one vernacular of the State. The vernaculars are provided in Clause 18.3 of this section of RFP

5.11.7 Case Record Management should have capability to show profile of the other Agents in the same State Call Centre. This profile would include the languages known. In case of language of incoming call/ data message is not known to the attending agent, he/she should be able to transfer the call/ data message to the appropriate agent.

5.11.8 Please refer Section 5A - Software Requirement Specifications for detailed specifications.

5.12 Geographical Information System (GIS)

5.12.1 GIS maps should be of high precision, comprehensive and detailed with roads, house and building level details and should be at a scale of 1:5000

5.12.2 Bidder has to ensure that the GIS Map provides complete details of the cities in various digital vector layers and allows for zoom in/out, searching, and retrieving information capabilities. Bidder has to procure the GIS map and Data on pan India basis.

5.12.3 Bidder 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
- Dynamically Turn On/Off map layers
- Availability in local language

5.12.4 The details procured should have an positional accuracy of up to 20 meters and shall include the following data with attributes:-

- Road Network.
  - National Highway.
  - State Highway.
  - District Roads.
  - City Arterial Roads.
  - Streets.
  - Village roads and Boundary
- Rail Network.
- Administrative boundaries (State, District, Sub-district, Towns, Wards, Village boundaries for a selected district)
  - District & Sub District Boundary.
  - Town Boundaries.
  - Village points.
- Building footprints and names.
- Points of Interest data to include:
  - Health services (Hospitals, Blood Banks, Diagnostics centre, Ambulance Services, Other Medical Services, Fitness & Yoga Centres etc)
  - Community services (fire stations, police stations, banks, ATMs, post offices, educational facilities, Govt. Buildings etc)
  - Business Centres (Shopping malls, markets, commercial complexes etc.
  - Residential areas (Apartments, housing societies etc.)
  - Transportation (bus stops/Terminus, parking areas, petrol bunks, metro stations, seaports, airports etc.)
  - Recreation facilities (Restaurants, theatres, auditoriums etc.)
  - Other utilities such as travel & tourism facilities, religious places, burial grounds, etc.

- Land-Cover
    - Green areas.
    - Open Areas.
    - Water bodies.
- Address layers (Pincode, Locality, Sub-locality, House numbers/ names for selected cities)
- Jurisdiction of Police Stations in discussion with State Police

5.12.5 Data is preferred in Geodatabase (gdb) - compatible for GIS analysis & application development and provision for conversion to other database formats. The shape files of all database features have to be supplied

5.12.6 GIS base maps (specific to each State) should be installed on Dispatcher's work stations at State Call Centres and MDT devices so that the rendering the GIS map at the states level doesn't take much bandwidth. The GIS maps and data replication should happen from central system remotely.

5.12.7 GIS map data would be purchased from third party by the Bidder. Purchaser will not provide map data. Map data needs to be updated periodically from the third party agent. Any update should be pushed to MDT devices as well.

5.12.8 Maps should have capability to tag the history of location. Any previous case recorded for the location should also be available to the dispatcher.

5.13 Location Detection

5.13.1 Bidder has to identify the caller location properly.

5.13.2 SMS: System should be capable to receive the SMS with mobile number and message and detect the location of the sender appropriately.

5.14 GMLC/HLR

5.14.1 The Bidder has to Integrate with the GMLC/HLR database provided by each TSP for supporting Location Based Service (LBS).

5.14.2 Bidder should account for the hardware and network required for connecting to GMLC database for 10 TSPs

5.15 Latitude/ longitude location detection

5.15.1 System should be able to detect the location from the GPS coordinates received from mobile application, IoT, panic button of vehicles etc.

5.15.2 System should have capability to register the mobile applications/ IoT/ devices/ panic buttons etc. before the data can be received from the same

5.16 MDT Software

5.16.1 MDT Software should be security tested and hardened

5.16.2 **GIS**

i. Field officers would be able to access the location of the caller, nearby vehicles, nearby police station etc. on the MDT GIS

ii. MDT GIS would also help in finding shortest route to the incident site

5.16.3 MDT management

i. MDT health including its availability, performance and usage should be continuously monitored

ii. MDT once installed should be discovered by Enterprise Management System

iii. MDT should have various status like available, away, on case, unavailable etc. to let dispatcher know the current availability of MDT vehicle

iv. In case all MDTs under a Police Station are shown as unavailable/ away, it should raise alert to Dispatcher

5.16.4 Please refer Section 5A – Functional Requirement Specifications for detailed specifications

5.17 Cloud services for Interactive Voice Recording System (IVRS)

5.17.1 IVRS to be used for non-emergency number to address the concerns, complaints, feedback, information and direct calls to other services etc.

5.17.2 IVRS can also be used for common emergencies and disaster.

5.17.3 IVRS would help caller in interaction with voice and DTMF (Dual tone multi-flexing signaling) via keypad. Through the IVRS system, caller would easily be able to direct the concern to appropriate agent at the call center.

5.17.4 Based on the identified location of the caller, IVRS would initiate the call in local language. Caller should be able to change the language of the call anytime during the call.

5.17.5 IVRS should be able to queue the calls and provide position number in queue and approximate time to reach agent

5.17.6 Bidder will size IVRS solution as per Purchaser requirements and make it scalable for future.

5.17.7 The menu options for the IVRS number will be finalized in consultation with Purchaser and other stakeholders.

5.18 BI, Data warehouse, Reporting & Analytics

5.18.1 System should be able to extract reports as per requirement of the Purchaser. These reports would assist the supervisor and other senior officials to take decisions. The system shall be able to provide real time reports with refreshed data from the system.

5.18.2 System should be able to collate the data collected through various applications and convert the same in useful information

5.18.3 Open BI tools would help to create the reports and dashboards required to facilitate the monitoring of the entire system, performance check of the system and also to draw patterns of the incident for better resource planning.

5.18.4 There should be a mechanism to conduct non structured search across the database irrespective of any parameter or database structure.

5.18.5 Please refer Section 5A - Software Requirement Specifications for the indicative reports required under each module.

5.19 Nirbhaya Portal

5.19.1 Bidder would develop portal which would be interface provided to the outside world to interact with the emergency response system

5.19.2 Portal should have some standard content as provided by Purchaser

5.19.3 It should provide option to citizen to register their phones/ devices to be able to connect with State Call Centre in case of emergency

5.19.4 It should have provision to initiate email, VoIP, chat with the agent of selected State

5.19.5 Please refer Section 5A - Software Requirement Specifications for detailed specifications.

5.20 Directory Services

5.20.1 Directory services should have a provision to create, update and modify the LDAP directory

5.20.2 It should have a provision to integrate with the Identity and access management

5.20.3 It should be used to define the roles and permission of different kind of users in the system

5.20.4 Directory services should have proper integrations with DNS, DHCP. Email and other infrastructure components and services.

5.20.5 Please refer section 5 A- Software Requirement Specification for detailed specifications.

5.21 Intranet Portal

5.21.1 Intranet portal should have functionality to manage the purchase documents with updated version and categorization of the documents

5.21.2 Intranet portal should have a provision to detect the user roles and permission and show the relevant functionality to the user as per requirement

5.21.3 Intranet portal should have a administrator console to manage all the documents, user and other features of the portal

5.21.4 Please refer section 5 A – Software Requirement Specification for detailed specifications

5.22 Anti-Virus

5.22.1 In order to protect all the desktops, field devices and other solution components from any kind of virus / worm / trojan attack and any other security threat, bidder should provision and implement an enterprise wide Anti-Virus and Anti-Spam solution for all IT asset, which will include the following:

- Agent for Desktop
- Agent for MDT
- Agent for Servers

5.22.2 Bidder should propose the latest version of the proposed Anti-Virus solution available in the market on the day of submission of the bid. However, it is mandatory that bidder should deploy the latest version of the Anti-virus available at the time of implementation in case newer version is available after the submission of bid.

5.22.3 Anti-virus should have auto update feature, it should be able to push signature from the centralized server to all the clients.

5.22.4 The solution should be able to take action based on the category and sensitivity level in which Spam is detected.

5.22.5 Bidder should provide requisite licenses for all the software required for the Anti-virus and Anti-spam Solution.

5.23 Enterprise Management System (EMS)

5.23.1 It is envisaged that the entire IT infrastructure (except Virtual machine) and network at location (DC, Operation center, state, field) shall be managed through this solution.Virtaul machine will be managed by the Cloud management platform.

5.23.2 The agents required for the EMS solution shall be deployed on all the desktops / servers / devices to be monitored.

5.23.3 Bidder shall propose infrastructure that shall be sufficient for leveraging all the capabilities of the EMS suite to the fullest extent

5.23.4 Bidder shall provide requisite licenses for all the software required for the EMS suite, along with EMS database, add-on tools / modules, etc.

5.23.5 EMS solution will be monitored by authorized personnel and bidder is expected to provide adequate training on EMS to the identified personnel.

5.23.6 EMS would be used to automate and monitor SLAs and generate the log of any defaults.

5.23.7 EMS would be used for asset management also.

5.23.8 Please refer Section 5A - Software Requirement Specifications for detailed specifications.

5.24 Identity Management Software (IMS)

5.24.1 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.

5.24.2 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.

5.24.3 The system shall have log data facility for the users which are logging in the system, log out time with IP address etc.

5.24.4 It should be possible to revoke the rights of users as per requirement of Purchaser or other competent authority.

5.24.5 Please refer Section 5A - Software Requirement Specifications for detailed specifications.

5.25 e-Learning

5.25.1 e-Learning capabilities are required to enhance self and anytime learning of the users of Emergency Response system located all across the country.

5.25.2 Bidder shall prepare interactive Online Training Module for the applications and SOPs for the project.

5.25.3 Interactive modules should be available in English, Hindi and one vernacular of the State. The vernaculars are provided in Clause 18.3 of this section of RFP

5.25.4 It should be accessible to all the users of system based on their requirements.

5.25.5 Changes in the training modules of e-Learning should be pushed through centrally.

5.25.6 Please refer Section 5A - Software Requirement Specifications for detailed specifications.

5.26 Webinar (Web conference)

5.26.1 The conferencing solution should be able to provide integrated audio, video and web conferencing.

5.26.2 The conferencing system should support collaboration features like desktop/application sharing, white boarding, annotations, polling, chat, voice and video recording

5.26.3 The conferencing system should be browser-neutral and must be accessible through any internet browser

5.26.4 The conferencing solution should be Operating-System (OS), platform neutral and should be operable on any of the commercially available OS for desktops and mobiles

5.26.5 The conferencing solution must be able to support analytics data that can allow the bidder to optimize the webinar sessions in real-time

5.26.6 System should allow for integration with Social Media platforms for an ability to share the recorded sessions on different social networks for wider dissemination

5.27 Operating System (OS)

5.27.1 Bidder should provide adequate number of licenses of proposed OS for all desktops, servers, MDT and other systems as required.

5.28 E-Mail Solution

5.28.1 An e-Mail solution provides the capability to send emails to internal and internet-type email addresses using an SMTP gateway.

5.28.2 Mail access to be provided to Supervisors at State Call Centre, all Purchaser officials and State Police officials

5.28.3 1,25,000 email addresses would be provided through this solution.

5.28.4 Please refer Section 5A - Software Requirement Specifications for detailed specifications.

5.29 Function Points

5.29.1 Function point is a unit which is used to quantify the amount of business functionality an IT system delivers. Function points are the units of measure used by the International Function Point Users Group ("IFPUG") Functional Size Measurement Method.

5.29.2 These function points would be used for estimating the cost of software development beyond the scope of work of this RFP and in future scenarios

5.29.3 IFPUG measurement method for calculating Function Points would be agreed between Purchaser and Bidder.

5.29.4 Bidder should provide cost of 15,000 Function Points

5.29.5 All function point development will be done by resources not deployed for maintenance.

5.29.6 The cost should be provided in the format provided in Section 4 of this RFP

5.30 Interface with other applications

5.30.1 **States with an existing ER system:** Bidder has to ensure that any call received to Nationwide Emergency Response System would be forwarded to the respective State's Emergency Response number and all other actions would need to be taken by State. System should capture the handing over of call to the State ER system

5.30.2 **Public Safety Answering Points (PSAPs):** PSAP database will be created by the bidder with web interface to view and create this database. Purchaser approval is required before any modification is made in this database.

5.30.3 **State with functioning Dial 181:** The bidder shall ensure that the system will be able to integrate with Dial 181 emergency response already functioning in the States. Incoming calls on 181, which get identified as 'emergency calls', will be transferred to Nationwide Emergency Number. Once, transferred these calls can be forwarded to the dispatcher for necessary action.

Non-emergency calls related to women and child received on Nationwide Emergency Number would be transferred to 181 and follow the standard operating procedures which have been defined for 181.

5.30.4 **State with functioning Dial 100 in some cities:** The bidder shall ensure that calls landing on state level PSAP are transferred correctly to those cities which have functional Dial 100.

5.30.5 **Provision of Video Calling integration:** The bidder shall provision for future requirement of video calling by users. The system should be so designed that users will be able to connect directly to the Call agents for Emergency requirements through video calls. Also dispatcher should be able to have video call with the police officer at the incident location. This would give clear picture to the dispatcher.

5.30.6 **Integration with Gateway Mobile Location Centre (GMLC):** The system should have the functionality for Integration with the GMLC for supporting Location Based Service (LBS). Once this integration is completed, real-time information of the mobile phone user will be provided on the GIS interface of Call Agent/ Dispatcher. For TSP using Wi-Fi hotspots for call connection, integration with Wi-Fi location should be part of scope of work of the bidder.

The system will also be provisioned to be integrated with ALI (Automatic Location Identification) wherein, the registered address of the landlines will be mapped in the system. Therefore, whenever a call is received from Mobile phone/ landline, the Call Agent/ Dispatcher will have an address for responding to the emergency situation.

5.30.7 **Integration with Video Surveillance (City surveillance projects)**

Various States/Cities across India have either installed CCTV surveillance cameras or are in phase of planning for the same. These are being monitored through a Command & Control Center established in the same city. Nationwide emergency response system should be so designed that it should be able to receive IP surveillance camera feeds on the dispatcher screen (third monitor). Only specific feed of identified camera should be streamed to the dispatcher module. The streaming of feed may be done through VPN connectivity over the Internet.

5.30.8 **Integration TETRA/UHV/VHF communication systems**

The state call center should be able to integrate with the standard communication systems of State Police. These communication systems could be TETRA/ UVF/VHF. These will be on requirement basis only.

5.30.9 **Integration with existing and future security apps**

The bidder shall be responsible for integrating the central integrated Emergency Response system with existing and future applications on security like “Himmat” application recently launched by the Delhi Police for the safety of women in New Delhi, “mysecurity.go.in” launched by MHA etc.

5.30.10 **Integration with MoRTH (Ministry of Road Transport and Highways) Nirbhaya system:** The bidder needs to integrate the centralized integrated Emergency Response System with the MoRTH‘s Nirbhaya system that involves setting up an emergency button on Road Transport buses. The integration shall ensure that the exact incident coordinates are sent immediately to the central Operations center and routed to the state call center for quick response to the incident

5.30.11 **Application developed by CAD Software Service Provider:** Bidder has to maintain, make changes and integrate with the purchasers CAD system. High level technical features of CAD system are:

- Java
- Apache

- Postgres
- JBOSS
- Open source and any other supportable CAD technologies

5.30.12 **Provision for government helpline:** CRM, IVRS and related software and database will be the responsibility of the Bidder. The bidder shall setup configure and maintain the government Helpline. Incoming calls on government Helpline which get identified as 'emergency calls', will be transferred to Nationwide Emergency Number. Once, transferred these calls can be forwarded to the dispatcher for necessary action. Non-emergency calls received on Nationwide Emergency Number would be transferred to respective Helpline and follow the standard operating procedures which have been defined for government Helpline. Any existing government helpline will have to be integrated with the system.

5.31 Access to applications

5.31.1 Below provided applications would be accessed by following personnel. Bidder should plan the solution accordingly.

S. No.	Application	Users
1.	Case Record Management / IP Phone software / Softphone	• Voice, Non voice agents, Dispatcher and Supervisor • Relevant personnel at Operations Centre
2.	GIS Map And Map Data	• Purchasers CAD software • Relevant personnel at Operations Centre
3.	SOC/NOC applications	• Relevant personnel at Operations Centre • Relevant personnel at Cloud enabled DC sites
4.	MDT applications	• Field officers in police vehicles
5.	Monitoring Application (Supervisors and Police officials) – Mobile App based	• Supervisors at State Call Centres • Senior Police officials
6.	Monitoring Application (Supervisors and Police officials) – Web based	• Supervisors at State Call Centres • Senior Police officials • SHOs at Station level
7.	EMS/Cloud Management Platform	• Supervisor and FMS personnel at State Call Centre for ticket logging and status updates • SHOs at Station level for ticket logging and status updates • Relevant personnel at Operations Centre • Relevant personnel at Cloud enabled DC sites
8.	Mailing solution	• Email Agents at State Call Centres • Supervisors at State Call Centres • Senior Police officials • SHOs at Station level • Relevant personnel at Operations Centre
9.	e-Learning	• Agents at State Call Centres • Dispatchers and Supervisors at State Call Centres • Senior Police officials • SHOs at Station level • Relevant personnel at Operations Centre

6 Field Hardware

6.1 Desktops/ Workstations

6.1.1 Bidder is expected to provide the desktops with 3 screens for the dispatcher and with single screen for all other agents and officials

6.1.2 The number of desktops required is provided in Clause 17.4

6.1.3 Please refer Section 5B - Technical Requirement Specifications for detailed specifications.

6.2 Laser Jet Printers

6.2.1 Bidder is expected to provide latest printers having copier and scanner functions as well

6.2.2 Printers would be online printers available for all users on LAN

6.2.3 The number of printers required is provided in Clause 17.4

6.2.4 Please refer Section 5B - Technical Requirement Specifications for detailed specifications.

6.3 UPS

6.3.1 Bidder shall provision for a centralized UPS at each of the State Call Centre and Operations Centre.

6.3.2 The number of UPS required is provided in Clause 17.4

6.3.3 Please refer Section 5B - Technical Requirement Specifications for detailed specifications.

6.4 Mobile Data Terminal (MDT)

6.4.1 All the identified police vehicles would have MDT device to track location of the vehicle and provide required instructions to it.

6.4.2 All the instructions/ communication to be made by the system would be delivered to field officers through MDT

6.4.3 This device would send the location periodically to the system

6.4.4 Bidder is required to quote for rugged and non-rugged MDT devices as per the commercial format from 2 separate vendors.

6.4.5 The number of MDT required is provided in Clause 17.4. However MDTs would be procured based on the State requirement.

6.4.6 Please refer Section 5B - Technical Requirement Specifications for detailed specifications.

6.5 Video wall

6.5.1 Video wall (3 columns and 2 rows) shall be setup at the Operations Centre to monitor performance of the system.

6.5.2 The Video wall should be able to display analytics on the operations of Emergency Response System across all the states

6.5.3 Please refer Section 5B - Technical Requirement Specifications for detailed specifications.

6.6 IP phones

6.6.1 Each agent, dispatcher and supervisor would have an IP phone

6.6.2 IP phone would be available with wireless headset gear for convenience.

6.6.3 The number of IP phones required is provided in Clause 17.4

6.6.4 Please refer Section 5B - Technical Requirement Specifications for detailed specifications.

7 Technical Requirement of Solution

7.1 Schedule of Requirements

7.1.1 The ICT infrastructure at the Cloud enabled DC1 and DC2 site will require various set of components for running the CAD ,contact center and other applications as mentioned in this section of RFP. The bidder should propose solution that is in accordance with the RFP Tender specifications.

7.1.2 The Bidder will be required to provide an infrastructure which is scalable and provides for latest technologies like virtualization, cloud computing etc. The Bidder is free to add any additional components that are deemed necessary for providing the solution as a whole.

7.1.3 Size and provision the bandwidth requirements across locations considering the application performance, replication, data transfer and other requirements.

7.1.4 Liaise with service providers for commissioning and maintenance of the links.

7.1.5 Size and provision the cloud infrastructure in line with business operations load of contact center.

7.1.6 Purchaser may at its sole discretion evaluate the cloud infrastructure sizing document. The bidder needs to provide necessary explanation for sizing document to the Purchaser

7.1.7 All billing of servers, storage, contact center, IVRS and security at DC will be cloud based.

7.1.8 Storage requirements for the application suite will have to be assessed by the bidder and the storage solution shall be sized accordingly.

7.1.9 All business critical hardware, applications (hardware and software licenses) and other devices are required to be in High Availability to avoid single point of failure.

7.1.10 The solution architecture should have No Single Point of Failure and shall be committed for uptime as per SLAs.

7.1.11 For cloud offering, Bidder shall offer latest and proven technologies that are available for items including but not limited to Processor model with higher clock speed processor, I/O, Memory, Cache, FC interface and bandwidth, Security products, etc.

7.1.12 The power supplies, cables/connectors for all servers / equipment should be for Indian power specifications of voltage, frequency and phasing.

7.1.13 The Bidder should ensure that all the peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to the devices, equipment, accessories, patch cords (copper/fibre), cables software, licenses, tools, etc. should also be provisioned according to the requirements of the solution..

7.1.14 Bidder should design architecture for implementation of the replication of data between cloud enabled DC sites. It is expected that bidder will draw knowledge from industry best practices and its experiences to implement the replication solution and BCP policy that is best suited for the critical applications. Bidder shall document the blueprint for BCP policy and cohesive replication architecture and obtain approval from the purchaser prior to actual implementation.

7.1.15 Bidder shall assist the purchaser in audit of replication envisaged to be undertaken every quarter. Bidder must provide all information, replication logs in a readily accessible manner as requested by the purchaser as part of this exercise.

7.1.16 Purchaser will not be responsible if the Bidder has not provisioned for any components, sub-components, assemblies, sub-assemblies as part of bill of material in the bid. The Bidder will have to provision to meet the solution requirements the same at no additional cost and time implications to the purchaser.

7.1.17 All applications will be hosted in active –active mode at cloud DCs and the load balancer will ensure high availability.

7.1.18 Please refer section 5B for more detail on cloud hosting specification.

7.2 Cloud enabled Data Centre IT infrastructure

Following indicative IT components are proposed at the Cloud enabled Data Centre sites which follows the cloud hosting specification.

7.2.1 **PRI lines:**

i. Bidder has to ensure end to end call connectivity with the maximum latency of 200 ms. Which is from the caller to the Agent.

ii. Bidder needs to procure PRI lines from more than one TSP for providing redundancy with each TSP having it's own Backup line.

7.2.2 **VPN:** VPN service needs to be enabled to cater remote users for at least 20000

7.2.3 Web Application Firewall

i. A web application firewall (WAF) appliance should be provisioned by the bidder in their solution that applies a set of rules to an HTTP conversation.

ii. The Web Application firewall that the bidder will provision should be able to provide protection against OWASP top ten vulnerabilities at the minimum.

7.2.4 Next Generation Firewall

i. A Next-Generation Firewall (NGFW) should be provisioned by the bidder that combines a traditional firewall with other network device filtering functionalities such as deep packet inspection ,an intrusion prevention system and/or other techniques such as SSL and SSH interception, website filtering, QoS/bandwidth management and antivirus inspection.

7.2.5 Network Intrusion Prevention System

Network Intrusion Protection System (IPS): An intrusion protection system to be provisioned by the bidder to detect several types of malicious behaviors that can compromise the security and trust of the ICT system.

7.2.6 Host based Intrusion Prevention System (HIPS)

i. A host-based intrusion prevention system is an Intrusion Prevention System which monitors the host for suspicious activity by analyzing events occurring within that host. The bidder is required to provision a host based HIPS as a part of its solution.

7.2.7 Anti- APT Solution

i. An Anti-Advanced Persistent Threat (Anti-APT) solution is to be provisioned by the bidder to protect against Advanced Persistent attacks including zero day vulnerabilities.

7.2.8 Data Leakage Prevention (DLP)

i. Data leakage prevention solution is a system that is designed to detect potential data breach / data ex-filtration transmissions and prevent them by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage). In data leakage incidents, sensitive data is disclosed to unauthorized personnel either by malicious intent or inadvertent mistake. The bidder is required to provision a DLP solution as a part of its solution.

7.2.9 **Database Activity Monitoring**

i. Database Activity Monitoring technology all activity on the database and provides alerts and reports on that activity. It essentially is the observation of actions in a database. A DAM tool monitors, captures and records database events in near-real time and provide alerts about policy violations. The bidder needs to provision for a Database Activity Monitoring tool

7.2.10 **Database:** The database/repository provides all the relevant information required to process the applications. Database server would be required to store and access data with ease. This would also be integrated with multiple applications, residing at the Cloud enabled DC1 and DC2 site.

7.2.11 **Document Repository:** The document repository provides the version controlling of all kind of documents like latest development code, designs document etc. of the applications. It would require to store and access the document with ease. The Bidder may use open source technology as per requirement.

7.2.12 **Web Server:** The web server would be used for providing access to the applications through internet / intranet. Using portal, relevant contents of the applications can be easily enabled, updated and deployed at the earliest. Portal would provide a base template to users who want to access the application via internet. The portal server shall allow users to access the application from internet and the same shall be configured in cluster mode.

7.2.13 **Development and Test Environment:** It would be required to deploy a separate set of VM on separate VLAN for Development and Test environment where all the new services will be developed and deployed before it is brought on to the staging and production servers. There shall be provision of the hardware for separate Development and Test System for each software application so that staging and 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 in 3-tier architecture with hardware as per sizing from respective application vendors.

7.2.14 **Staging Environment / Pre-Production:**

A staging environment or Pre-Production 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. It would be required to deploy a separate set of VM on separate VLAN for staging environment

7.2.15 **Production Environment:**

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

i. Plan releases as per the requirements for the approved changes

ii. Build release packages for the deployment for approved changes into production

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

iv. Effectively communicate and manage expectations of the customer/internal stakeholders/end customer during the planning and rollout of new releases

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

vi. Deploy the release as per release guidelines

7.2.16 **SAN Storage**

i. Storage requirements for the application suite will have to be assessed by the bidder and the storage solution shall be sized accordingly.it should be SAS drive.

7.2.17 **Backup storage:** Backup storage would be used for backing up the key data on regular interval. The backing up of the data would be an automated process. Whenever desired the backed up data can be restored/retrieved to the desired system configuration. Short term backup storage should be provided on SATA and long term on tapes.

7.2.18 **Enterprise Management System:** Bidder has to provide tools which include features but not limited to Incident Management, Patch management, Asset Management, Server, Storage, Network Infrastructure performance and availability monitoring . The tool should be capable to support monitoring of multi-vendor and multi-platform infrastructure devices.

7.2.19 **SMS Service:** Both incoming and outgoing SMS service needs to be provided by the Bidder.

8 Operations Center

8.1 General Requirements

8.1.1 Bidder has to set up Operations Center (OC) to perform the following activities:

8.1.1.1 Set up NOC and SOC services to monitor and control the network and security operations for the entire project.This will augment Cloud service providers SOC and NOC center.

8.1.1.2 Set up IT Help Desk, Reception and Visitor gallery.

8.1.1.3 Monitor usage and performance of Emergency Response solution.

8.1.2 Bidder has to set up OC at the allocated place by the purchaser or Bidder has to setup OC at his own identified(approved by the purchaser) location till Purchaser allocates space for the same. The site preparation in both the circumstances is bidder's responsibility

8.1.3 The OC will provision for an IT Helpdesk to facilitate users on their day to day activities. OC 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 NOC and SOC will be manned 24X7X365 for the duration of the contract.

8.1.4 The tools required for the NOC and SOC will be hosted in the Data Center (DC) sites while the Operations Center (OC) will be at a different location in Delhi/NCR.

8.1.5 Bidder shall develop the NOC and SOC operating procedures in adherence with Purchaser's applicable policies and guidelines.

8.1.6 The bidder has to ensure that at minimum two factor authentication based access controls are followed for NOC and SOC operations.

8.1.7 Bidder shall be responsible for supply, installation, configuration, testing, commissioning, operations and maintenance of network infrastructure items for the Operations Centre:

Please refer section 5B - **Technical Requirement Specifications** for IT infrastructure requirements for Operations Centre.

8.2 Network Operations Centre

8.2.1 The NOC will analyze 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. 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.

8.2.2 The bidder should develop Services catalog for NOC and get a sign off on the same from Purchaser.

8.2.3 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

8.2.4 **Features of NOC**

8.2.4.1 Incident Management based on resource workload, incident Category etc.

8.2.4.2 Creates service request or incident tickets when new request will come from state call centers.

8.2.4.3 Tracking and reporting of all contractual SLAs in an automated way.

8.2.4.4 Updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.

8.2.4.5 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.

8.3 **Services to be provided through NOC**

The Services Catalog for the NOC has to be prepared by the bidder and get a sign off from Purchaser. Indicative list of services that have to be provided through the NOC are mentioned below.

8.3.1 **Monitoring, Management & Reporting with Enterprise Management System (EMS)**

The EMS system should provide 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 bidder will be under the supervision of Purchaser. The EMS system must have the following features including but not limited to and as well act as authoritative source for the same:

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.

8.3.2 **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:

8.3.2.1 **Discovery, Configuration and Faults**

i. Monitoring and Management

- 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
- The proposed system must support exclusion of specific IP addresses or IP address ranges.
- The system should provide discovery & inventory of physical network devices like

Layer-2 & Layer-3 switches, Routers and other IP devices and should provide mapping of LAN & WAN connectivity.

- The discovery should be able to identify and model of the ICT asset.
- 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.
- The proposed system must determine device availability and should exclude outages from the availability calculation with an option to indicate the reason.
- The proposed system should provide out of the box root cause analysis.
- 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.
- 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.
- The proposed solution must have the ability to collect data from the virtual systems without solely relying on SNMP.
- The proposed solution must support an architecture that can be extended to support multiple virtualization platforms and technologies.
- The proposed system must support SNMPv3-based network discovery and management out-of-box without the need for any external third-party modules.
- 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 & startup configuration, Upload configuration etc.

ii. Reporting

- 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.
- The proposed system must able to perform real-time or scheduled capture of device configurations. It should also provide features to capture, view & upload network device configuration.
- The proposed system must 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.
- The proposed system should be able to monitor compliance & enforce change control policies within the diverse infrastructure by providing data & tools to run compliance reports, track & remediate violations, and view history of changes.
- 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.

8.3.2.2 Service Level Management

i. Monitoring and Management

- The proposed service management system should provide a detailed service dashboard view indicating the health of each of the departments / offices in the organization and the health of the services they rely on as well as the SLAs.
- 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.
- 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/Departments/ Organizations with the services they rely on and related Service/Operational Level Agreements. Presently, services shall include E-mail, Internet Access, Intranet and other services hosted.
- 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).
- SLA violation alarms must be generated to notify whenever an agreement is violated or is in danger of being violated.
- 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.

ii. Reporting

- 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.
- 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.
- 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.
- 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.

8.3.3 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 unified reporting interface for network components.

8.3.3.1 Network Performance Monitoring, Management and Reporting

i. Monitoring and Management

- 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 & availability to define service levels and further improve upon them.

- The tool should provide a live exceptions list displaying the various health and threshold exceptions that are occurring in the managed infrastructure.
- The tool should have the capability to configure different polling speeds for different devices in the managed infrastructure with capability to poll critical devices
- The proposed system should use intelligent alarm algorithms to learn the behavior of the network infrastructure components over a period of time

ii. Reporting

- The Network Performance Management console must provide a consistent report generation interface from a single central console.
- 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
- The proposed system should enable complete customization flexibility of performance reports for network devices and monitored servers.
- 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.
- 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, Packets out etc.
- The Proposed Performance Management must provide charts for Health Reports like:
- 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.
- 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.

8.3.3.2 Application Performance Monitoring, Management and Reporting

i. Monitoring and Management

- 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
- 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.
- The proposed solution should correlate performance data from HTTP Servers (external requests) with internal application performance data

- 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
- The proposed Solution must be able to correlate Application changes (code and configuration files) with change in Application performance.
- The proposed solution should allow data to be seen only by those with a need to know and limit access by user roles
- The proposed solution should measure the end users' experiences based on transactions
- The proposed solution should give visibility into user experience without the need to install agents on user desktops.
- The solution should be deployable as an appliance-based system acting as a passive listener on the network thus inducing zero overhead on the network and application layer.
- 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.

ii. Reporting

- 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
- The proposed system must be able to instantly identify whether performance problems like slow response times are within or outside the data center without having to rely on network monitoring tools.
- 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.

8.3.3.3 Systems and Database Performance Monitoring, Management and Reporting

i. Monitoring and Management

- The proposed system should addresses management challenges by providing centralized management across physical and virtual systems
- 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.
- It should be possible to configure the operating system monitoring agents to monitor based on user-defined thresholds for warning/critical states and escalate events to event console of enterprise management system.
- 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.
- The proposed solution should support monitoring Processors, File Systems, Log Files, System Processes, and Memory etc.
- 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

- 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.
- The proposed database performance management system shall integrate network, server & database performance management systems and provide the unified view of the performance state in a single console.
- It should be able to automate monitoring, data collection and analysis of performance from single point.
- 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.
- The Monitoring tool should support database performance agents for performance reporting of standard RDBMS like Oracle, MS-SQL, Sybase and DB2.
- 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.

ii. Reporting

- The proposed system must provide Performance Management and Reporting — Provides real-time and historical performance of physical and virtual environments enabling customers 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 .
- Role based Access — Enables role-based management by defining access privileges according to the role of the user.
- The proposed Virtual Performance Management system must integrate latest virtualization technologies

8.3.4 Helpdesk - Monitoring, Management and Reporting

8.3.4.1 The proposed helpdesk system must provide flexibility of logging, viewing, updating and closing incident manually via web interface.

8.3.4.2 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.

8.3.4.3 Each incident must be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.

8.3.4.4 The proposed helpdesk system must be able to provide flexibility of incident assignment based on the workload, category, location etc.

8.3.4.5 Each escalation policy must allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no or minimum programming.

8.3.4.6 The proposed helpdesk system must provide grouping access on different security knowledge articles for different group of users.

8.3.4.7 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.

8.3.4.8 The proposed helpdesk system must support tracking of SLA (service level agreements) for call requests within the help desk through service types.

8.3.4.9 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.

8.3.4.10 The proposed helpdesk system must integrate tightly with the Knowledge tools and CMDB and should be accessible from the same login window.

8.3.4.11 It should support remote management for end-user & allow analysts to do the desktop sharing for any system located anywhere, just connected to internet.

8.3.4.12 Remote desktop sharing in the system should be agent less & all activity should be automatically logged into the service desk ticket.

8.3.4.13 It should allow IT team to create solution & make them available on the end – user login window for the most common requests

8.3.5 **Traffic analysis**

8.3.5.1 The proposed system should enable the Cloud enabled 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.

8.3.5.2 The traffic analysis system must be from same OEM providing Network Fault & Performance Management System.

8.3.5.3 The tool must support Flow monitoring and traffic analysis for NetFlow, J-Flow, sFlow, Netstream, IPFIX technologies.

8.3.5.4 The solution must provide a central web based integration point for NetFlow based reporting and able to report from a single console across 100,000 interfaces.

8.3.5.5 The solution should be of the type passive monitoring without a need to install any probe or collector for data collection.

8.3.5.6 The solution must provide the following NetFlow based metrics:

8.3.5.7 Rate,Utilization,Byte Count,Flow Count,IP hosts with automatic DNS resolution,IP conversation pairs with automatic DNS resolution,Router/interface with automatic SNMP name resolution,Protocol breakdown by host, link, ToS or conversation,Utilization by bit pattern matching of the TCP ToS field,AS number,BGP next hop address,IPv6 addresses

8.3.5.8 The proposed solution must keep historical rate and protocol data for a minimum of 12 months (most recent) in its current long term operating database. All data in that database must have a maximum 15 minute window granularity without roll up. A user must be able to select any 15 minute window over the last 12 months and display unique utilization and protocol data for every monitored interface.

8.3.5.9 The proposed solution must 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 must have a maximum 1 minute window granularity. A user must be able to select any 1 minute window over the last 30 days and display unique utilization and protocol data for every monitored interface.

8.3.5.10 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.

8.3.5.11 The proposed solution must keep and report on unique hosts and conversations per day for each monitored interface.

8.3.5.12 The system must maintain this custom ToS based information for each interface for at least 12 months at a minimum 15 minute granularity.

8.3.5.13 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.

8.3.5.14 All reports should be generated and displayed directly by the system from a common interface.

8.3.5.15 The system should allow via API for Excel to download data to generate reports.

8.3.5.16 The system must be able to restrict views and access for defined users to specific routers, interfaces, and reports.

8.3.5.17 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.

8.3.5.18 Search for any traffic using a specific configurable destination port, or port range, autonomous system (AS) number, BGP next hop IP address, ToS bit, clients or servers that are experiencing more than a specified number of TCP resets per hour, IPv4 or IPv6 conversation bad IP Header, unreachable destination, TTL expired, traceroute requests, MAC addresses, TCP flags, VLAN.

8.3.5.19 The proposed system must be capable of automatically detecting anomalous behavior such as virus attacks or unauthorized application behavior. The system should analyze all NetFlow traffic and alert via SNMP trap and syslog of any suspicious activity on the network..

8.3.5.20 NetFlow collection device must support a minimum of 5 million flows per minute up to 9 million flows per minute and be capable of storing gathered information in a common database where all long term reporting information is held.

8.3.5.21 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.

8.3.5.22 The proposed system must be capable of sending alerts via SNMP trap. Alerts should the having the following configurable parameters:

8.3.5.23 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.

8.3.5.24 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.

8.3.5.25 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.

8.3.5.26 This page should display a graph representing the total number of NetFlow flows that the data was derived from. It must represent flows for the selected period of time, for this interface.

8.3.5.27 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.

8.3.5.28 The monthly view must provide a graphical representation of the level of utilization for each fifteen minute interval of each day of the month.

8.3.5.29 The user must be able to easily change the data type of the main interface view to a tabular format showing the increase or decrease of traffic generated by that protocol as a percentage using discrete least-squares approximation to find a best fit line of growth

8.3.6 Asset Management through EMS

8.3.6.1 Ability to provide inventory of hardware and software applications on end-user desktops, MDTs including information on processor, memory, OS, mouse, keyboard, etc. through agents installed on them

8.3.6.2 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

8.3.6.3 Ability to provide the facility to collect custom information from desktops

8.3.6.4 Ability to provide facility to recognize custom applications on desktops

8.3.6.5 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

8.3.6.6 Facility for User self-registration.

8.3.6.7 Ability to support configuration management functionality using which standardization of configuration can be achieved of all the desktops

8.3.6.8 Software metering should be supported to audit and control software usage. Should support offline and online metering.

8.3.6.9 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

8.3.6.10 Ability to use the query tool to identify specific instances of concern like policy violation (presence of prohibited programs / 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.

8.3.6.11 Facility to track changes by maintaining history of an asset

8.3.6.12 Ability to have web based console

The proposed EMS 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. Purchaser must provide the specifications and numbers for all necessary Hardware, OS & DB (if any) which is required for an EMS to operate effectively.

8.3.7 Incident Management and RCA Reporting

8.3.7.1 Incident management will be governed by the change management and configuration management policy of MHA. The policy will be shared with the successful bidder.

8.3.7.2 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 / misuse of systems by staff, loss of power / communications services and errors by users or computer staff) should be dealt with in accordance with a documented information security incident management process.

8.3.7.3 Incidents should be categorized and prioritized. While prioritizing incidents the impact and urgency of the incident must be taken into consideration.

8.3.7.4 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.

8.3.7.5 Testing should be performed to ensure that recovery action is complete and that the service has been fully restored.

8.3.7.6 The bidder should keep the end users informed of the progress of their reported incident.

8.3.7.7 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.

8.3.7.8 Information security incidents and weaknesses associated with information systems should be communicated in a manner allowing timely corrective action to be taken.

8.3.7.9 The bidder should conduct regular reviews on performance of incident management activities against documented Key Performance Indicators (KPI's).

8.3.7.10 The incident management activities should be carried out by the bidder in such a way that an incident is resolved within the agreed time schedule.

8.3.7.11 Root Cause Analysis (RCA) should be conducted by the bidder.

8.3.7.12 Controls related to incident management need to be implemented and each implemented control should have a documentary evidence to substantiate and demonstrate effective implementation.

8.3.8 Change and Configuration Management

8.3.8.1 Change and configuration management will be governed by the change management and configuration management policy of MHA. The policy will be shared with the successful bidder.

8.3.8.2 Change management provides information on changes, and enables better control of changes to reduce errors and disruption in services.

8.3.8.3 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.

8.3.8.4 The bidder shall ensure that all changes are logged, prioritized, categorized, assessed, authorized, planned and scheduled to track and report all changes.

8.3.8.5 Ensure review of changes for effectiveness and take actions agreed with interested parties. Requests for change should be analyzed at planned intervals to detect trends. The results and conclusions drawn from the analysis should be recorded and reviewed to identify opportunities for improvement.

8.3.8.6 Controls related to change management need to be implemented and each implemented control should have a documentary evidence to substantiate and demonstrate effective implementation.

8.3.8.7 The roles and responsibilities of the management should include review and approval of the implementation of change management policies, processes and procedures.

8.3.8.8 A configuration management database should be established which stores unique information about each type Configuration Item CI or group of CI.

8.3.8.9 The Configuration Management Database (CMDB) should be managed such that it ensures its reliability and accuracy including control of update access.

8.3.8.10 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.

8.3.8.11 Corrective actions shall be taken for any deficiencies identified in the audit and shall be reported to the management and process owners.

8.3.8.12 Information from the CMDB shall be provided to the change management process, and the changes to the CI shall be traceable and auditable.

8.3.8.13 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.

8.3.8.14 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.

8.3.9 EMS Ability to integrate with other services

8.3.9.1 The proposed EMS solution must comply with key integration points out of the box as listed below but not limited to:

8.3.9.2 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 created prior to submitting the ticket. NMS console must show associated helpdesk ticket number for the alarms that generated those tickets.

8.3.9.3 SLA's violation on monitored end user response time must open a helpdesk incident out of the box.

8.3.9.4 Proposed Application Performance Solution must integrate with Network Fault Monitoring Solution to forward Application Performance Threshold violation alarms in proposed Network Fault Manager Console.

8.3.9.5 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:

- Manually creates tickets when requested by Fault Management GUI operators
- Automatically creates tickets based on alarm type
- Provides a link to directly launch a Service Desk view of a particular ticket created by alarm from within the Network Operation console.
- 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.

8.3.9.6 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.

8.3.9.7 The proposed virtual performance management system should integrate with proposed Network Management and Performance Management system out of the box.

8.3.9.8 The proposed NMS should provide unified workflow between the fault and performance management systems including bi-directional and context-sensitive navigation, such as

8.3.9.9 Navigate from the Topology View to At-a-Glance or Trend Reports for any asset

8.3.9.10 Navigate from the Alarm View to At-a-Glance, Trend or Alarm Detail Reports

8.3.9.11 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 bidder must use Industry standard EMS tools recognized by analysts (like Gartner, Forrester etc.) to report desired SLA's for availability & 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/seamless integration and out of the box workability of the offered solution.

8.3.10 **ICT Assets Hardening**

8.3.10.1 All the ICT assets should be hardened as per the Hardening guidelines and industry leading practices.

8.3.10.2 Remove all unauthorised software, utilities, and services.

8.3.10.3 All required logs should be configured and monitored

8.3.11 **Identity Management Services**

8.3.11.1 IDM services should have tight integration with Directory service, which acts as exclusive User repository and directory services for the entire infrastructure.

8.3.11.2 IDM should understand the domain schema and have integrations with Devices and applications for Authentication and Authorization services across the network.

8.3.11.3 IDM should have the feature either to publish or accommodate Organization Group policy publishing.

8.3.11.4 The Identity Manager architecture should be an N Tier Architecture to allow portability between Operating systems and Application servers.

8.3.11.5 Solution must be comprehensive with user provisioning, de-provisioning and password management tools

8.3.11.6 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. Bidder should own the responsibility for the Identity & 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

8.3.11.7 The solution for identity lifecycle management should support Web Services standards

8.3.11.8 Provisioning tool must support and provide business role based provisioning.

8.3.11.9 IDM solution should take care of Privileged user access management, single sign on, effective governance mechanism on complete User Management life cycle.

8.4 **IT Infrastructure at the NOC**

8.4.1 The bidder has to ensure the proposed NOC services can be operated from NOC.

8.4.2 Bidder has to provide required Desktops with OS and other relevant software.

8.4.3 Bidder has to provide the required network connectivity to operate NOC.

8.5 **Security Operations Centre**

8.5.1 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.

8.6 **Services to be provided through SOC**

8.6.1 The Services Catalog for the SOC has to be prepared by the bidder and get a sign off from Purchaser. Indicative list of services that have to be provided through the SOC are mentioned below.

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

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

- 24/7 security monitoring
- Threat intelligence
- Log collection and management
- Event correlation
- Rapid response to incidents & forensics
- Patch Management,
- VA and PT Management.
- Perimeter Security Management

8.6.4 Bidder should 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 Bidder to stop the attacks. Bidder will provide the services using the SIEM platform procured by Purchaser and through its dedicated personnel & processes based out of the Security Operations center of Purchaser.

8.6.4.1 Bidder 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/complete set of events. Bidders should indicate their event list in proposal response.

- Buffer Overflow attacks
- Port & vulnerability Scans
- Password cracking
- Worm/virus outbreak
- File access failures
- Unauthorized server/service restarts
- Unauthorized changes to firewall rules
- Unauthorized Bidder access to systems
- SQL injection
- Cross site scripting

8.6.5 Bidder operations team at Purchaser should send alerts with details of mitigation steps to designated personnel within Purchaser and any identified service provider of Purchaser.

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

8.6.7 Bidder 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 Purchaser. Team should send customized alerts advisories to respected teams in Purchaser.

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

8.6.9 Bidder should add/delete/modify rules, reports and dashboards based on Purchaser requirements

8.6.10 Bidder should provide backend support to the onsite team from its own SOC. Such support at the minimum include

- Managing escalations from onsite team for detection & response to new threats & complex attacks that onsite team is unable to resolve.
- For adding new/updated threat scenarios and other best practices in Purchaser’s SIEM tool for detection & response based on Bidder SOC visibility & experience across other customers.
- Forensic analysis of attacks/incidents including making available specialists, domain experts, tools.

8.6.11 Bidder should identify threat and incident patterns and devise mitigation plans for the same to facilitate Threat intelligence.

8.6.12 Bidder 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.

8.6.13 **Vulnerability Assessment:** This section provides an outline of the various items to be investigated during our Vulnerability Assessment phase. The said activities should follow the various guidelines for cyber security including Purchaser policies and guidelines, NCSP, IT Act and Cert-In Guidelines. This part has to be offered by the bidder as a service. The bidder does not have to procure a tool for Purchaser for this service. The bidder is required to provision for tools/software/hardware/appliance as a part of its technical solution that have the required technical specifications to ensure quality. The required technical specifications have been mentioned in the Section 5B – Technical Requirement Specifications.

The activities performed should be included but not limited to the following:

- Web Application based vulnerability assessment: To provide proper evaluation of security vulnerabilities associated with web applications – Apache, IIS, Tomcat, Sun and Oracle, thereby, recommend solutions to problems.
- OS level vulnerability assessment: To provide proper evaluation of security vulnerabilities associated with operating systems – Unix, Linux, Sun OS, Windows, thereby, recommend solutions to problems.
- Database Vulnerability assessment: To 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.
- The bidder has to be provision for authenticated mode VA. This will include assessment by providing credentials of assets in the VA process.
- Android Vulnerability Assessment – The bidder shall provide the facility of Vulnerability Assessment of Android platform that will be running on the MDTs.

8.6.14 **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 bare 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:

- Network Security
- Network Surveying
- Port Scanning

- System Identification
- Services Identification
- Vulnerability Research & Verification
- Application Testing & Code Review
- Router Testing
- Firewall Testing
- Intrusion Detection System Testing
- Trusted Systems Testing
- Password Cracking
- Denial of Service Testing
- APT Testing

Penetration Testing shall be done for either sample of MDT 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 MHA and the successful bidder.

8.6.15 **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 & configuring all appropriate security features. The entire scope of this service will differ on different Operating System basis.

8.6.16 **Secure Code Review**

- Code review is a way of ensuring that the application has been developed so as to be “self-defending” in its given environment. It is a method of assuring application developers are following secure development techniques.
- This part has to be offered by the bidder as a service. The bidder does not have to procure a tool for Purchaser for this service. The bidder is required to provision for tools/software/hardware/appliance as a part of its technical solution that have the required technical specifications to ensure quality. The required technical specifications have been mentioned in the Section 5A – Technical Requirement Specifications.

8.6.17 **Infrastructure Security Management:** The Bidder 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 Bidder will be under the supervision of Purchaser.

8.6.18 **Firewall Monitoring and Management**

- Installation and maintenance of the firewall
- Firewall Hardening with initial configuration
- Performance Monitoring
- Regular Monitoring of the LAN errors
- Firewall Rule based policy changes

- Create and maintain Network Access Policy (NAP) document (the access specification) agreed between the parties from time to time.
- Log File review and analysis of information on traffic flow
- Log File trend upgrade and analysis
- Compliance Testing
- Design, configure and maintain all Network Address Translation (NAT) services.
- Access control management through creation of the Network Access Policy and firewall rules
- Implementation and maintenance.
- Manage access to F/W logs policies and performance statistics for viewing through secure web portals in conjunction with SOC tools
- 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
- Incidence response
- Lifecycle Management of all Hardware and Software components
- Firewall Backup

8.6.19 Virtual Private Network Monitoring and Management

- Configuration and maintenance of the VPN gateway to meet customer's specific requirement of VPN - Client to Site and Site to Site.
- Monitoring of the local and remote VPN gateway availability
- Monitoring of the VPN tunnel availability through artificial traffic inside the VPN tunnel
- Monitoring of the VPN tunnel delays and detection of slow VPN connections
- Transparent VPN tunnel (virtual connection) between pairs of sites using technology specification
- Cryptographic services according to IPsec specification with strong encryption and pre-shared secrets authentication.
- Access control management through creation of the Network Access Policy and firewall rules

8.6.20 Network Based Intrusion Prevention System - Monitoring and Management

- Traffic Profiling
- Define Alert levels and Incident response level
- Root cause analysis
- Technical support
- Monitor NIPS for 24*7 availability
- Restore NIPS availability
- Determine Intrusion occurrence
- Upgrade of vendor provided intrusion signatures
- Provide security event correlation(Need SOC)
- Regular Monitoring of the attack logging rules' logs
- Regular Monitoring of the generic deny rules' logs

- Regular Monitoring of the attack bandwidth utilization
- Network attacks and serious attack attempts analysis
- Uncovered new vulnerabilities assessment
- Propose corrective and preventive actions.
- Monitoring and subscribing to external network security information in order to evaluate new attacks and propose preventive steps.
- Installation and configuration of NIPS Software and Hardware
- Provide maintenance and upgrade of service component Software
- Provide reporting of intrusions and actions, web based access
- Regular Reports
- Incidence response
- Prevent all known network based attacks
- Design and Configuring IPS services in response to DDOS attack types
- Filter out IP and TCP illegal packet types
- Design and Configuring IPS services in response to Flooding limits (per source, destination and intensity)
- Design and Configuring IPS services in response to DDOS bandwidth floods prevention within limitations of the provisioned network access bandwidth

8.6.21 **Patch Management:** The bidder 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 backed up data. The patch management should be executed efficiently for all kinds of environments like for operating systems like Windows and Linux, Data bases like DB2, Postgre SQL, MS SQL, Oracle, My SQL. The activities mentioned above are indicative in nature. The bidder will be required to provide services related to Patch management as per organizational Security Policy.

8.6.22 **Key Management Service:** One of the key 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 bidder and it should be only Tool based Key management

8.6.23 **Data Leakage Prevention Services:** The key objectives to be achieved through this service are:

i. Locate and catalog 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.

8.6.24 **Network Access Control Service:** Network Access Control Service will aim at controlling access to a 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 Purchaser defined policy; including anti-virus protection level, system update level and configuration.

8.7 IT Infrastructure at the SOC

8.7.1 The bidder has to ensure the proposed NOC services can be operated from NOC.

8.7.2 Bidder has to provide required Desktops with OS and other relevant software.

8.7.3 Bidder has to provide the required network connectivity to operate NOC.

8.7.4 Security management dashboard

i. Bidder is required to provide a Security Management Solution Console for reporting all the SOC activities including incidents from Anti-APT, HIPS, NIPS, Firewall, SIEM, vulnerability scan reports, remediation process progress etc.

ii. This service will help Purchaser to centralize the management of security products like SIEM, Firewall APT etc. and to have tight control on the security rules.

iii. The SIEM solution should provide dashboard functionality for all the above requirements.

iv. The dashboard solution should be on premise 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.

8.8 Physical Infrastructure Requirements for Operations Centre

8.8.1 OC Operations Area

The minimum requirements/ specifications for the Operations Center (OC) Operations area are detailed in the following sub-sections. While it is mandatory for the Bidder to meet these minimum requirements, if the Bidder estimates that a particular requirement would need a higher category of equipment, the Bidder should provision for the same in his bid. The Bidder should however provide basis for arriving at the solution being proposed as part of his bid. The overall Scope of Work (SOW) for the Bidder includes the following:

8.8.1.1 OC area consists of the Network Operation Area (NOC), Security Operation Center (SOC), Reception area (including Visitor's gallery), Conference room.

8.8.1.2 The NOC and SOC room should be separated by a partition to ensure segregation of duties and services between NOC and SOC operations.

8.8.1.3 Design, Supply, installation and setting up of the necessary basic Infrastructure for OC operation area in terms of civil, interior, electrical and Air-Conditioning System, Fire Prevention, Detection and Suppression System, Lighting system, Power, multi-layer Physical Security infrastructure like bio-metric based access-control system, CCTV/ surveillance systems etc.

8.8.1.4 Bidder should take consultation and approval of Purchaser, for the interior layout and material to be procured for the operations area.

8.8.1.5 Sensor based lighting must be used by the bidder to save energy, wherever possible. This shall be presented by the bidder as a part of its technical solution.

8.8.1.6 The monitoring of the Operations Center physical infrastructure should be done using BMS software and the bidder shall propose the same as well.

8.8.1.7 The Operations Centre should be managed by strict access control.

8.8.2 NOC Room

8.8.2.1 Bidder shall provision for 15 seats in the NOC room of approximately 1200 sq. ft. of carpet area. The bidder should provide the necessary infrastructure such as furniture, fixtures, PSTN phones, other services with the following per Workstation:

i. Data- 4 ports

ii. Voice- 2 ports

iii. Raw Power- 2 Nos., 5/ 15 Amps

iv. UPS Power- 3 Nos., 5/ 15 Amps

8.8.2.2 The NOC operations area requires round the clock monitoring and therefore the officials shall be provisioned for comfortable and ergonomically designed modular office furniture, one white board, 1 set of trolley type storage space (3/ 4 drawer unit) with 3 sets of keys, etc.

8.8.2.3 NOC operation room shall have finished floor with blinds, Fire rated glass window, Furniture etc. NOC operation room shall be planned as elevated floor with steps arrangement for each seating rows

8.8.2.4 Thin clients to be used by individuals operating and administering the NOC as per technical specification

8.8.2.5 NOC operation area shall have split comfort air-conditioning system with redundancy level of N+1.

8.8.2.6 NOC operation area shall have proximity readers for entry and Push switches for exit.

8.8.2.7 NOC operation area shall have CCTV system (fixed dome variable cameras) at entry and exit points.

8.8.2.8 NOC room should have stepped flooring arrangement.

8.8.2.9 Cabling

8.8.2.10 Any other utilities or equipment required to establish a state of the art NOC operations area shall be provided by the bidder without any additional cost.

8.8.3 SOC Room

8.8.3.1 Security Operation center (SOC) area shall be provisioned to accommodate sitting space for fifteen (15) nos. within an area of approximately 1200 sq. ft. The infrastructure to be provided to each workstation shall be the same as specified above for NOC Room along with 1 sets of trolley type storage space (3/ 4 drawer unit) with 3 sets of keys, etc.

8.8.3.2 SOC operation room shall have finished floor with blinds, Fire rated glass window, Furniture etc.

8.8.3.3 Systems (thin clients) to be used by individuals operating and administering the SOC per technical specification

8.8.3.4 SOC operation area shall have split comfort air-conditioning system

8.8.3.5 SOC operation area shall have proximity readers for entry and Push switches for exit.

8.8.3.6 SOC operation area shall have CCTV system (fixed dome variable cameras) at entry and exit points.

8.8.3.7 Cabling

8.8.3.8 Bidder needs to provide the 3 column x 2 row video wall in SOC room as per the specifications.

8.8.4 Conference Room

8.8.4.1 The Conference room shall be provisioned for sitting space of approximately 8-10 persons with comfortable chairs and round table. Conference room should be equipped with video conference facility shall be provisioned for comfortable and ergonomically designed modular office furniture. Conference room shall have comfort air-conditioning system.

8.8.4.2 The carpet area of the conference room should be 1200 sq. ft.

8.8.4.3 One LED TV of 65 inches to be provisioned for the Conference Room.

8.8.5 **Reception area**

8.8.5.1 Reception area will cover a total carpet area of 300 sq. ft. The reception area shall be provisioned for the seating space for one person along with reception table and chair and additional seating 4 persons (guests) in waiting area with chairs/sofa. The Bidder shall provision for:-

i. Data- 4 ports
ii. Voice- 2 ports
iii. Raw Power- 2 Nos., 5/15 Amps
iv. UPS Power- 3 Nos., 5/ 15 Amps
v. CCTV monitoring display
vi. Comfort split air-conditioning system.
vii. Decorative reception lighting

8.8.6 **Civil Works**

8.8.6.1 **Civil Works**

i. Dismantling of existing walls, if applicable.
ii. The construction of fire resistant walls (QED) or 9 inch brick wall with plastering @ 180 c for 1 hour) as and where required to provide fortification.
iii. The False ceiling (if provided) should be recessed to just provide enough space for Lighting within the Beams structure. The Beams that are jutting out should be aesthetically covered.
iv. The Color and make of the materials may be symmetrical with the overall architecture of the OC site and should ensure the aesthetic aspects of the ambience.

8.8.6.2 **Walls / Partitions**

i. At the external level around the OC area, the area should be sealed & fortified to avoid any heat absorption and moisture through any medium.
ii. The fortification shall be done with an impact resistant and fire-proof bricks. All external facing windows should be sealed to avoid heat light & moisture ingress
iii. Half height toughened Glass partition is proposed between the NOC and SOC room.
iv. Upon smoothened surface, three coat of primer and three coats of Luster paint will be applied. Adequate care to be taken to reduce the effect of fumes generated from the batteries.

8.8.6.3 **False Ceiling**

i. The Bidder should build a false ceiling for providing light panels, fire detection systems & suppression system and respective cabling, pipes etc. as required for the OC.
ii. The false ceiling should be recessed with the beams jutting out thereby giving extra 1 to 1 ½ feet space between the beams
iii. The Bidder should build a false floor of minimum 1 ½ feet to supply cold air via the false floor grilles.
iv. Metal false ceiling is planned for the NOC room, SOC room, Conference room and Reception area.
v. The Bidder shall use easy to install and remove tiles. These tiles should be non-combustible and dust free. The false ceiling board should be adequately insulated.
vi. The false ceiling should be supported with hangers of adequate strength and dampers should be provided to protect against vibrations.

8.8.6.4 **Painting**

i. Providing and applying Fire retardant paint of approved make and shade to give an even shade over a primer coat as per manufacturers' recommendations after applying painting putty to level and plumb and finishing with 2 coats of fire retardant paint. Base coating shall be as per manufacturer's recommendation for coverage of paint.
   - For all vertical Plain surface.
   - For fireline gyp-board ceiling.

ii. Providing and laying POP punning over cement plaster in perfect line and level with thickness of 10 - 12 mm including making good chases, grooves, edge banding, scaffolding pockets etc.

8.8.6.5 **Furniture and Fixtures**

i. Workstation size of 2' depth made with 1.5mm thick laminate of standard make over 19mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc. complete with French polish. The desk top will be 25mm thick & edges shall be factory post formed. The desk shall have the necessary drawers, keyboard trays, cabinets etc. along with sliding / opening as per design, complete with approved quality drawer slides, hinges, locks etc.

ii. Providing & making of storage unit with 18 mm thick MDF board along with 1.5 mm approved laminate color outside and 2 coat of enamel paint inside the storage of size 1'6"x1'9"x2'4". The same should be provided with all the required accessories including the handle, lock, sliding channel and necessary hardware, etc. complete with French polish

iii. Cabin table of depth 2' made with 1.5mm thick laminate of standard make over 19mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc. complete with French polish.

iv. Providing, making & fixing 6" high laminated strip using 1.5mm thick laminate over 10mm thick commercial board on all vertical surface in the entire server & ancillary areas including low height partition, brick wall, partition wall, cladding etc. complete with French polish in all respect.

v. Providing, making & fixing an enclosure for gas cylinder of Shutters and Partitions along with wooden support and 18 mm thick MDF board along with 1.5 mm approved laminate color outside and 2 coat of enamel paint inside the shutter. The same should be provided with all the required accessories including the handle, lock, loaded hinges, tower bolt and necessary hardware etc. complete with French polish.

vi. Fire proof safe (300 Liters. or above) with one hour fire rated.

8.8.6.6 **Electrical System**

i. Power Requirement

- Bidder will responsible for the design, supply and installation of electrical panels and distribution up to feeding points.
- Bidder to follow the detailed specifications provided for each equipment selection as per the specification sheet.
- Bidder should provide the 24*7 electricity power along with DG backup system.
- All the electricity charges should be borne by the bidder.
- Bidder should provide the UPS system with 30 minutes battery backup.

- Bidder should provide the separate electrical distribution board for lighting, Emergency lighting, UPS power and raw power points.
- Bidder should provide the separate distribution board with MCB's for air conditioning system.
- Bidder should provide the complete wiring and switch boards for lighting and power points.
- Bidder shall provide the necessary raw power points at all strategic locations as per requirements.

ii. Wiring

- PVC insulated copper conductor cable shall be used for sub circuit runs from the distribution boards to the points and shall be pulled into conduits. They shall be stranded copper conductors with thermoplastic insulation of 650 / 1100 volts grade. Looping system of wring shall be used, wires shall not be jointed. No reduction of strands is permitted at terminations. No wire smaller than 3.029sq.mm shall be used.
- Wherever wiring is run through trunking or raceways, the wires emerging from individual distributions shall be bunched together with cable straps at required regular intervals. Identification ferrules indication the circuit and D.B. number shall be used for sub main, sub circuit wiring the ferrules shall be provided at both end of each sub main and sub-circuit.
- Where, single phase circuits are supplied from a three phase and a neutral distribution board, no conduit shall contain wiring fed from more than one phase in any one room in the premises, where all or part of the electrical load consists of lights, fans and/or other single phase current consuming devices, all shall be connected to the same phase of the supply.
- . Each power plug shall be connected to each separate and individual circuit unless specified otherwise. The power wiring shall be kept separate and distinct from lighting and fan wiring. Switch and socket for light and power shall be separate units and not combined one.

iii. Lighting

- The Bidder should provide evenly distributed lighting of 500 LUX illumination at 3 ft. level from ground. It is necessary to align the distribution of lights with floor and equipment layouts to avoid shadowy areas caused by tall equipment, cabinets or racks. The lighting, sectional controlled by switches, should be able to switch off when they are not required. Lighting in each row will be controlled by occupancy sensor. Minimal lighting to achieve 50 LUX should be made available through manual switch control. These lighting fixtures should preferably be of LED type.
- In addition to above emergency lights to be provided in each row to achieve 10 LUX level for emergency evacuation. These lights will be wired through separate circuits. All emergency lights will be of LED type. Supply to these emergency lights will be provided through appropriate capacity of Inverter having one hour battery backup from SMF batteries. The lighting fixtures to achieve 500 LUX should be with Downward Light Output Ratio ('DLOR') 76% & CGR less than 90%.
- Following should be the average LUX level to be maintained in different areas.

Area	Type of Fixtures	Lux levels Required	Emergency Lighting LUX levels
NOC Room, SOC Room, Reception and Conference Room	2x28W T5 or 4x28W T5 or 2x36W CFL T5 or 3x36W CFL or more lamps fixture should be with DLOR 76% & CGR less than 90%. With electronic ballast controlled through occupancy sensors	450 - 500 Lux	10 LUX Average
Material Handling Room	2x28W T5 or 4x28W T5 or 2x36W CFL T5 or 3x36W CFL or more lamps fixture should be with DLOR 76% & CGR less than 90%. With electronic ballast controlled through override switch	350 - 450 Lux	10 LUX Average

iv. Comfort Air-conditioning system

- Bidder should ensure that the entire area of the OC is covered with air-conditioning system.
- Bidder will responsible for the design, supply, installation testing and commissioning of Hi wall units at designated locations of the OC including all low end works, cabling, piping, base stands for outdoor units etc. of air-conditioning system.
- Rack space and rack area should have appropriate temperatures and bidder needs to size the cooling capacity accordingly.
- Comfort air-conditioning system should be minimum 3 star rated BEE approved products.
- Bidder should comply to the following minimum technical requirements if the new comfort air-condition system is needed
  - Cooling Capacity – minimum 22000 BTU / Hr
  - Compressor – Hermetically Sealed Scroll Type
  - Refrigerant – R 22 Type
  - Power Supply – Three Phase, 380-415 V, 50 Hz
  - Air Flow Rate – minimum 19 cu m / min
  - Noise Level - < 50 dB
  - Operation – Remote Control

v. Safety & security System

- **Surveillance & Security System**
  - Bidder should ensure that the entire area of the OC is covered using CCTV at strategic locations and addresses the following as minimum specifications:
  - Bidder should ensure that the entire area of the OC is using Closed Circuit Video Surveillance, Recording and Replay facilities. The OC covered with IP based CCTV surveillance solution and should function on the POE

technology; this CCTV solution should be capable of storing 7 days CCTV logs. CCTV logs should be saved in archive. The bidder is required to provide CCTV – Still and movable cameras in appropriate places to provide maximum coverage. All the modes should follow the below mentioned specifications wherever appropriate. The use of all the variants will be judiciously decided.

- The CCTV surveillance system should support operations in duplex communication (record and relay) mode. The CCTV system should not only provide recording facilities but also support relay functionality whenever required. The CCTV proposed should have higher light sensitivity, dual encoding in MJPEG/MPEG4 and external alarm input.
- Alerts and sensor data should be posted to web servers using built-in HTTP port support, or can be forwarded to other systems using FTP data delivery.
- The data should be viewed using a web browser or the client Advanced View Application
- The system should support interfaces like Integrated 10/100 Mbps Ethernet Network interface, optional 802.11a/b/g, GSM, SMS, PPP modem etc.
- The resolution and frame rate minimum requirement of 720 x 480/576 @ 30/25 fps (D1) or higher.
- The system should provide with indicators like Device status, alert, network, speed and network activity LEDs
- The system should have professional quality audio/video monitoring solution, which provides digital video monitoring capabilities combined with a built in imager.
- The camera should have motion based detection system.

- **Access Control System**
  - The entry of personnel into the OC shall be restricted. For critical areas like NOC room and staging room entry points should be covered with authentications by use of proximity/contact less card. Only pre-authorized officials shall be allowed into the OC using authentication procedures.
  - The Bidder should keep spare inactivated proximity/contact less cards and provide a facility for onsite access card activation in case of emergency requirement of entering the OC.
  - The Access control system should manage Card Access Control. The software should connect and communicate with TCP/IP protocol. The standard options should at least include features like the access control with Alarm Management, backup and restore facilities of master and swipe data, reports on employee master and swipe data.

- **Fire Prevention, Detection and Suppression**

  Materials
  - In order to minimize damage to the equipment due to fire, the equipment used inside OC should, as far as possible, be made of non-combustible material or at least have minimal fire propagation or smoke generating properties.

Detection System

- The OC along with it associated area shall be protected from Fire using State-of-the-art Automatic Smoke/ Heat Detection/ Notifier Alarms & Fire Control mechanism using Code of Practices approved by agencies such as Bureau of Indian Standards (BIS), British Standards Institute (BSI) or National Fire Protection Association (NFPA). The alarms need to be monitored on a 24 x 7 basis & logged for providing reports.
- The Fire system shall deploy High Sensitivity Smoke/ Heat Detectors (HSSD) to allow swift detection of heat and/or smoke. The System shall consist of a high sensitive smoke detector, aspirator, and filter. It shall have a display featuring LEDs and Reset/Isolate button. The system shall be configured by a PC software or a hand held programmer
- The system shall for Multiple Smoke Threshold Alarm Levels, Time Delays, Indication of faults including airflow, detector, power, filter block and network as well as an indication of the urgency of the fault and configurable relay outputs for remote indication of alarm and fault Conditions.
- The detector shall have a multicolor LED to streamline system maintenance/inspection by plainly indicating detector status as follows: green for normal operation, amber for maintenance required, red for alarm.
- The detector shall be designed to eliminate the possibility of false indications caused by dust, moisture, RFI/EMI, chemical fumes and air movement while factoring in conditions of ambient temperature rise, obscuration rate changes and hot/cold smoke phenomenon into the alarm decision to give the earliest possible real alarm condition report
- The intelligent smoke detector shall be capable of providing three distinct outputs from the control panel. The outputs shall be from an input of smoke obscuration, a thermal condition or a combination of obscuration and thermal conditions. The detector shall be designed to eliminate calibration errors associated with field cleaning of the chamber.
- Thermal Detectors shall be rated at 135 degrees Fahrenheit fixed temperature and 15 degrees Fahrenheit per minute rate of rise. Detectors shall be constructed to compensate for the thermal lag inherent in conventional type detectors due to the thermal mass, and alarm at the set point of 135 degrees Fahrenheit.
- Detector bases shall be low profile twist lock type with screw clamp terminals and self-wiping contacts. Bases shall be installed on an industry standard, 4" square or octagonal electrical outlet box

Notification Appliances

- The notification appliance shall be audible/visual appliance or equivalent. Notification appliance shall be electronic and use solid state components
- Each electronic appliance shall provide multiple field selectable alarm tones. The tones available shall be HORN, BELL, MARCH TIME HORN, CODE-3 HORN, CODE-3 TONE, SLOW WHOOP, SIREN and HI/LO, etc.
- The appliance shall provide at least two output sound levels: STANDARD and HIGH dBA.

- The combination audible/visual appliances shall be installed indoors and may be surface or flush mounted. They shall mount to standard electrical hardware requiring no additional trim plate or adapter. The aesthetic appearance shall not have any mounting holes or screw heads visible when the installation is completed.

Suppression system

- Portable Extinguishers (CO2 or Halon based Extinguishers are not acceptable) shall be placed at strategic stations throughout the OC along with its associated support area.
- Illuminated Signs indicating the location of the extinguisher shall be placed high enough to be seen over tall cabinets & racks across the room. Linear heat detection cable should be placed along all wire pathways in the ceiling and below false floor. This should not directly trigger the suppression system—rather; it should prompt the control system to sound an alarm.

9 State Call Center

9.1 General requirements

9.1.1 State call Centre will have agents who would be responsible for attending all the incoming calls/ data messages at the State.

9.1.2 State Police would provide the infrastructure for the State Call Centre including space, manpower, power and other facilities and undertake civil work and Interiors to make the call center site usable for ITSP.

9.1.3 Bidder should ensure that in the event datacenter connectivity or applications are not accessible, Call agents should be able to answer emergency calls routed to IP Phone of the state call center.

9.2 Installation work at the State Call Center

9.2.1 Bidder would provide State specific site plan for the setup of Call Centre

9.2.2 Bidder shall be responsible to carry out the necessary installation work for connecting the required Office IT Hardware e.g. Workstations, Softphone/IP Phones etc. and for establishing the LAN connectivity in the Call Centre

9.2.3 Bidder would also provide the connectivity between State Call Centers and DC sites

9.3 **IT Infrastructure at the State Call Centres**

9.3.1 Bidder shall be responsible for installation and configuration of the Office IT hardware required at the State Call Centres and shall include the following (but not limited to):

i. Workstations (Desktop with single monitor for agents) with wireless headsets

ii. Workstations (Desktop with triple monitor for Dispatcher/Supervisor) with wireless headsets

iii. Softphones/IP Phones

iv. UPS

v. Router/MPLS CPE

vi. PoE switch

Please refer section 5B - Technical Requirements Specifications for detailed technical specifications.

9.3.2 Bidder is required to maintain and support the IT hardware and software provided at the State Call Centre

9.4 **Network bandwidth at State Call Center**

9.4.1 Bidder would provide primary and secondary connectivity (two separate vendors & separate routes) between State Call Centers and Cloud enabled DC sites.

9.4.2 Bidder would be responsible for the network bandwidth throughout the contract period.

9.5 **Facility Management Services**

9.5.1 Bidder shall deploy required manpower as provided in Clause 17.3 at each State Call Centre

9.5.2 FMS staff would be responsible to manage the IT system at the State

9.5.3 Detailed responsibility of FMS staff is provided in Clause 10 of this section

10 Manpower

10.1 Overview

10.1.1 Bidder shall provide adequate number of personnel each responsible for a specific role within the project. Bidder must provide clear definition of the role and responsibility of each individual personnel.

10.1.2 Bidder shall have a defined hierarchy and reporting structure for various teams that shall be part of the project.

10.1.3 Changes in Manpower deployment will have to be approved by the purchaser.

10.1.4 The following table provides an indicative list of resource categories and the minimum resource requirements estimated for the different sites. However, bidder shall independently estimate the teams size required to meet the requirements of Service Levels as specified as part of this tender. Bidder shall propose qualified personnel with adequate skills levels to manage the infrastructure.

Table 3: Minimum Resource requirement till Go-Live

S. No.	Description	Key Personnel	No. of resources (Min)	Minimum Qualifications	Min. Experience required	Desirable Certifications	Min. Deployment Percentage
1.	Project Director	Yes	1	MBA / M.Tech/B.E / B.Tech	15 years		50%

S. No.	Description	Key Personnel	No. of resources (Min)	Minimum Qualifications	Min. Experience required	Desirable Certifications	Min. Deployment Percentage
2.	Project Manager	Yes	1	M.Tech/B.Tech / B.E/ MCA/ MSc.(Computer Science/IT)	12 years	PMI / Prince2 certification	100%
3.	Solution Architect (Cloud expert/Virtual Machine expert)	Yes	1	M.Tech/B.Tech / B.E/ MCA/ MSc.(Computer Science/IT)	10 years		100%
4.	Solution Architect (Applications)	Yes	1	M.Tech/B.Tech / B.E/ MCA/ MSc.(Computer Science/IT)	10 years		100%
5.	Solution Architect (Network)	Yes	1	M.Tech/ B.Tech / B.E/ MCA/ BSc.(Computer)/ MSc. (Computer)/ Diploma in IT/Networking/ Graduate In IT	10 years	CCNA/CWNA/CCNP etc.	100%
6.	Solution Architect (Information Security)	Yes	1	M.Tech/B.Tech / B.E/ MCA/ MSc.(Computer Science/IT)	10 years	CISSP/CISC/CISA	100%
7.	Database Architect/ Modeler	Yes	1	M.Tech/B.Tech / B.E/ MCA/ MSc.(Computer Science/IT)	10 years	-	100%
8.	Database Administrator for ITSP	Yes	1	B.E./B.Tech /MCA	6 years	DBA Certification for the proposed database	75%
9.	Database Administrator for CAD service provider	Yes	1	B.E./B.Tech /MCA	6 years	DBA Certification for the proposed database	75%
10.	System Administrator	Yes	2	B.E./B.Tech /MCA	6 years	Relevant certifications for proposed OS such as UNIX, LINUX MCSE, etc.	100%

S. No.	Description	Key Personnel	No. of resources (Min)	Minimum Qualifications	Min. Experience required	Desirable Certifications	Min. Deployment Percentage
11.	Network Administrator	Yes	2	B.E./B.Tech/ MCA	6 years	CCNA/CWNA/CCNP etc.	100%
12.	GIS Expert (from OEM of the proposed product)	Yes	1	M.Tech/B.Tech/M.Sc./ B.Sc.	10 years	OEM certifications	50%
13.	Case Record Management Expert (from OEM of the proposed product)	Yes	1	M.Tech/B.Tech/M.Sc./ B.Sc.	10 years	OEM certifications	50%
14.	Contact Centre expert	Yes	1	Graduate in any discipline	10 years	OEM certifications	50%
15.	Application Developers	No	4	M.Tech/B.Tech / B.E/ MCA/ MSc.(Computer Science/IT)	-		100%
16.	BI/Data warehouse specialist	Yes	1	M.Tech/B.Tech / B.E/ MCA/ MSc.(Computer Science/IT)	5 years	BI certification of proposed product	As required
17.	QA Manager	Yes	1	M.Tech/B.Tech / B.E/ MCA/ MSc.(Computer Science/IT)	10 years	ISTQB	75%
18.	Test Analysts	No	2	M.Tech/B.Tech / B.E/ MCA/ MSc.(Computer Science/IT)	-	ISTQB	100%
19.	Master Trainer	Yes	2	M.Tech/B.Tech/M.Sc./ B.Sc.	10 years		100%

Table 4: Resource requirement after Go-live of first State

S. No.	Description	No. of resources (Minimum)	Minimum Qualifications	Minimum Experience required	Desirable Certifications	Minimum Deployment Percentage
1.	Project Director	1	MBA / M.Tech/B.E / B.Tech	15 years		20%
2.	Project Manager	1	M.Tech/B.Tech / B.E/ MCA/ MSc.(Computer Science/IT)	12 years	PMI / Prince2 certification	100%
3.	System Administrator	4*	B.E./B.Tech/ MCA	6 years	Relevant certifications for proposed OS such as UNIX, LINUX MCSE, etc.	100%
4.	Network Administrator	8*	B.E./B.Tech/ MCA	6 years	CCNA/CWNA/ CCNP	100%
5.	Database Administrator for ITSP	4*	B.E./B.Tech/ MCA	6 years	DBA Certification for the proposed database	100%
6.	Database Administrator for CAD service provider	4*	B.E./B.Tech/ MCA	6 years	DBA Certification for the proposed database	100%
7.	Application Developer	3	B.E./B.Tech or M.C.A/BCA/M.Sc./BSc or Diploma in IT	3 years		100%
8.	IT Helpdesk Staff	8*	Graduate in any discipline	3 years		100%
9.	FMS Staff (India-wide)**	150**	B.E./B.Tech or M.C.A/BCA/MSc/BSc / Diploma	3 years		100%
10.	Documentation Specialist	2	Graduate in any discipline	5 years		100%
11.	Project Coordinator	1	Graduate in any discipline	5 years		100%
12.	Process and Compliance Manager	1	B.E./B.Tech or M.C.A/BCA/M.Sc./BSc or Diploma in IT	5 years		100%
13.	SOC Analyst	4	B.E. /B.Tech / MCA.	5 years	At least one industry leading SIEM product and preferably other leading certifications in security, such as	100%

S. No.	Description	No. of resources (Minimum)	Minimum Qualifications	Minimum Experience required	Desirable Certifications	Minimum Deployment Percentage
					CISA, CISM, CRISC.	
14.	Forensics and RCA Analyst	2	B.E. /B.Tech / MCA	5 years	- Must be CISSP Certified - Certification in at least one industry leading SIEM product and preferably other leading certifications in security, such as CISA, CISM, CRISC.	100%
15.	VAPT Analyst	2	B.E. /B.Tech / MCA	5 years	- Must be CISSP Certified - Certification in at least one industry leading SIEM product and preferably other leading certifications in security, such as CISA, CISM, CRISC	50%
16.	Business Analyst	1	Graduate in any discipline	5 years		100%
18	Operations Center Manager	1	M.Tech/B.Tech / B.E/ MCA/ MSc.(Computer Science/IT)	10 years	Certification in Risk management, CCNA etc.	100%
19	Geo Fencing expert	36	Any Graduate in any discipline	-		100%
20	Build and Release Manager	1	B.E. /B.Tech / MCA	4 years		100%

*Geo fencing expert will be deployed for 2 years after first Go-Live

Table 5: Resource requirement during Contract Period

The below mentioned resources would be at the disposal of Purchaser for the entire contract period and should not be accounted by Bidder for its tasks.

S. No.	Description	No. of resources (Min)	Minimum Qualifications	Minimum Experience required	Minimum Deployment Percentage
1	Media/ Communication manager (Content Manager)	1	Graduate in any discipline	5 years	100%
2	UI/UX designer	1	Graduate in any discipline	5 years	100%
3	Project coordinator	5	Graduate in any discipline	5 years	100%
4	Java Application developer	4	Graduate in any discipline	5 years	100%

*** For three shifts in a day.**

**** Please refer clause 17.3 for more details on the FMS staff distribution per state. Actual deployment will be based on state going live.**

10.2 Resource Profiles

10.2.1 Project Director

i. (S)He shall be responsible for organizing, planning, directing, and coordinating the overall program effort.
ii. (S)He shall be responsible for allocating resources to the project.
iii. (S)He shall review the quality of project deliverables to ensure compliance with the agreed quality measures and standards.
iv. (S)He shall participate in all project meetings and project review meetings.
v. (S)He shall be responsible for conflict management, issue and dispute resolution.
vi. (S)He shall ensure compliance to the terms and conditions of the Contract

10.2.2 Project Manager

i. (S)He shall be responsible for organizing, planning, directing and coordinating the program effort.
ii. (S)He shall be at the onsite office as designated by PURCHASER.
iii. (S)He shall be responsible for overall Project Planning.
iv. (S)He shall be responsible for managing the team resources and ensuring their optimum allocation.
v. (S)He shall review the solution proposed and the integration plan for completeness and correctness.
vi. (S)He shall manage the solution implementation in close coordination with all the Solution Architects, administrators, experts, support staff, multiple agencies, vendors, project stakeholders etc.
vii. (S)He shall be responsible for organizing, planning, directing, and coordinating FMS staff at the field locations.
viii. (S)He shall participate in the steering committee meetings.
ix. (S)He shall have extensive experience and proven expertise in managing complex multi-task contracts

x. (S)He 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.

xi. (S)He shall be available onsite for full time during project implementation.

xii. (S)He shall be responsible for the overall contract performance and shall not serve in any other capacity under this contract.

10.2.3 Solution Architect (Cloud expert)

i. (S)he should have experience in formulating functional and technical specifications for the physical infrastructure components of large scale cloud enabled DC's & DR's

ii. (S)He shall be responsible for designing the Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) that should include but not limited to, data replication strategies between DC & DR, DC-DR connectivity and failover procedures

iii. (S)he would interact with other architects, project management to determine the solution interdependencies and interfacing requirements with DC and DR

iv. (S)he should be able to identify improvements areas/upgradation needs in DC-DR services

v. (S)He shall have a thorough understanding of the technical and quality standards and ensure adherence to those in order to maximize the future investment value and minimizing costs in the DC/DR operations.

vi. (S)He shall have an experience on virtual machine and optimization on cloud infrastructure.

10.2.4 Solution Architect (Applications)

i. (S)He would be responsible to conceptualize and interpret new architecture designs and requirements into an architecture and design that shall become the blueprint for the solution being created as required by the Purchaser

ii. (S)He would be responsible for implementing the applications as defined in the application architecture using appropriate technologies and thereby design secure applications.

iii. (S)He should possess extensive knowledge and experience in applications for Computer Aided Dispatch systems, IVRS, CTI, LBS, ACD, Case Record Management, Dialer, EMS, AVLS, ESB etc. and would provide detailed inputs on the design considerations for these ER applications

iv. (S)He should have comprehensive knowledge of overall software architecture and software engineering methodologies, principles and practices

v. (S)He would be responsible to research, analyze and interpret highly complex technical data for comprehension at various organizational levels and provide recommendations

vi. (S)He should have the ability to work with the other consultants in applying solutions to business problems, and fit solutions to the enterprise architecture across all viewpoints

vii. (S)He should have the ability to troubleshoot and resolve highly complex software problems that require highly creative solutions

viii. The Solution Architect should have the capability to address key requirements of the overall solution.

10.2.5 Solution Architect (Network)

i. (S)He would be responsible for interacting with other project stakeholders, agencies and solution architects for defining the network requirements for seamless interfacing of all project components.

ii. (S)He would be responsible for sizing the required Network bandwidth and for Server Load Balancing requirements.

iii. (S)He should have experience in design of network architecture for large scale distributed and heterogeneous environments

iv. (S)He should have experience in integration of public/ private networks like SWAN, mobile networks etc.

v. (S)He should have experience in design of network security architecture for large-scale distributed and heterogeneous environments, including firewall, intrusion detection systems, intrusion prevention systems, encryption, PKI & key management and would be responsible for defining the integrated security architecture in close coordination with the other ER system components.

vi. (S)He should have knowledge of installation, configuration and trouble-shooting of switches, Routers, Firewalls, and IPS. VLAN configuration etc., Knowledge of Networking protocols. (S)He should also have Knowledge of network security appliances such as firewall, IPS, Application firewall etc.

vii. (S)He shall possess extensive working knowledge and acumen in enterprise architecture best practices, including, but not limited to, logical and physical data architectures, network communications, operating systems, applications, data base servers, application servers, web servers, server consolidation, server performance, middleware etc.

viii. (S)He shall possess extensive knowledge in implementing similar solutions in a complex environment for computer aided dispatch.

ix. (S)He shall have the ability to address specialized and complex infrastructure architectural issues.

x. (S)He shall have extensive experience in infrastructure architecture discipline(s) of similar complexity as described in the tender.

10.2.6 Solution Architect (Information Security)

i. The Information Security Solution Architect shall be responsible for designing information security architectures for the project and identify the gaps, strategic impacts, financial impacts and the risk profile in the technical solutions

ii. (S)He shall works closely with IT architects, other functional area architects and security specialists to ensure adequate security solutions are in place throughout all the IT systems proposed in the project and mitigate the identified risks sufficiently

iii. (S)He shall serve as a security expert during application development, database design, network and/or platform (operating system) efforts, helping project teams comply with enterprise and IT security policies, industry regulations, and best practices.

iv. (S)He shall contribute to the development and maintenance of the information security strategy

v. (S)He should have experience in design and implementation of Information Security policy for complex and large scale IT application deployments

vi. (S)he should have done assignments involving assessment of information security policies and should be able to identify areas of improvements in the information security architecture

vii. (S)he should have designed information security architectures for large internet-based applications for safeguarding against security threats, vulnerabilities, cyber and phishing attacks

viii. (S)He should have specialization on a range of solutions, including, but not limited to, making appropriate use of PKI, intrusion detection / prevention, VPN, single sign-on, firewalls, and all elements of network-level security.

ix. Desirable to have Industry standard security certifications

10.2.7 Database Architect/ Modeler

i. Database Architect/Modeler shall be responsible for database design activities like data modelling, table creation, indexing, performance optimization, stored procedures, constraints, normalization, integration with different types of databases etc.

ii. (S)He should have Hands-on experience in design and development of large databases including workload analysis

iii. (S)He should have experience in sizing and design of server specifications

iv. (S)He should have experience in designing OLTP and high performance distributed applications

v. (S)He should have experience in designing storage, back-up, replication architectures for large IT systems

vi. (S)He should have experience in integrating servers, databases, and storage technologies

vii. (S)He should be familiar with server virtualization and cloud computing technologies

10.2.8 Database Administrator

i. (S)He shall provide highly specialized technical expertise towards administration of Databases

ii. (S)He shall be responsible for installation of database, creation of schemas, table spaces, define number of users in the database, create user profiles, memory utilization, caching etc.

iii. (S)He 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

iv. (S)He 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

v. (S)He shall have extensive experience in administering databases of similar size and criticality as described in the tender

vi. Certification on the storage products proposed shall be preferable.

vii. The Database Administrator shall handle the database maintenance so that maximum availability of the database is ensured

viii. (S)He will ensure proper backup and restore, database validity, database consistency and security

10.2.9 System Administrator

i. The systems administrator will be responsible for maintaining the optimum performance of the Emergency Response system as a whole.

ii. (S)He shall provide highly specialized technical expertise to handle System Administration challenges for complex and large scale systems

iii. (S)He shall be able to assist in the day-to-day tasks, including, but not limited to, monitoring of system activities, analysis of system utilization and resources, capacity control, performance tuning, coordination of system updates or fixes, adding/deleting users from the system, and generating reports as required.

iv. (S)He will also ensure the systems security by ensuring usage policies, the systems backup and restore, etc.

v. (S)He will grant access and permission to various users to the system.

vi. (S)He will not make any changes without the instructions of the Purchaser.

10.2.10 Network Administrators

i. The Network Administrator shall provide support for tasks, including, but not limited to installation, setup / configuration, troubleshooting, tuning, diagnostics and maintenance of networking and related equipment.

ii. The network administrator shall also coordinate with the other vendors/agencies to resolve all network related issues.

iii. (S)He shall have extensive experience in troubleshooting and management of network technologies as described in this tender.

iv. (S)He shall have technical expertise to manage deployment and maintenance of IT Security infrastructure, including, but not limited to, administration of appropriate access protection; system integrity / 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 Purchaser.

v. (S)He shall have the technical expertise to monitor various devices / tools such as content filtering and blocking, virus protection and vulnerability protection.

vi. (S)He shall escalate any security breaches and make sure patches are installed in case of threats related to OEM products.

vii. (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.

10.2.11 GIS Expert

i. (S)He shall closely interact with the Purchaser, other project stakeholders and the associated agencies to gauge system and interface requirements and accordingly customize & configure the OEM GIS solution followed by assistance in implementation across all the project locations

ii. (S)He would be required to monitor all the OEM GIS databases for accuracy and data integrity

iii. (S)He shall possess knowledge about GIS systems specifically deployed for emergency response systems in India

iv. (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

v. (S)He shall possess experience of handling complex projects that involved large scale usage of GIS

vi. (S)He shall have ability to address the complexities of the project with relation to hardware being deployed at the states to have GIS software

vii. (S)He should have hands-on training on deployment on similar projects with MDTs

viii. (S)He should be able to perform complex spatial data processing including geodatabase management, data collection, detailed editing, reporting etc.

ix. (S)He should provide training and technical assistance to agencies in the use of GIS data and computerized mapping programs

10.2.12 Case Record Management Expert (from OEM)

i. (S)He would be responsible for reviewing and overseeing the implementation of OEM developed Case Record Management system, product design diagrams, documents, test plans and results to ensure the design and delivery of a sound Case Record Management system architecture that meets all the Emergency user needs.

ii. (S)He would contribute to the efforts of Solution Architects in documenting the Case Record Management product capabilities, participating in formal customer acceptance testing, reviewing potential Case Record Management product enhancements

iii. (S)He must 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 center operations.

iv. (S)He must possess an in-depth practical working knowledge of public safety call center operations and technologies.

v. (S)He must have experience of designing a large scale complex Case Record Management systems

vi. (S)He would be required to work in close conjunction with multiple agencies, project stakeholders, system designers, architects etc. to understand the Case Record Management interfacing requirements and ensure that the Case Record Management system is integrated into the system as a whole

vii. (S)He should be able to provide technical assistance and consultant oversight related to the Case Record Management system with overall project implementation including installation, configuration, testing, reporting, migration and transition etc.

10.2.13 Contact Centre Expert

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 Purchaser for ensuring the acceptance of the same based on the acceptance criteria as defined by the Purchaser

iii. (S)He should be familiar with the components of a centralized contact center’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

iv. (S)He shall closely work with the solution architects and other experts (from the different OEM's based on the applications being installed) to ensure seamless integration of all the components. This shall involve detailed integration/design planning, Method of Procedure (MOP) development.

v. (S)He would need to work closely with the QA Analysts for the design of integration test plan, test scripts

vi. (S)He must be familiar with all the Contact Centre system components e.g. IP PBX, ACD, CTI, Case Record Management, LBS, IVRS etc. and should be able to assist in the configuration, installation and customization of these applications

vii. (S)He should have experience of designing and implementing the Contact Centres for large scale complex projects

viii. (S)He should have hands-on experience of integrating the Contact Centre with other critical components of the Emergency Response System

ix. (S)He would be responsible for gathering all Contact Centre solution requirements and then customize and configure the OEM solution and assist in its implementation

x. (S)He would be responsible for providing technical assistance and consultant oversight related to the Emergency Response Contact Centre with overall project implementation including installation, configuration, testing, reporting, migration, transition and cutover activities etc.

xi. (S)He should have worked on the Case Record Management solution that shall be required to support the Contact Centres

10.2.14 Application Developers

i. (S)He shall Work closely with analysts, solution architects, database designers and the Purchaser to customize the ER applications as planned

ii. (S)He shall gather business requirements and develop specifications for the ER applications

iii. (S)He shall produce the detailed specifications and writing the program codes

iv. (S)He shall unit-test the software work-products in controlled, real situations before going live

v. (S)He shall be responsible for preparation of training manuals for users

vi. (S)He shall assist the System administrators in maintaining the systems once they are up and running

10.2.15 BI and Data warehouse Specialist

i. (S)HE shall support projects throughout the solution development life cycle from establishing vision and scope to validating requirements in the testing phase

ii. (S)He shall have expert knowledge of the entire data management landscape and deep understanding of core Big Data design patterns and the associated challenges involved with data analytics, analysis, certification, Data ware housing, modeling, quality improvement and data management implementation projects

iii. (S)He shall provide reporting and data visualization options that support large and highly dispersed business teams

iv. (S)He shall have previous experience in business intelligence and data warehouse tools to match solutions with business needs

10.2.16 QA Manager

i. (S)He shall have expert knowledge of the entire QA (Quality Assurance) management landscape and deep understanding of data analytics, analysis, certification, modeling, quality improvement and large scale complex implementation projects

ii. (S)He shall identify and manage implementation of test plans and cases based on leading edge techniques and statistical evaluation.

iii. (S)he shall work closely with the Solution Architects, Application Developers and Support staff for defining the project Test Strategy, Testing Plans, Test Scripts and should ensure the comprehensiveness through effective usage of the Traceability Matrices

iv. (S)He should periodically inspect the completed quality control checklists, forms and other documents for conformance to prescribed standards.

10.2.17 Test Analysts

i. (S)He shall be responsible for developing and executing software Test Plans

ii. (S)He shall identify and facilitate issue resolution with functional and technical groups

iii. (S)He shall 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

iv. (S)He shall work with the Documentation Specialist for documenting the test results and reporting them to the senior management

v. He shall be having an experience on automation testing tool as per required solution

vi. Automation testing tool should be mentioned into scope of work

10.2.18 Documentation Specialist

i. (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

ii. (S)He must have experience in writing Technical documents like SRS, FRS etc.

iii. (S)He must have experience with Government or PSU agencies

10.2.19 Master Trainers

i. (S)He shall coordinate with the Project Manager and Purchaser to plan the training calendar for all the project stakeholders

ii. (S)He shall organize the required qualified resources for the identified training courses.

iii. (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, Dialer, EMS, IVRS, AVLS, and GIS etc.

iv. (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 class-room or e-Learning training modules as shall be prepared by the bidder

v. (S)He shall be responsible for designing the training materials.

vi. (S)He shall ensure proper conduct of training sessions and also ensure continuous training sessions are organized for the officers.

vii. (S)He shall ensure collection and collation of Trainee Feedback for all training sessions.

viii. (S)He shall ensure any issues/concerns raised by the participants are documented and shared with the Project Manager and PURCHASER.

10.2.20 Operation Center Manager

i. The Operations Centre manager shall be responsible for ensuring 24X7 operations of the Security Operations Centre (SOC) and the Network Operations Centre (NOC)

ii. (S)He would be responsible for resolving the incidents related to SOC/NOC in a timely manner, ensuring that the service SLAs are met

iii. (S)He would supervise, mentor and train the NOC engineers and should be able to continuously develop and improve the SOPs

iv. (S)He would lead the end-to-end security vulnerability assessments for network elements including security for user data, management and control planes, risk analysis & security design/implementation

v. (S)He must have working knowledge of network troubleshooting

vi. (S)He will be accountable for the organization, execution, planning and administration of the SOC/NOC functions

vii. (S)He should be responsible to oversee, direct and enhance the operational functions of SOC to detect, analyze and respond to advanced and emerging cyber threats

viii. (S)he should be able to direct, guide, oversee the activities of SOC staff who are charged with the analysis and management of threat identification information from a variety of sources

ix. (S)He should recommend courses of action based on analysis of both existing and emerging internal/external threats to the emergency response applications and deliver reports, briefings and assessments to the Purchaser while facilitating understanding of cyber threat entities and environments.

x. (S)he should be able to provide technical investigative support to other Law Enforcement Agencies or any other stakeholders as required

10.2.21 SOC Monitoring

i. Should be responsible for 24 X 7 monitoring basis with onsite personnel.

ii. Should be responsible for reporting of security alerts & incidents.

iii. Should be responsible for detecting internal and external attacks on NICCA infrastructure.

iv. Should be responsible for capturing data from all devices on real time basis.

v. Should be responsible for providing security reports to NIC on daily, weekly, monthly, quarterly and yearly basis.

10.2.22 Business Analyst

i. Responsible for implementation of Project Governance Systems and Procedures in consultation with Purchaser

ii. Planning and Project Management of all transition and scaling activities of requirements.

iii. Responsible for analysis of macro-level inputs from Purchaser for scaling

iv. Responsible for managing resources, procurement, forecasting and demand management of services in requirements.

v. Design and manage cost and process improvement initiatives

vi. Requirement gathering, business analysis and functional testing of proposed Software System

vii. Shall participate in all fortnightly / monthly project meetings and project review meetings

10.2.23 Geo fencing Expert

i. Responsible for doing the geo-fencing on map for each state in the guidance of state officials

10.2.24 Media/ Communication Manager

i. Responsible for creation of content and portals content for solution and media
ii. Responsible for follow up with media in awareness campaign and other requirements
iii. Responsible for all communications with Media
iv. Shall participate in all fortnightly / monthly project meetings and project review meetings

10.2.25 UX/UI Designer

i. Responsible for creation of software user behavior and user interface designs in photo shop tools
ii. Responsible for create wireframes, PSD files, HTML5 files, CSS files etc. related to UX/UI designs for Web application, Mobile application design
iii. Responsible for making the internet browser compatibility like internet explorer, Firefox, Safari, Opera etc. of created designs
iv. Shall participate in all fortnightly / monthly project meetings and project review meetings

10.2.26 Project Coordinator

i. Responsible to the project coordination with multiple resource of SI team and Purchaser team
ii. Manage all kind of documentation related to the project
iii. Arrange project meeting between purchaser and IT service provider on requirement basis

10.2.27 Forensics and RCA

i. Should be responsible for handling of security alerts and incidents.
ii. Should be responsible for conducting forensic analysis for security incidents.
iii. Should be responsible for conducting RCA (Root Cause Analysis) for security incidents.

10.2.28 VAPT

i. Should have prior experience of working with standards such as ISO 27001, ISO 20000, COBIT framework, ITIL.
ii. 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.
iii. Should have comprehensive knowledge on regular network scanning, firewall logging, penetration testing and related domains.
iv. 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.
v. Should be capable of performing rigorous analysis to identify and ascertain vulnerabilities, risks and threats.

vi. Should be able to test customized patching solutions.

vii. 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.

10.2.29 Process and Compliance Manager

i. Responsible to conduct periodic internal reviews to ensure that compliance procedures are followed

ii. Conduct or direct the internal investigation of compliance issues.

iii. Assess product, compliance, or operational risks and develop risk management strategies.

iv. Identify compliance issues that require follow-up or investigation.

v. Disseminate written policies and procedures related to compliance activities.

vi. File appropriate compliance reports with regulatory agencies.

vii. Evaluate testing procedures to meet the specifications of environmental monitoring programs.

viii. Verify that software technology is in place to adequately provide oversight and monitoring in all required areas

10.2.30 IT Helpdesk staff

i. IT Helpdesk staff shall be the dedicated personnel for PURCHASER – Contact center, responsible for handling all IT related problems.

ii. The reporting office and day-to-day assignments for the IT Helpdesk staff shall be controlled by the Project Manager and the PURCHASER Representative.

iii. (S)He shall be qualified enough to do first level diagnosis and troubleshooting the problems relating to network, IP phones, applications etc.

iv. (S)He shall also be qualified enough to do first level diagnosis and troubleshooting the problems relating to standard software such as OS, Internet Explorer, Open Office, messaging solutions, Anti-virus, etc.

v. (S)He shall also be capable of troubleshooting problems encountered by the end users in the application from the states.

vi. (S)He would be required to monitor and respond quickly and effectively to requests received through the IT helpdesk

vii. (S)He shall have formal training and experience of managing and troubleshooting the problems under proposed environments and others like Operating system , LAN / WAN, PCs and associated peripherals, backup / restoration using various tools, etc.

10.2.31 FMS Staff at State level

i. FMS staff shall be the dedicated personnel for state office locations responsible for handling problems related to the facility.

ii. The reporting office and day-to-day assignments for the FMS staff shall be controlled by the Project Manager He shall be qualified enough to do first level diagnosis and troubleshooting the problems related to hardware and software installed at the office locations

iii. Basic understanding of MDT, Desktop, Network and Telephony and other software deployed

iv. He shall be familiar with reporting and dashboard usage for effective monitoring and reporting of the facility management services.

v. Should be able to provide basic training on the software and hardware to the state officials

10.2.32 Build and Release Manager

i. Responsible to build, release and deploy the latest changes in all environments of the project

ii. Responsible to coordinate with all stakeholder to get the sign off on any release in cloud data center

iii. Responsible to comply all policy and procedures related to build and release processes

11 Training

11.1 General requirements

11.1.1 As per the User Training Plan as mutually agreed between the bidder and Purchaser, Bidder shall prepare the Training Manuals and submit the same to Purchaser for review and approval. The training manuals are to be prepared in English, Hindi mandatorily. Bidder has to ensure the preparation of Training material in atleast one vernacular of each state.

11.1.2 Bidder should be responsible for necessary environment setup including setup of IP phones, GIS, MDT, AVLS, CTI, ACD etc. to conduct end user training. End user training shall include all the equipment and applications. End user training will be conducted in a centralized location or at state location as identified by Purchaser & other stakeholders.

11.1.3 To ensure the quality of training and for active participation by the trainees, the Bidder should ensure that maximum size of a batch does not exceed 50. It shall be bidder's responsibility to plan the number of Master Trainers and number of sessions based on the indicative trainee audience as depicted in the table below.

11.1.4 Bidder's Master Trainers shall provide initial Functional Training (during implementation phase) to the Functional users, Senior Officials and the State level Trainers

11.1.5 Bidder's Master Trainers shall be required to provide the “Train the Trainer” training on all the system components to the State Level identified Trainers who shall be Senior Police Officials and will be responsible for imparting the Administrative, Functional, Refresher trainings to the other system users at regular intervals.

11.1.6 Bidder should understand that “Train the Trainer” trainings are an extremely critical important component of the entire Training programme as these State level identified trainers shall be responsible for trainings on a regular basis (as per the Training plan) to the operators and the field personnel. Bidder should ensure that these trainers are adequately trained on all the functional and technical aspects of the Emergency Response solution and should devise structured evaluation and assessment mechanisms to gauge their training competence and accordingly customize and impart the “Train the Trainer” trainings.

11.1.7 Bidder shall provide Senior Officials' training to selected officers from PURCHASER/ Police officials from states covering the MIS reporting and comprehensive project monitoring aspects of the project.

11.1.8 Based on the identified training needs, Bidder shall design efficient delivery mechanisms and trainers. Bidder shall appoint trainers and organize training sessions on a timely basis and ensure that the attendance, performance evaluations are recorded.

11.1.9 Bidder shall update the Training Manuals, procedures manual, deployment/Installation guides etc. to reflect the latest changes to the solutions implemented.

11.1.10 Bidder shall ensure that all concerned personnel receive regular training sessions, from time to time, as and when required.

11.1.11 Bidder will provide certificates to the trainees on successful completion of the training for using the applications, handheld devices or any other system (Database / MDT etc.). A transparent mechanism shall be devised by the bidder and approved by the Purchaser for certifying the trainees.

11.1.12 Performance of Bidder 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 Purchaser. Bidder performance shall be measured as per the procedure defined in “Annexure (Service Level Agreements), Section 3”. Bidder shall provide, collect and collate the trainee feedback and submit the Trainee Feedback Report to the Purchaser. Individual trainee feedback shall also be submitted as part of this report.

11.1.13 Training on CAD software is Bidders responsibility.

11.2 Trainees

11.2.1 **Functional users**: Field personnel and the personnel at the Central Operations Centre and State call centers, Supervisors, Dispatchers

11.2.2 **Senior Officials**: Officials from PURCHASER and State Police Purchasers

11.2.3 **State level Trainers**: State identified trainers for “Train the Trainer” trainings

11.3 Types of trainings

11.3.1 **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 trouble-shooting etc.

11.3.2 **Functional Training**: This training would focus on the use of the Emergency Response system applications at the Central Contact Centre, State Call Centre and the primary system users so that the users are aware of all the operations of the system and are able to implement the overall process defined by PURCHASER for an optimum use of the system

11.3.3 **Soft skills training**: Bidder needs to provide the soft skills training to the call agents and dispatchers to be able to communicate in defined manner for citizen service delivery. Call etiquettes and call scripts should be provided to the trainees. Bidder would have to include specialized trainers for the soft skills training.

11.3.4 **Senior Officials’ Training**: This training would focus on how to use the Emergency Response system's MIS reporting functionality for day-to-day monitoring by the Senior Management and access the various exception reports

11.4 Modes of trainings

11.4.1 **Classroom Training:** The trainings during “Implementation Phase” as defined in the table below shall be classroom trainings that would be conducted by trained and qualified Master Trainers in a classroom setting. To maintain consistency across trainings, standard templates shall be used for each component of a module. The class room courses for all the core trainings as mentioned in the table below will have the following components:

i. Course Presentation (PowerPoint or an Interactive Audio-Video presentation)
ii. Instructor Demonstrations (Application training environment)
iii. Hands-on Exercises (Application training environment)
iv. Application Simulations
v. Job Aids (if required)
vi. Course Evaluations (Inquisition)

11.4.2 **e-Learning modules:**

i. Bidder should ensure that the training is a continuous process for the users and it becomes important for the key project personnel who are involved in the day to day operations of the new ER system to keep themselves abreast of the latest developments and also to brush up their existing skills. Similarly, the new operators and field personnel need to have a fast learning curve and be able to handle the system effectively. For this reason Bidder shall be responsible to create e-Learning modules for all the key components of Emergency Response solution. Bidder shall ensure that these e-Learning modules are easily accessible by the key system users as and when needed

ii. Bidder shall design the e-Learning modules for General IT Skills as well as for the Functional aspects of the overall ER solution e.g. Usage of ACD, IP PBX, IVRS, CTI, MDT, MIS etc.

iii. Bidder should ensure that the e-Learning modules are not limited to Technical aspects of the solution but should also include the SOP's as defined by the Purchaser

iv. It will be bidder's responsibility to develop, test and deploy the e-Learning modules on the cloud enabled Data Centers and shall bear all the costs related to the same

v. Bidder should ensure that these e-Learning modules are accessible by the learners at their respective operation centers or can even be accessed from home (through a web-URL based Learning Management System).

vi. For the police personnel on the field, bidder shall design e-Learning module that can be accessed through the MDT devices installed in their vehicles

vii. In order to track the effectiveness of training programmes, Bidder should also provide an online catalogue of e-Learning modules and allow for Training and Competency Assessment through online tests

viii. e-Learning module's content generation and updation shall be bidder's responsibility

11.4.3 **Webinar Training:**

In addition to the Classroom trainings and the e-Learning modules as described above, it shall be the bidder's responsibility to provide a web-based unified conferencing solution in order to provide additional flexibility to the trainees. The webinars shall act as a powerful medium to provide interactive and high-quality learning experience to the system users.

11.5 Quarterly award

11.5.1 To encourage the State Police officials, quarterly awards would be given to the best performing calls agents, dispatcher and supervisors.

11.5.2 Bidder would be required to identify the measurable and tangible KPIs for call agents, dispatchers and supervisors. These KPIs would be monitored to select the best performing personnel and report quarterly statics of all agents.

11.6 Indicative training requirements

11.6.1 Broad indicative training requirement for the three training types (for the purpose of calculation of effort) is provided in the table below:

S.No	Indicative Training Courses	Indicative Training content	Mode of Training	Indicative Location	Target Audience	Indicative Duration (Days)	Frequency	Indicative number of trainees (nation-wide)
Initial Training during Implementation Phase								
General Training								
1	Basic IT skills	▸ Desktop operations, User admin, application installation, basic computer troubleshooting, Open Office, Operating Systems etc.	Classroom training	State Capital	State level identified trainers State Call center personnel	5 days	Once	15000 3350
2	Soft Skills	▸ Call etiquettes, voice quality, control of conversation, processional writing, self-management & attitude, methods of questioning etc.	Classroom training	State Capital	State Call center personnel	5 days	Once	3350
Functional Training								
1	All type of call center agents like call taker, dispatcher, supervisor	▸ Call center operations and usage of technology	Classroom training	State Capital	State Call center operators	5 days	Once	3350
2	MDT functionality	▸ Receiving the case file, recording & reporting incidents, updating actions, transfer of case,	Classroom training	State Capital	State level identified trainers			15000
3	MIS Reporting software	Generation and usage of the following: ▸ ACD Reports	Classroom training	State Capital	State Call Centre operators, Dispatcher, Supervisor			3350

S.No	Indicative Training Courses	Indicative Training content	Mode of Training	Indicative Location	Target Audience	Indicative Duration (Days)	Frequency	Indicative number of trainees (nation-wide)
		▸ Agent Login/Logout Reports ▸ Queue Reports ▸ Abandon Call Reports ▸ Call by Call Details Report ▸ Agent/Call taker Performance Reports ▸ Call Volume Reports			Senior Police Purchaser Officials			720
Senior Officials Training								
1	Usage of Emergency Response solution for monitoring, MIS reports, accessing various exception reports	▸ Real time dashboard training (To analyse the no. of alerts & their status, operator status, performance of a Command & Control center etc. ▸ Exception report analysis & delegation	Classroom training	Purchaser State Capital	Purchaser officials Senior State Police Officials	1 Day	Every 6 months	10 720
Operations Center Training (On-going)								
1	Functional/Operational training on ER System components and IT basics (for new operators and identified existing personnel)	▸ Basic refresher courses (e-learning modules) to the selected existing personnel and new operators ▸ Instructor Led Training courses on key system components (H/W, S/W)	e-Learning online modules	State Capital	State level identified trainers Call Center Operators, Dispatchers & Supervisors	2 Days	Every 6 months	15000 5000 700
2	Refresher Trainings for Senior Management	▸ Short e-learning modules, ILT courses on MIS report generation, analysis etc.	e-Learning online modules	Purchaser State Capital	Purchaser officials Senior State Police Officials	2 Days	Every 6 months	10 720

12 Implementation and rollout requirements

Bidder shall plan the rollout of solutions in stages. The indicative stage-wise rollout plan is mentioned in Clause 15 of this section. The requisite hardware and other equipment shall also be rolled out in stages along with the solutions implemented. The indicative bill of material is provided in Clause 17.4. The following services at the minimum shall be provided by Bidder as part of implementation and rollout.

12.1 Project planning and monitoring

12.1.1 Bidder is expected to adopt a comprehensive and efficient Project Management methodology to ensure that project milestones are tracked and met. Bidder will be required to finalize the Project plan in order to determine and agree on the project expectations, ground rules, work plan, communication matrix, timelines etc. within 15 days of effective date of signing of the contract with the Purchaser. Following activities would be covered under Project planning and monitoring:

- Finalize a set of activities for the project with identification of resource assignments, roles and responsibilities against each activity
- Prepare a project plan including milestones
- Communicate the project plan to stakeholders
- Measure project deadlines and budget utilization figures
- Project Quality Plan shall document specific process elements and the quality actions that the project intends to implement. This shall include the derivation of quality goals, standards followed, schedule of quality assurance activities in the project, defect control, correction and preventive methodology, handling process deviations.
- Configuration Management Plan shall contain procedures to be implemented for managing the configuration of the software solution to be produced by the project. In this plan, bidder shall identify configuration items, responsibilities of configuration controller, access restrictions, directory structure needed for configuration management, procedure for change control, method of tracking the status of configuration items, backup procedure, configuration audits, release management, archival procedure, procedure for version / revision numbering.

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

- Project Organization and Management plan
- Software Design and Development plan
- Implementation plan
- Pre-commissioning, Operational and User Acceptance Testing Plan
- Design, Delivery and Installation Plan for Hardware and Network
- Training Plan
- Support Service Plan
- 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)
- Post-support Service Plan
- Technical Support Plan
- Quality Assurance and Control Process details which must include (but not limited to) detailing on Metrics, Reviews, Problem Reporting and Corrective action etc.
- Technical and Operational Process which must include (but not limited to) detailing on Methods, Tools, Techniques etc.

12.1.3 The detailed project plan shall be internally reviewed for completeness and correctness by Bidder and subsequently delivered to the Purchaser for its review and acceptance. The mutually agreed Project Plan will form the basis for regular project monitoring.

12.1.4 Bidder shall hold fortnightly review meetings with the Purchaser 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 / concerns affecting the project progress, impact on the overall project timelines, project related risks with their mitigation plans.

12.1.5 Bidder shall ensure proper configuration management functions are being performed as per the configuration management plan. Bidder's Project Manager shall review the activities periodically.

12.1.6 Bidder's independent quality assurance team shall conduct regular reviews of the project and ensure that the project adheres to the project plan documents.

12.2 Software development, customization, rollout of applications

12.2.1 Guidelines for software development and testing

12.2.1.1 Bidder needs to setup the Development and Testing, Staging, Production environments and should be separate at the Cloud enabled DC sites, establish the required secure connectivity of its development centers with the DC sites and carry out the development and testing exercise from its development centers. Staging and Production environment will be deployed at both DC sites separately.

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

12.2.1.3 Bidder shall ensure that the COTS solution, if any selected are such that they are configured/customized with minimal modifications to the source code.

12.2.1.4 Bidder shall implement quality standards like CMM/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

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

12.2.2 Software Requirement Analysis and Specification

12.2.2.1 Software Requirement Analysis and specification is a key stage in the project and recognizing its pivotal role in the subsequent phases, sufficient time will be provided to the bidder to capture the requirements from all the project stakeholders accurately.

12.2.2.2 Bidder shall understand the processes related to Emergency Response Systems and other related documents and seek clarifications from the Purchaser, if any. Bidder shall then hand over these documents to the Purchaser.

12.2.2.3 Bidder shall interact with the State Police Purchasers, Telecom Service Providers (TSPs), Internet Service Providers (ISP's) and other associated agencies etc. as well as the Purchaser's project team to gather requirements. It is expected that Bidder gathers requirements through structured questionnaires, focused discussions with different stakeholders.

12.2.2.4 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

12.2.2.5 After the requirements analysis, Bidder shall prepare software requirement specification (SRS) document. 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/ update/delete/view etc.) shall also be included in this document. Acceptance Criteria shall also be included explicitly promoting clear understanding with the Purchaser about what it considers acceptable.

12.2.2.6 The SRS document shall be reviewed and approved by the Purchaser.

12.2.3 Software Design specifications

12.2.3.1 In this phase, Bidder shall develop a logical view of the Emergency Response solution to meet the Purchaser and other stakeholder requirements. This logical view shall consist of the functional architecture of the application and the new database design. Bidder shall also define standards for coding, documentation; user interfaces etc., if the same is not already defined.

12.2.3.2 Bidder 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 Purchaser.

12.2.4 Preparation of Databases design

12.2.4.1 Bidder shall design the Logical Data Model of all the Databases as proposed for the ER Solution e.g. Location Database, Case Record Management Database, MDT Database, GIS Database etc. based on the understanding of the information needs of the Purchaser and existing information items. The Logical Data Model shall include the definition of data structure or schema diagram and data dictionaries and metadata developed explaining specific entities, relationships and dimensions identified as a part of the Logical Data Model.

12.2.5 Build Stage – Coding and Unit Testing

12.2.5.1 Bidder shall carryout detailed design (Low Level Design, High Level Design), Coding and Unit testing and document should be approved by the bidder architect. And all release plan should be approved by purchaser. Purchaser may opt to get third party agency for SPQC testing.

12.2.6 Regression Testing

12.2.6.1 For any subsequent changes, enhancements to the applications or fixes made to any bugs/defects in the applications, it shall be bidder’s responsibility to perform comprehensive regression testing on the system to ensure that the existing applications work as expected even with the new changes.

12.2.6.2 It shall be bidder’s responsibility to create the Regression Testing Plan and Test Scripts with all possible scenarios.

12.2.6.3 Bidder may use an automated testing tool for quicker execution of Regression Test Cases if it so desires

12.2.7 Roll out

12.2.7.1 Bidder, in coordination with the Purchaser, shall set up the production environment at the cloud enabled Data Centre, install all the applications in the production environment, create application databases, application user profiles, load the legacy data etc. Production environment would not be accessible through Bidder’s Development Centre. It would be accessed only through the Operations Centre of the Purchaser.

12.2.7.2 Bidder shall coordinate with the Purchaser to resolve any problems encountered during/after rollout. All post implementation issues shall be documented and the necessary fixes/resolutions shall be implemented by the Bidder.

12.2.7.3 Bidder shall ensure that necessary support is provided to resolve defects. Bidder shall document the defects/bugs encountered during this phase as well as document the resolution of the same. Bidder shall also prepare and maintain a database of Consolidated List of Common Errors & their Resolution.

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

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

12.2.7.6 The bidder 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 Bidder at no additional cost to the Purchaser and without any project delays.

12.2.8 Change Requests Management

12.2.8.1 The bidder should note that the system should be designed so that any rules, alerts, triggers, reports as required by the Purchaser should be catered to. The bidder is required to study the requirements and present the required changes in the system to the Purchaser and implement the changes in the system. The Bidder should define a formal process to manage the requirement changes as defined for illustration below:

12.2.8.2 The Purchaser shall be responsible to present the change requests initiated by user-groups and forward to the selected bidder.

12.2.8.3 The bidder should assess the need to implement the suggested changes, take necessary approvals to implement the suggested changes and present the change control note to the Purchaser for approvals.

12.2.8.4 Bidder shall maintain a change request log to keep track of the change requests. Each entry in the log shall contain a Change Request Number, a brief description of the change, the effect of the change, the status of the change request, and the key dates.

12.2.8.5 Bidder shall assess the effect of the change by performing impact analysis.

12.2.8.6 Bidder shall maintain the change request log with updated information and provide the same to the Purchaser as and when desired.

12.2.9 **Performance Testing**

12.2.9.1 The bidder shall carry out the performance test run of the complete system after satisfactory installation/ implementation. Training of identified agents of State call centers shall be done as in consultation with the Purchaser and State officials.

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

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

12.3.1 Planning and Scheduling for Installation and commissioning of hardware and equipment at all the locations including Cloud enabled Data Centre sites, Operations Centre, State Call Centers, Mobile Police Vehicles, etc.

12.3.2 Pre-installation planning at all the locations including Central Operations Centre, State Call Centers, Mobile Police Vehicles, Data Centre but not limited to space planning, structured cabling, power points, check on utility services, environmental conditions, etc.

12.3.3 Delivery, Installation and commissioning of the hardware servers and related equipment in the DC sites shall be carried out by Bidder.

12.3.4 The plan and design documents thus developed shall be submitted to the Purchaser for approval and the acceptance shall be obtained prior to commencement of installation.

12.3.5 Bidder shall carry out installation of equipment in accordance with plans and layout design as approved by the Purchaser.

12.3.6 **MDT Distribution, Installation, Configuration in the vehicles:**

12.3.6.1 The bidder shall be responsible for distribution of MDT devices & the associated accessories like MDT Docking stations, wiring etc. at the State/ Zonal offices of the respective State’s Police departments. Bidder has to visit to the district level to place the MDT in vehicles. If due to any operational constraints, some police vehicles are not able to join the MDT installation drive at the State Zonal office on the given date(s), the bidder shall hand over the MDT devices to a person-in-charge (duly identified by the state police Purchaser and trained on MDT device installation and configuration by the bidder’s master trainers). The State identified personnel shall then be responsible for installation and configuration of the devices in vehicles at the respective police stations.

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

12.3.6.3 Bidder shall undertake necessary changes to harden the OS to prevent against malicious and unwarranted attacks.

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

12.3.6.5 Bidder shall undertake Installation and configuration of clustering software wherever provisioned.

12.3.6.6 Configuration / re-configurations / tuning of all the installed equipment and software

12.4 Integration and testing of installed systems / subsystems / equipment / Software

12.4.1 Bidder 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

12.4.2 Bidder shall provide for testing of changes/ updates/ patches in the testing environment before applying them on production environment

12.5 Preparation of Technical and End-User Documents

12.5.1 Bidder is expected to prepare technical documents including but not limited to:

12.5.2 Inception Report containing the project plan

12.5.3 Software Requirement Specifications Document (SRS)

12.5.4 Software Design Document (SDD) consisting of the following:

12.5.5 Functionality requirements of Applications (with internal and external access)

12.5.6 Server Side Detailed Hardware Specifications including related networking components

12.5.7 Software Development Document which will contain documentation pertaining to the development of each unit or module, including the code / software, approvals, etc.

12.5.8 Unit and Integration Testing Plan and Procedure

12.5.9 User Acceptance Testing Plan and Procedure

12.5.10 Test cases for all tests

12.5.11 Test input data set, test results

12.5.12 Hardware configuration Documents

12.5.13 Network and Security Configuration Documents

12.5.14 Version Control Mechanism document

12.5.15 Operational Procedures Manual

12.5.16 Roll Out Completion Report

12.5.17 Contingency Plan document containing emergency response procedures; backup arrangements, procedures, and responsibilities; and post-disaster recovery plans, procedures and responsibilities

12.5.18 Exit Management Plan

12.5.19 Bidder must ensure that the Emergency System modules that are being developed are thoroughly documented with comprehensive manuals and adhere to standard methodologies in software development as per ISO and/or CMM models. The documents including but not limited to are:

12.5.20 Quality Assurance / Testing Plan documenting containing information on the software test environment to be used for independent testing, the test cases to be performed, and the overall testing schedule to ensure that the software developed will conform to the functional and technical requirements with traceability to those requirements. This include methodology, schedule, resources, tools, procedures, environment definition, test cases, and software test results.

12.5.21 Documentation on interface characteristics of one or more systems and documents agreements between interface owners e.g. integration with TSPs etc. as envisaged through this solution. This document should contain information on both the physical and data element requirements that are necessary to make the transfer of information between the two different systems feasible.

12.5.22 Preparation and maintenance of end-user documents including but not limited to user manuals. The manuals and documents etc. shall be in English and in soft and/or hard copy and equal to the number of the deliverables. Some of the user manuals are:

12.5.23 Operations Manual providing instructions for installing the application, troubleshooting, interpreting message logs, and FAQs (Frequently Asked Questions)

12.5.24 Maintenance Manuals

12.5.25 Administration Manual

12.5.26 Security Manual

12.5.27 Applications manual and others (if any) as per acceptable standards

12.5.28 Systems Manual Detailing the data structure, table, forms and report structures.

12.5.29 Installation and maintenance manual for the servers and other hardware, Trouble Shooting Guide/ Handbook for helpdesk which describes the various trouble shooting methods

13 Ongoing Administration and Maintenance requirements

13.1 Operational Support

This section describes the operational requirements of the project including project management requirements, acceptance testing & certification and solution maintenance & support. Bidder shall provide operational support and maintenance services for the contract period at the Operations Centre, State Call Centers, Cloud enabled DC sites & other project locations. Operational support shall ensure that the system is functioning as intended and meeting the service levels. Operational support will include:

13.1.1 Project status reporting

Bidder shall submit progress reports on periodic basis. The progress report shall include the following:

13.1.1.1 Tasks completed/Results achieved during the period (fortnight)

13.1.1.2 Tasks/Results to be completed in the subsequent period

13.1.1.3 Cumulative deviations to date from schedule of progress on milestones Corrective actions to be taken to return to planned schedule of progress; Revision to planned schedule provided

13.1.1.4 Other issues and outstanding problems, and actions to be taken from each stakeholder

13.1.2 Software solution maintenance

13.1.2.1 The objective of application maintenance is to provide application maintenance and support services, including request based services (problem requests/defect fixes), enhancements, configuration management and post release support. As part of these services,

13.1.2.2 Bidder shall provide support for bug fixes, enhancements, operational support, and assistance to the Purchaser.

13.1.2.3 Bidder should be required to undertake the Application maintenance and Support services. This service should not be sub contracted to third party.

13.1.2.4 Bidder should commit to provide all necessary resources and expertise to resolve any issues and carry out required changes, optimizations and modification so that complete system as a whole works according to the specified requirements and satisfaction of the Purchaser.

13.1.2.5 Bidder should ensure that the entire solution as a whole is operational and run according to stipulated performance standards.

13.1.2.6 Bidder should ensure efficient knowledge transfer on a continuous basis so as to ensure that application knowledge is passed on to new members subsequently joining the team.

13.1.2.7 The services that bidder needs to provide during this phase shall include:

i. **Bug-fixes and end-user problem resolution**

- The end user support shall include all activities related to resolving the bugs/defects reported by solution users. Every bug/defect shall be logged. Every bug/defect shall be categorized on the severity levels.
- Bidder shall identify the solution and take necessary approvals from the Purchaser and release the patch for UAT after fixing the defects.
- Bidder shall document defects/bugs encountered as well as document the resolution of the same.
- Ensure re-installations, in the event of system crash/failures

ii. **New development and enhancements**

- The solution may require modifications or enhancements in the functionality. The enhancements or new development may also be required to fix some complex problem requests or defect fixes.
- Bidder shall ensure that correct version of the application/program units are being considered to carry out application enhancements/new development through configuration management plan for configuration management and version control using the version control software.
- Bidder shall support the Purchaser in carrying out the UAT for the modifications/ enhancements.

iii. **Configuration management and Version Control**

- As the solution and its underlying component applications, Servers, Network, storage, databases undergo enhancements and modifications due to problem requests, upgrades and patches provided by the vendors & OEMs, defect fixes and change requests, it becomes increasingly important to have version control on the deployed applications, Track all the configuration changes in the and report changes at regular intervals to the Purchaser.
- Bidder should adhere to the configuration management process as defined in conjunction with the Purchaser

iv. **Release management**

- Release management procedure shall be defined in conjunction with the Purchaser to ensure smooth transition of the application changes from release environment to production environment.
- As part of the release management, Bidder shall perform the following activities:
    - Bidder shall group the related change requests, assess their development progress and accordingly prepare a schedule for their release
    - Bidder shall in consultation with the Purchaser 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.

v. Maintenance of post implementation support environment

- Bidder 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/developments, subsequent user acceptance, etc.
- Bidder would be responsible for ensuring appropriate OS, Database versions and patches are installed on the respective servers in this environment.

13.1.3 **AMC Administration**

13.1.3.1 The bidder should ensure availability of AMC support with all the OEMs for proposed software and hardware components. This AMC support period should commence from the deployment of software and hardware components till the end of contract.

13.1.3.2 Bidder should track the Annual Maintenance Contracts for all the IT assets at the locations identified for the project: Cloud enabled Data center and Disaster Recovery Center, Operations Center (SOC and NOC), State Call Center, Mobile devices Terminals and initiate procedure for renewal of the same at appropriate points in time.

13.1.4 **Software Inventory Management**

13.1.4.1 Manage Software licenses of all types including OEM, node locked, server based, floating, time bound, CAL, Enterprise, concurrent, Volume Licensing, trial, free, open source etc.

13.1.4.2 Provide license compliance reports, listing all used and unused assets/licenses

13.1.4.3 The software licenses should not be restricted to a location

13.1.4.4 Maintain an inventory for all software components – details of software version, patches installed, and details of the server where the software is installed

13.1.5 **IT infrastructure management**

13.1.5.1 The Bidder shall provide complete support for the entire IT infrastructure of the system including all the items supplied/procured & installed as part of the contract, for the contract period.

13.1.6 **Administration of System, Database and Network**

13.1.6.1 Bidder will be required to perform tasks including but not limited to setting up servers, configuring and apportioning storage space, setting up of e-mail accounts and mailing lists, creating and updating of information about Police officials, vehicles etc., management and integration of databases, implementing security on the Internet / Intranet, setting up of firewalls and authorization systems, performing periodic backup of data and automating reporting tasks, and executing hardware and software updates when necessary in accordance with guidelines as specified by the Purchaser

13.1.6.2 Bidder should assign onsite support as specified in the clause 10: Manpower details to diagnose, troubleshoot and resolve issues with the equipment / components supplied. The onsite support should possess capability for supporting the equipment and components proposed, but not limited to undertaking preventive and break-fix maintenance, troubleshooting, resolving problems, tuning, etc.

13.1.6.3 The Bidder 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.

13.1.6.4 The Bidder shall provision skilled and experienced manpower resources to administer and manage the entire IT Infrastructure solution at the Cloud enabled Data Centre.

13.1.6.5 Bidder may be required to assist the system users in performing periodic health check of the systems, troubleshooting problems, analyzing and implementing rectification measures.

13.1.6.6 The Bidder shall implement and maintain standard operating procedures for the maintenance of the IT infrastructure based on the policies formulated in discussion with Purchaser and based on the industry best practices / frameworks. The Bidder shall also create and maintain adequate documentation / checklists for the same.

13.1.6.7 The Bidder shall be responsible for managing the user names, roles and passwords of all the relevant subsystems, including, but not limited to servers, other devices, etc. The bidder will be required to set up the Directory server

13.1.6.8 Bidder will be responsible for not only the new systems provided as part of this tender but also ensuring the upkeep of existing systems that would be reused and also incorporate necessary changes for new applications if any during the tenure of the contract.

13.1.6.9 On an ongoing basis, Bidder shall be responsible for troubleshooting issues in the infrastructure, network and applications for the centralized ER solution to determine the areas where fixes are required and ensuring resolution of the same.

13.1.6.10 Bidder should be responsible for identification, diagnosis and resolution of problem areas pertaining to the solution and maintaining assured SLA levels.

13.1.6.11 The Bidder shall be responsible for management of passwords for all relevant components and devices under his purview and implement a password change mechanism in accordance with the security policy formulated in discussion with Purchaser and based on the industry best practices / frameworks like ISO 27001, ISO 20000 etc.

13.1.6.12 The administrators will also be required to have experience in latest technologies like virtualisation and cloud computing so as to provision the existing and applicable infrastructure on a requirement based scenario

13.1.6.13 Bidder may be required to manage the user names, roles and passwords of all the relevant systems, including, but not limited to servers, applications, devices, etc. Bidder may be required to manage passwords for all relevant components and devices under their purview and implement a password change mechanism in accordance with the security policy of the Purchaser. User account management includes and is not limited to:

i. Setting up new user accounts for all system users
ii. Grating access and review
iii. Removal of user accounts
iv. Privilege management
v. Password management
vi. Access to OS, databases and applications
vii. Monitoring access and usage
viii. Logging
ix. Session time-out

13.1.6.14 Bidder should be responsible for the synchronization of system clocks and automatic lockout of the terminal after defined inactivity time.

13.1.6.15 Bidder should be responsible for maintenance of logs of user Internet activity, failed login attempts, etc.

13.1.6.16 Bidder will be required to download the patches and updates for OS, Anti-virus, RDBMS and other systems using a two-step procedure. In the first step, patches and updates should be downloaded to a standalone system. In the second step, the patches and updates should be updated to the relevant systems.

13.1.6.17 Bidder should provision a dedicated team consisting of Operations Centre Manager, System Administrator, Network Administrator and Database Administrator etc. for a minimum period specified in Clause 10, Section 5 to perform the activities mentioned in the following sections:

i. System administration:

- System administration services for management of server environment to maintain performance at optimum levels.
- 24*7*365 monitoring and management of the servers in the Cloud enabled Data Center.
- The Bidder shall ensure proper configuration of server parameters. The Bidder shall be the single point of accountability for all hardware maintenance and support the IT infrastructure at the Data Centre.
- Operating system administration, including but not limited to management of users, processes, resource contention, preventive maintenance and management of patches to ensure that the system is properly updated. Bidder is also responsible for re-installation in the event of system crash/ failures.
- Bidder shall also ensure that the bottlenecks in the infrastructure are identified and fine tuning is done for optimal performance.
- Facilitate application migration in coordination with application owners/Purchasers
- The Bidder shall appoint system administrators to regularly monitor and maintain a log of the monitoring of servers to ensure their availability to the Purchaser at all times.
- Regular analysis of events and logs generated in all the sub systems including but not limited to servers, operating systems, databases, applications, security devices, messaging, etc. Bidder 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.
- Adopt a defined process for change and configuration management in the areas including, but not limited to, changes in parameter settings for application, servers, operating system, devices, etc., applying patches, etc.
- Managing the trouble tickets, diagnosis of the problems, reporting, managing escalation, and ensuring rectification of server problems as prescribed in SLA.
- Bidder shall provide administration services related to user access including administrative support for user registration, creating and maintaining user profiles, granting user access and authorization, providing ongoing user password support for users.

- The system administrators should provide hardening of servers in line with the defined security policies
- The system administrators should provide integration and user support on all supported servers, data storage systems etc.
- The system administrators should provide directory services such as local LDAP services and DNS services and user support on all supported servers, data storage systems etc.
- The system administrators will be required to trouble shoot problems with web services, application software, desktop/server relationship issues and overall aspects of a server environment like managing and monitoring server configuration, performance and activity of all servers.
- Documentation regarding configuration of all servers IT Infrastructure etc.
- The administrators will also be required to have experience in latest technologies like virtualization and cloud computing so as to provision the existing and applicable infrastructure on a requirement based scenario

ii. Storage Administration

Certain minimum deliverables sought from the Bidder with regards to Storage Administration are provided below:-

- The Bidder shall be responsible for the management of the storage solution including, but not limited to, storage management policy, configuration and management of disk array, SAN fabric / switches, tape library, etc.
- The Bidder shall be responsible for storage management, including but not limited to management of space, SAN/NAS volumes, RAID configuration, LUN, zone, security, business continuity volumes, performance, etc
- PURCHASER would additionally remotely manage the storage system and components and appropriate setup should be provided by the Bidder
- The storage administrator will be required to identify parameters including but not limited to key resources in the storage solution, interconnects between key resources in the storage solution, health of key resources, connectivity and access rights to storage volumes and the zones being enforced in the storage solution.
- The storage administrator will be required to create/delete, enable/disable zones in the storage solution
- The storage administrator will be required to create/delete/modify storage volumes in the storage solution
- The storage administrator will be required to create/delete, enable/disable connectivity and access rights to storage volumes in the storage solution
- To facilitate scalability of solution wherever required.
- The administrators will also be required to have experience in latest technologies like virtualisation and cloud computing so as to provision the existing and applicable infrastructure on a requirement based scenario

iii. Security administration

- Management of security environment to maintain performance at optimum levels.
- Address ongoing needs of security management including, but not limited to, monitoring of various devices/tools such as content filtering and blocking, virus

protection and vulnerability protection through implementation of proper patches and rules.

- Maintain an updated knowledge base of all the published security vulnerabilities and virus threats for related software, including, but not limited to, operating systems, application servers, web servers, databases, security solutions, messaging solutions, etc.
- Ensure that patches/workarounds for identified vulnerabilities are patched/ blocked immediately.
- Respond to security breaches or other security incidents and coordinate with respective OEM in case of a new threat is observed to ensure that workaround/patch is made available for the same.
- Maintenance and management of security devices, including, but not limited to detecting intrusions or unauthorized access to networks, systems, services, applications or data, protecting email gateways, servers, desktops from viruses.
- Operating system hardening through appropriate configuration and patch updates on a regular basis.

iv. Database administration

- Management of database environment to maintain performance of each database at optimum levels
- End-to-end management of the databases on an ongoing basis to ensure smooth functioning of the same.
- Tasks including, but not limited to managing changes to database schema, disk space, storage, user roles.
- Conduct code and configuration reviews to provide inputs to the Purchaser in order to improve the performance or resolve bottlenecks if any.
- Performance monitoring and tuning of the databases on a regular basis including, preventive maintenance of the database as required.
- Back up of data. Report backup status on a regular basis.
- Manage database patch update as and when required with minimal downtime.
- Bidder shall co-ordinate with Datacenter operators/engineers for back-up activities.
- Use of DBA tools to perform database creation, maintenance and database monitoring related tasks.
- Management of storage environment to maintain performance at optimum levels.
- Management of the storage solution including, but not limited to, storage management policy, configuration and management of disk array, SAN, tape library, etc.
- Storage management, including but not limited to management of space, volume, RAID configuration, LUN, zone, security, business continuity volumes, performance, etc.

v. Backup / Restore

- The Bidder shall be responsible for backup of storage as per the policies of Purchaser at the cloud enabled Data Centre. These policies would be discussed with the Bidder at the time of installation and configuration.

- The Bidder shall be responsible for monitoring and enhancing the performance of scheduled backups, schedule regular testing of backups and ensuring adherence to related retention policies
- The Bidder shall be responsible for prompt execution of on-demand backups of volumes and files whenever required by PURCHASER or in case of upgrades and configuration changes to the system.
- The Bidder shall be responsible for real-time monitoring, log maintenance and reporting of backup status on a regular basis. The Bidder shall appoint administrators to ensure prompt problem resolution in case of failures in the backup processes.
- The administrators shall undertake media management tasks, including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets (onsite and offsite).
- The Bidder shall also provide a 24 x 7 support for file and volume restoration requests at the Data Centre.

13.1.7 Network Monitoring

13.1.7.1 Provide services for management of network environment to maintain performance at optimum levels.

13.1.7.2 The Bidder shall provide services for management of network environment to maintain performance at optimum levels on a 24 x 7 basis.

13.1.7.3 The Bidder shall be responsible for monitoring and administering the network within the Data Centre up to the integration points with WAN. The Bidder will be required to provide network related services for routers, switches, load balancer, NTP services etc.

13.1.7.4 The Bidder shall be responsible for creating and modifying VLAN, assignment of ports to appropriate applications and segmentation of traffic.

13.1.7.5 The Bidder shall co-ordinate with the Data Centre Site Preparation agency in case of break fix maintenance of the LAN cabling or maintenance work requiring civil work.

13.1.7.6 Coordinating with the Network Provider and ensure integration and monitoring of the network within the DC sites, Operations Center, State Call Centres etc.

13.1.7.7 Polling / collecting of server, devices and desktops security logs from all the systems on Network at pre-defined intervals.

13.1.7.8 Ensure smooth routing of network traffic to the active cloud enabled DC site in case of disaster / drill.

13.1.8 Cloud enabled DC Operations & Administration

13.1.8.1 The Bidder shall provide comprehensive onsite support to Purchaser on a 24 x 7 x 365 basis to ensure an uptime of 99.5% for the IT infrastructure solution at the Cloud enabled Data Centre in accordance with the Service Level Agreement mentioned as part of this tender.

13.1.8.2 The Bidder shall commit to provide all necessary manpower resources onsite to resolve any issues/incidents and carry out required changes, optimizations and modification.

13.1.8.3 Co-ordinate with the Data Centre Provider to resolve any problems and issues related to the datacenter.

13.1.8.4 Co-ordinate with the Datacenter provider to make any changes that may be required towards the placement and layout of infrastructure within the datacenter.

13.1.8.5 Prepare a list of equipment, software and configuration installed in the datacenters and the same shall be approved by the Purchaser. Bidder shall maintain and modify the list in accordance to the modifications.

13.1.8.6 Any breach of security or non-compliance on part of the datacenter vendor and/or datacenter facilities should be immediately brought to the notice of the Purchaser with suggestions for improvements.

13.1.8.7 Maintain at the datacenter, a log of all Bidder personnel entering or visiting the datacenter. Such a log should be provided to the Purchaser whenever required.

13.1.8.8 Manage an inventory of critical components and spares that are provisioned onsite and co-ordinate with the OEM to ensure replenishment of the same whenever required.

13.1.9 Disaster Administration

13.1.9.1 Bidder shall provide services for management of disaster environment to maintain performance at optimum levels and as required in case of a disaster or drill.

13.1.9.2 Bidder shall ensure that Disaster documentation is up to date and the site is in full readiness for switch over in case of any disaster.

13.1.9.3 Bidder shall manage the data synchronization processes in co-ordination with the DC provider to ensure that data and application is updated at DC site.

13.1.9.4 Bidder shall ensure that configuration of equipment and application maintained at the Cloud enabled DC 1 site is replicated regularly at the DC2 site and vice versa.

13.1.9.5 Mock drills and plan updates shall be carried out once/twice in a year and report submitted to the Purchaser as per MHA policy.

13.1.9.6 Bidder shall test, review and monitor the business continuity plan bi-annually for its effectiveness and provide test results to the Purchaser.

13.1.9.7 Bidder shall provide training to the Purchaser users in order to apprise them of the Disaster plan and of their involvement for business continuity.

13.1.9.8 Bidder has to ensure restoring all databases, servers etc. as per disaster and recovery policy of the purchaser.

13.1.10 Software Change Management

13.1.10.1 Bidder shall be responsible for managing the changes that happen to the Cloud enabled DC sites setup on an ongoing basis, including but not limited to, changes in hard/soft configurations, changes to system software, changes to policies, applying of updates/patches, etc.

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

13.1.11 MIS Reports

The following is an indicative list of MIS reports. The Bidder should draw an exhaustive list of reports along with the Purchaser. Bidder should submit the reports on a regular basis in a mutually decided format.

13.1.11.1 Weekly reports

- Log of backup and restoration undertaken.
- Log of component-wise downtime, replaced components at the Cloud enabled Data centers
- Summary of resource utilization of critical components

13.1.11.2 Fortnightly reports

- Project Progress Report with schedule slippage details
- Overall performance reports including the analysis of queries completed, queries pending, queries escalated, completion time, responsiveness, concern areas, etc.
- Network availability report
- Summary of resource utilization of all components in the Cloud enabled Data Centers
- Summary of measured end user application response time for selected business transaction

13.1.11.3 Monthly reports

- Network Availability and Utilization Report
- Asset modification report at Operations Centre, State Call Centres, Field locations (for MDT devices) and Cloud enabled DC locations.
- Summary of component wise uptime in the DC sites
- Summary of resource utilization of all components in the DC sites
- Log of preventive / break-fix maintenance undertaken
- Summary of usage of tape media provisioned.
- Summary of changes undertaken in the DC sites including major changes like configuration changes, release of patches, database reorganization, storage reorganization, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.
- Consolidated SLA / non-conformance report

13.1.11.4 Quarterly Reports

- Asset database report and Asset Audit report
- Summary of incidents reported like Application down, Components down, overall downtime, security vulnerabilities detected, hacker attacks / security threats, peaking of utilization etc.
- Feedback report from users for the services rendered.

13.1.11.5 Incident Reporting (as and when it occurs)

- Complete system down – with root cause analysis
- Peaking of resource utilization on any component
- Bottlenecks observed in the system and the possible solutions and workarounds.

13.1.11.6 **Security Incident Reporting (as and when it occurs)**

- Detection of security vulnerability detection with the available solutions / workarounds for fixing
- Hacker attacks, Virus attacks, unauthorized access, security threats, etc. – with root cause analysis and plan to fix the problems.
- Any hazards or events like fire, environmental conditions, physical security, etc. at the Data Centers.

13.1.11.7 **SLA Reports**

- All type of reporting should be submitted periodically as per SLA measurement interval to the purchaser

13.1.12 **Vendor Management Services**

Certain minimum deliverables sought from the Bidder with regards to vendor management are provided below:-

13.1.12.1 The Bidder should coordinate with all the relevant vendors of Purchaser for Cloud enabled Data Centre basic infrastructure, other vendors etc. to ensure that the user problems and issues are resolved in accordance with the SLA of the vendor. The Bidder should also ensure that unresolved items are escalated in accordance with the escalation matrix.

13.1.12.2 Maintain database of the various vendors with details like contact person, telephone nos., escalation matrix, response time and resolution time commitments etc.

13.1.12.3 The Bidder shall also coordinate with vendors of other Government agencies and ensure that the issues are resolved in accordance with the SLA signed between the Government agencies and the vendors. Bidder shall maintain a track of SLA performance for such vendors.

13.1.12.4 Draw a consolidated quarterly SLA performance report across vendors for consideration of Purchaser

13.1.12.5 The SLA performance acceptance of the bidder will have to be certified by Purchaser

13.1.13 IT Helpdesk Services

13.1.13.1 The bidder needs to provide IT Helpdesk services at the Operations Centre for all the system users (Call center operators, Field personnel, Dispatchers, Supervisors, Support staff, FMS staff etc.) to address and assist in troubleshooting any IT related issues they might face on a day to day basis.

13.1.13.2 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 & resolution for all the users. It shall be integrated with the EMS and shall be designed to meet the SLA response & resolution timelines

13.1.13.3 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.

13.1.13.4 The IT helpdesk staff shall assign severity level to each query, assign the queries to the appropriate personnel for resolution e.g. System/Network/Database/Security administrators for queries/issues related to any of the corresponding areas.

13.1.13.5 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.

13.1.13.6 The IT helpdesk must always maintain high user satisfaction levels

13.1.13.7 The IT helpdesk must maintain the SLA statistics & submit monthly report to the Purchaser

13.1.13.8 Help Desk Coordinators shall generate reports using a call logging and reporting tool which should have the following reporting capabilities:

i. Call Analysis
ii. Call Trend
iii. Call History Report
iv. Daily Call Completed and pending Reports

13.1.14 Facility Management Services

13.1.14.1 Bidder shall be responsible for providing 24X7 Facility Management Services (FMS) at the State level Call Centres for addressing any issues related to basic IT Infrastructure like Desktops, networking and Telephony services.

13.1.14.2 Bidder shall ensure that the FMS staff is conversant with issue resolution and troubleshooting of IT Infrastructure, networking concepts and telephony and should be able to provide prompt responses to the problems the State Call Centre Operators, Dispatchers and Supervisors may face.

13.1.15 L3 level support by OEM

13.1.15.1 This project envisages L3 level support by OEM's for all the Hardware and Software components being configured, installed and customized by them.

13.1.15.2 The L3 level support staff as provided by OEM shall work in close coordination with the bidder during all the phases of the project and shall be responsible for troubleshooting all the problems/bugs/issues arising in the hardware/software components supplied by them

13.1.15.3 The L3 level support should include Onsite Support along with the provisions of Remote Support for component problems that can be addressed from a remote location

13.1.15.4 The L3 level support shall include responsible to run engineering diagnostic for unidentified errors or existing bugs in the hardware and software applications that they have installed

13.1.15.5 The L3 level support shall be responsible for generating end-user workarounds

13.1.15.6 The L3 level support shall track issue descriptions, bug fixes, case status, and case root cause analysis

13.1.16 Third Party Audit Support

13.1.16.1 The Purchaser reserves the right to inspect and monitor/assess the performance/maintenance of the project systems at any time during the course of the contract. The Purchaser may demand and upon such demand being made, the Purchaser or its authorized Third Party Audit Agency (TPA) shall be provided with any documents, data, materials or any other information which it may require, to enable it to assess the progress/performance of the project.

13.1.16.2 The Purchaser also have the right to conduct itself or through another third party audit agency as it may deem fit, an audit to monitor the performance by the bidder on its obligations/functions in accordance with the standards committed to or required by the Purchaser undertake to cooperate with and provide to the Purchaser/Audit agency, all documents and other details or information as may be required by them for this purpose. Any deviation or contravention identified as a result of such audit/assessment would need to be rectified by the bidder.

13.1.16.3 The core objective for Third Party Audit (TPA) is to provide objective assurance to monitor and assess the conformance by the Bidder on various project activities and add value to improve the project operations. It would help the Purchaser to accomplish the project objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of infrastructure, operations, service level management and control and governance processes.

14 Technology Refresh and Technology Change Management (TCM)

Since the Technology associated with Emergency Response Systems is constantly improving and costs are coming down, the same must be passed on to the system as envisaged by the Purchaser. All the TCM processes must be followed for introducing new technologies into the Emergency Response Solution.

14.1 TCO management

14.1.1 Introduction

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 bidder. This section outlines key objectives of cost optimization and TCO management and the bidder's scope of work and deliverables associated with this.

14.1.2 Objective

14.1.2.1 Bidder is required to optimize cost in all areas of bidder's work through various measures that could include automation, deployment of tools and optimizations in management of services.

14.1.2.2 The key areas of focus expected from the bidder in this regard are the following:

i. Continuous measureable reduction in overall cost of providing Emergency Response services to Personal in distress

ii. The Purchaser 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

14.1.2.3 Scope of work and components where cost optimization is expected

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

14.1.2.5 **Optimization of Cloud Data centre operations**: Bidder shall perform the following tasks as part of optimization of data center operations:

14.1.2.6 Use and optimization machine and storage should be undertaking.

14.2 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 bidder shall have an opportunity for improving the performance and efficiencies of the operations of DC sites of the proposed Emergency Response system.

14.2.1 Technology Refresh scope

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

14.2.1.2 Track key technology trends and determine key technology refresh areas e.g. Cloud management suite, Hypervisor , Operating System and upgraded/advanced IT Infrastructure components at the Data Centre sites. Track key technology trends and determine key technology refresh areas e.g. new OS and upgraded/advanced IT Infrastructure components Identify potential alternative technologies and solutions that can be deployed in the DC sites and co-develop analysis parameters with the Purchaser

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

14.2.1.4 Drivers for technology refresh (e.g. Change in the Emergency Response solution components – Telephony, Network, Database & storage technology etc.)

14.2.1.5 Key options and evaluation of each option (Cost-Benefit analysis, Degree of Social Impact the refreshed solution shall have etc.)

14.2.1.6 Detailed plan for implementation of technology refresh at the DC sites

14.2.1.7 Likely impact, if any, on service level agreements with the OEM's, bidder, DC provider etc.

14.2.1.8 Expected cost reduction due to induction of new technology

14.2.1.9 Expected process and SLA improvements

14.2.2 **Technology Refresh Feasibility Study:** Bidder shall be responsible for performing a feasibility study, prepare an improvement plan and implement the same. This is part of the overall responsibility of bidder for TCO reduction end to end Project operations. Technology refresh has to be conducted by the Bidder annually.

14.2.2.1 **Automation of data centre operations**

i. Following transition of the data centre operations and deployment of automated management tools as proposed by the bidder, the bidder shall study the current state of automation of data centre operations.

ii. The impact on services and associated manpower requirement of the data centre on account of automation shall also be assessed.

iii. Bidder shall benchmark the current state of operations against leading industry standards for data centre operations and prepare a detailed improvement plan focused around automation of data centre operations. This improvement plan shall also outline the overall impact on TCO on account of automation of data centre operations.

iv. The solution implemented for automation of data centre operations shall be reviewed every year.

14.2.3 **Third Party Independent Assessment**

i. Bidder shall be responsible for getting the Third Party assessment done independently for the Data Center components identified for optimization. Based on the results of third party assessment and the proposed benefits from the technology refresh exercise, the actual refresh process shall start.

14.3 **Deliverables**

14.3.1 First Report on Technology Refresh every year from steady state operations of the DC sites and acceptance of the Emergency Response Technology Solution successfully deployed by the bidder for the first state. Subsequently, the report shall be prepared every year.

14.3.2 TCO reduction report at the time of Technology Refresh

15 Project Milestones

Project milestones are divided into 2 categories:

- Cloud enabled Data centre and operation centre
- State call centre

Project timelines and deliverables for each phase are provided below. Bidder needs to adhere to these timelines throughout the project period.

S. No	Milestone	Timeline (in month)	Deliverable
Cloud enabled Data Centre and Operation Centre			
1.	Signing of contract &submission of PBG	T	
2.	Team mobilization a. 75% of key resources b. 90% of resources	a. T+7 days b. T+30 days	1. Letter of deployment with team names 2. NDA with team members
3.	Preparation of detailed project plan with timelines	T + 21 days	1. Project inception report
4.	Issue of Purchase order to OEMs (based on Purchaser's request/ order) within 15 days of PO issued by Purchaser (T' = time of release of purchase order by Purchaser)	T' + 15 days	1. Copy of purchase order with no reference to commercials
5.	Preparation of detailed solution including location of Operation Centre, site preparation plan, network plan, application architecture and other components	T+1	1. Solution design report
6.	System requirement specification and system design documents	T+1.5	1. SRS document 2. High level design document 3. Low level design document 4. Deployment document in development, QA and Production environment
7.	Commissioning of cloud data center and cloud service provider's, operation center	T+1	1. Specification of IT hardware 2. EMS report
8.	commissioning of Contact center on cloud	T+1	
9.	Commissioning of Operation center	T+3	
10.	Installation and commissioning of EMS	T+2	
11.	Nirbhaya portal, intranet portal	T+4	

S. No	Milestone	Timeline (in month)	Deliverable
12.	BI and data warehouse	T+5	
13.	Integration with CAD Service Provider	T+5	
14.	Go-Live at Cloud enabled DC1, DC2, Operations Centre and 2 States	T+5	1. Set up of IT Infrastructure at State Call Centre including network and MDT installations 2. Training of identified personnel at State level 3. Go Live Approval by Purchaser/ State
15.	Preparation of technology refresh document including DC, Operations Centre and State Call Centre	T+24 T+36 T+48	1. Technology refresh including SLA review and reduction of TCO plan
16.	Security audit	T+12 T+24 T+36 T+48	1. Security audit report
15.A	Quality Audit as per CMMI level 5 for Operation center, Development Center and Call center	T+12 T+24 T+36 T+48	1.Quality Audit report
State Call Centre			
17.	State specific approval for setting State Call Centre	T1	
18.	Design of State specific solution including bill of material, layout plans, customization needs (if any) and other related documents	T1+15 days	1. Copy of purchase order without cost details 2. Detailed plan
19.	Site readiness	T2	
20.	Supply, commissioning and testing of hardware including MDT	T2+1	1. Specification of IT hardware 2. EMS report
21.	Training of State call agents, dispatchers, supervisors and senior police officials	T2+1.5	1. Training Manuals 2. Training completion report
22.	Go-Live of the State	T2+2	1. Go-Live acceptance

15.1 Work products/ documents/ reports required

The below are the minimum reports required but not limited to:

15.1.1 Software Requirement Specifications (SRS)

15.1.2 System Design Document (SDD) / Process Design Report

15.1.3 Testing Stage

- Integration Test Cases with Results
- System Test Cases with Results

15.1.4 User Acceptance Testing

- UAT Case and Results
- Source code and executables
- Installation Manuals

15.1.5 Implementation

- Implementation Plan including data migration, user training and rollout plan
- User Manuals
- Training Manuals
- FAQ & Trouble Shooting Guide

15.1.6 Warranty Support

- Defect / Bugs log with resolution
- Consolidated List of Common Errors and their Resolution

15.1.7 Requirements Change Management

- Change Request Log
- Impact Analysis including changes in effort and schedule

15.1.8 Penetration Test Report

15.1.9 Vulnerability Test Report

15.1.10 Application Assurance Certificate

15.1.11 Recommendations on IT Plan

15.1.12 Report on Closure of Audit issues (if any)

15.1.13 End user Support

- Defect / Bugs log with resolution
- Consolidated List of Common Errors and their Resolution

15.1.14 Application enhancement and new developments

- Change Request logs
- Impact Analysis with Effort Estimates
- Software Requirement Specifications (SRS)
- System Design Document / Process Design Document
- Integration Test cases & results
- System Test Cases & Results
- UAT Case and Results
- Source code and executables
- Installation Manual
- Training Manuals / User Manuals
- FAQ & Trouble Shooting Guide

15.1.15 Release Plan and Release Note

16 Acceptance Criteria

16.1 General

16.1.1 The Cloud Computing Solution meets all the requirements as per RFP

16.1.2 The Solution installed in the DC should be in accordance with DC Policies and Guidelines and been certified as compliant with applicable Security Policies

16.1.3 Application to be on-boarded has been tested and accepted on the Cloud Computing Solution

16.1.4 Adequate operational facilities (such as a Cloud Operations Center and Cloud Help Desk) and staff been put in place – ready for the Solution to commence production operations.

16.1.5 The necessary initial training / education / awareness programs been conducted to the stakeholders as identified.

16.1.6 All the documentation and engineering artifacts as given in the project plan been delivered by the vendor and accepted by the Government.

16.1.7 Any shortfalls in the Government responsibilities – necessary for the smooth operation of the Solution – such as policies, governance structures and guidelines been identified and communicated to the Government

16.1.8 Any issues identified with the Solution, have been closed as rectified or categorized as not-material to these acceptance criteria

16.1.9 The Cloud hosting DC facility shall be Tier3 or above and it should be a certified DC.

16.1.10 The bidder should develop user acceptance test cases in line with the minimum acceptance criteria mentioned under Clause 16 of this section with the assistance from the Purchaser.

16.1.11 The Purchaser may have the acceptance test done by its representatives, prospective system users, Testing Committee of the officials from State Police Purchasers, TSP's, ISP's or consultants or any third party at any time at its own convenience. The bidder would be required to cooperate with such representatives/third party and provide the required support for this activity

16.1.12 The acceptance test shall involve successful supply, delivery, installation & commissioning of all hardware and related software in the Cloud enabled DC sites, Operations Centre, Police Vehicles, State Call Centres:

16.1.13 All the required hardware and software must be installed and working properly. The bidder can be asked to demonstrate all the features/facilities mentioned in the bid and technical requirement laid in various section of the RFP.

16.1.14 During this period, the installed systems must demonstrate its capability of providing the services enumerated in the contract, RFP document and claimed by the bidder in its bid and specified in the catalogues attached with the respective bid. The bidder will arrange the test equipment, if required for performance verification. Successful bidder will also provide documented test results.

16.1.15 On the successful completion of the acceptance test and after the Purchaser is satisfied with the working of the entire system at Cloud enabled DC sites, Operations 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.

16.1.16 The bidder 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 & software as per the RFP. The test parameters, commitments etc. as decided & approved by the Purchaser shall be final and binding on the bidder.

16.1.17 If the quality and the quantity of the items supplied by the vendor are found unacceptable, the successful bidder 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 bidder as per the payment schedule mentioned in the RFP would be made after the successful clearance of the following acceptance tests.

16.1.18 All the functionality, features and configuration relevant to this project shall be documented and demonstrated by the successful bidder to the purchaser.

16.1.19 The entire solution will be monitored under production use for a pre-defined period of time for satisfactory performance of the solutions.

16.1.20 In case of any performance issues during this period, the bidder should resolve the issues identified on a priority basis.

16.2 Criteria for Acceptance

S. No.	Component	Acceptance Criteria
Cloud Enabled DC Sites		
1.	Hardware (like servers, storage)	• Item should be captured by Bidder Cloud Management Platform or EMS
2.	Servers (except virtual machine)	• Demonstrate Hardware RAID functionality by simulating internal disk failure. • Demonstrate High Availability. • 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	• Demonstrate capability to take backup of specialized servers that are not connected to SAN. • Demonstrate backup/restore of SAN data • Demonstrate backup/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	• Demonstrate functioning of all the relevant components of EMS solution for respective phases
5.	Mailing solution	• Demonstrate mailing functionality between internal users. • Demonstrate outbound & inbound mail relay to and from

S. No.	Component	Acceptance Criteria
		internet. - Demonstrate anti-virus and anti-spamming activities.
6.	Network switching	- Demonstrate the network switching from DC1 to DC2 & access of applications / solutions at the DC from Operations Centre. The network switching should be transparent to end user without the need for any manual changes at the sites.
7.	Replication	- Demonstrate async Replication of SAN data from DC to DC and vice-versa ensuring its consistency.
8.	Integrated testing	- Comprehensive integrated testing of all the solutions to re-validate the Phase-wise acceptance criteria.
9.	Acceptance of Cloud enabled DC sites	- Hardware, applications and other components delivered, installed and configured as per agreement with the Purchaser - All components as described above are tested and accepted - Sites are connected with primary and secondary network - Applications can be accessed from both the DC sites - Training is completed for all DC personnel
Operations Centre		
10.	Presentation Layer	- Demonstrate the accessing and serving of emergency response applications - Demonstrate test cases as prepared by Bidder
11.	Information Security Solution	- Conduct a comprehensive penetration testing covering all the solutions implemented. A penetration testing report should be submitted to PURCHASER. - Conduct a threat and vulnerability assessment with a view to demonstrate that PURCHASER infrastructure is adequately secured against internal and external attacks. The assessment report should be submitted by Bidder - Close mutually agreed issues observed during Security Audit.
12.	Acceptance of Operations Centre	- Hardware, applications and other components delivered, installed and configured as per agreement with the Purchaser - All components as described above are tested and accepted - Hardware components can be tracked through EMS - Installation and working of video wall - All phones connected and working

S. No.	Component	Acceptance Criteria
		• Operations center is connected with both DC sites • Applications can be accessed from Operations Centre • Training is completed for all Operations center personnel
State Call Centre		
13.	Hardware (like desktop, IP phones)	• Item should be captured by EMS • Testing of hardware functioning by State Call Centre supervisor
14.	Presentation Layer	• Demonstrate the accessing and serving of emergency response applications • Demonstrate test cases as prepared by Bidder
15.	Acceptance of State Call Centre	• Hardware, applications and other components delivered, installed and configured as per agreement with the Purchaser • Installation and working of IP phones • Connected with both DC sites with primary and secondary network • Applications can be accessed from State Call Centre • Test cases can be run from the State Call Centre • GIS map shows the position of all installed MDTs • Training is completed for all State Call Centre personnel
Field Location		
16.	Acceptance of MDT	• MDT should be listed in EMS • Tracking of MDT from State Call Centre • Successful test case of sending messages to MDT and closing case through MDT

17 Volumetric data estimations

17.1 Growth estimation for Call Volume

The centralized integrated country-wide Emergency Response system envisions providing prompt emergency response to women/citizen in distress. The system has been designed to handle a large volume of calls daily with a significant busy hour call volume percentage that shall ensure that maximum number of calls can be handled in an hour in peak-load conditions.

The system envisages best-in-class average Agent call handling time that includes the entire cycle of receiving the call, recording the incident, locating the appropriate mobile vehicles and dispatching to the incident location. Total number of PRI's (Primary Rate Interface) based on the call volume estimates have been estimated keeping into consideration the PRI's for Inbound and Outbound calls.

As the popularity of centralized Emergency Response system increases and more number of states opt-in for the same, the call volume is also expected to rise proportionally. The system has been designed to be scalable for handling the increased number of calls. Given below is the Year-On-Year growth chart for call volume for the entire duration of project:

Call Volume Data

	Year 1	Year 2	Year 3	Year 4	Year 5
Yearly call volume	18,00,00,000	21,78,00,000	26,35,38,000	30,60,00,000	36,00,00,000
Monthly Call Volume	1,50,00,000	1,81,50,000	2,19,61,500	2,55,00,000	3,00,00,000
Daily Call Volume	5,00,000	6,05,000	7,32,050	8,50,000	10,00,000

Assumption:

- Average call handle time is 4 minutes
- Average agent efficiency is 80%
- Busy hour call volume may increase by 10%

17.2 State wise Call Agent distribution

One of the most critical components of the centralized integrated Emergency Response system is the number of Call Agents at the State Call Centres. In order to handle the large volume of calls as projected, there needs to be an optimum provisioning of call agents i.e. Inbound Voice Agents, Outbound Voice Agents, Dispatchers and Supervisors. Based on the daily minimum call volume per state (as per the latest population census data), the optimum number of call agents has been derived and depicted as below:

S.No.	State	Inbound Agents	Outbound Agents	Non voice agents	Dispatcher	Supervisor
1	Andaman and Nicobar Islands	1	1	1	1	1
2	Andhra Pradesh	136	5	2	19	1
3	Arunachal Pradesh	1	1	1	1	1
4	Assam	70	3	1	10	1
5	Bihar	224	9	2	31	1
6	Chandigarh	4	1	1	1	1
7	Chhattisgarh	112	5	1	15	1
8	Dadra and Nagar Haveli	1	1	1	1	1
9	Daman and Diu	1	1	1	1	1
10	Delhi	138	6	1	19	1
11	Goa	1	1	1	1	1
12	Gujarat	136	5	1	19	1
13	Haryana	60	3	1	8	1
14	Himachal Pradesh	3	1	1	1	1
15	Jammu and Kashmir	27	1	1	3	1
16	Jharkhand	73	3	1	10	1
17	Karnataka	114	5	2	16	1
18	Kerala	77	3	1	11	1
19	Lakshadweep	1	1	1	1	1
20	Maharashtra	218	8	2	30	1
21	Manipur	1	1	1	1	1
22	Meghalaya	1	1	1	1	1
23	Mizoram	1	1	1	1	1
24	Madhya Pradesh	168	7	2	23	1
25	Nagaland	1	1	1	1	1
26	Odisha	92	4	1	13	1
27	Puducherry	4	1	1	1	1
28	Punjab	63	3	1	9	1
29	Rajasthan	157	6	2	22	1
30	Sikkim	1	1	1	1	1
31	Tamil Nadu	135	5	2	19	1
32	Tripura	2	1	1	1	1
33	Uttar Pradesh	469	18	5	65	1
34	Uttarakhand	23	1	1	3	1
35	West Bengal	170	7	2	24	1
36	Telangana	55	2	1	8	1
Total		**2741**	**124**	**48**	**392**	**36**

17.3 Bandwidth requirement estimates

17.3.1 Bandwidth requirement at Central level:

Considering the huge volume of calls expected everyday, the Centralized & Integrated Emergency Response system needs the availability of sufficient bandwidth that can handle the system load requirements and ensure uninterrupted delivery of emergency services to women/citizen in distress. The bandwidth requirements need to be calculated across the locations considering the application performance, replication, data transfer, Cloud enabled DC and other requirements. It’s a bidder resposibility to provide dedicated and non dedicated bandwidth as per requirement of the solution at center.

17.3.2 Bandwidth requirement at State level:

To ensure successful emergency response operations at the State level, it is essential to provision sufficient bandwidth to the state call centres considering the volume of calls they handle daily, busy hour call volume percentage and the number of call agents stationed at the State Call Centre (including the Inbound, Outbound, Non-voice, Dispatchers and Supervisors). It’s a bidder resposibility to provide dedicated and non dedicated bandwidth as per requirement of the solution at center.

17.4 Bill of Quantity (BoQ)

17.4.1 Hardware

Sr. No.	Description	No. of Units
1.	Voice Gateway	
2	Desktop For Operation Center	10
3	UPS for Operation Center	1
4	Router/MPLS CPE for Operation Center	1
5	Managed Access Switch for Operation Center	3
6	Video Wall for Operation Center	2
7	Laser Jet Printer for Operation Center	1
8	IP Phones for Operation Center	40
9	Desktops (Thin Clients)	30
10	Desktop with triple monitor (Dispatcher, Supervisor)	428
11	Desktop with Single Monitor (Voice Agent and Non-Voice Agent)	2922
12	IP phones for each agent desk	3350
13	Router/ MPLS CPE	
13.A	50 mbps router	15
13.B	200 mbps router	13
13.C	400 mbps router	8
14	Managed Access Switch	
14.A	48 Port	34
14.B	24 Port	3
14.C	16 Port	10
15	MDT Device 8” (Rugged) – Vendor 1	20000
16	MDT Device 8”(Non Rugged) – Vendor 1	20000
17	MDT Device 8” (Non Rugged) – Vendor 2	20000
18	MDT device 5.5” (Non Rugged) – Vendor 1	20000
19	MDT device 5.5” (Non Rugged) – Vendor 2	20000
20	UPS for	
20.A	Tier-I states (small)	30
20.B	Tier-II states (medium)	5
20.C	Tier-III states (large)	1
21	LED	1
22	PRI Lines	

17.4.2 Software Licenses

Sr. No.	Description	No. of Units
1	CRM license	1000

Sr. No.	Description	No. of Units
2	GIS Map (Map Data and POI)	1
3	Database for ITSP	
4	Database – Postgre Advanced server 9.4 (64 bit version for Linux) for CAD service provider only	10
5	Enterprise Management Software	
6	Identity Management System (IMS)	
7	Email Solution (base License)	
8	Email Solution (Web based client license)	1,25,000
9	Anti-Virus	
10	Function Points	15,000
11	E-Learning Software	
12	Webinar Software (At 50 resource Conference)	
13	Directory Services	
14	Code Review	
15	Nirbhaya Portal and Intranet Web Portal	
16	BI, Reporting and Analytics	
17	Location Detection Interface	
18	Incoming SMS per day	20,000
19	Outgoing SMS per day	50,000
20	Virtual Machine	
20.A	Grade 1	
20.B	Grade 2	
20.C	Grade 3	
20.D	Grade 4	
20.E	Grade 5 for CAD	16
20.F	Grade 6 for CAD	16
20.G	Grade 7 for CAD	8
21	Database Activity Monitoring	
22	Public IP Address	10
23	VPN User License	20000

*Depending upon the successful implementation of the project, Agents licensees and MDT may increase by about 50%.

17.4.3 FMS staff distribution

S.No.	State	Indicative No. of FMS staff (Considering 1 FMS personnel per 50 operators)
1	Andaman and Nicobar Islands	1
2	Andhra Pradesh	3
3	Arunachal Pradesh	1
4	Assam	2
5	Bihar	5
6	Chandigarh	1
7	Chhattisgarh	3
8	Dadra and Nagar Haveli	1
9	Daman and Diu	1
10	Delhi	3
11	Goa	1
12	Gujarat	3
13	Haryana	1
14	Himachal Pradesh	1
15	Jammu and Kashmir	1
16	Jharkhand	2
17	Karnataka	3
18	Kerala	2
19	Lakshadweep	1
20	Maharashtra	5
21	Manipur	1
22	Meghalaya	1
23	Mizoram	1
24	Madhya Pradesh	4
25	Nagaland	1
26	Odisha	2
27	Puducherry	1
28	Punjab	2
29	Rajasthan	4
30	Sikkim	1
31	Tamil Nadu	3
32	Tripura	1
33	Uttar Pradesh	11
34	Uttarakhand	1
35	West Bengal	4
36	Telangana	1
	Total	80

18 Annexure

18.1 Services to be provided by CAD provider

18.1.1 CAD Software

18.2 Vernaculars to be supported

- Assamese
- Bengali
- Gujarati
- Kannada
- Malayalam
- Marathi
- Oriya
- Punjabi
- Tamil
- Telugu
- Urdu

Instructions for filling Section 5 - A

1	It is **mandatory** to fill up **all sheets** provided under this **Section 5 - A**
2	Bidder should fill up the specification sheets in the given format.
3	Bidder should ensure that none of the listed parameters are modified, deleted and no additional parameter is added. (Remarks, if any, should be indicated separately in the Remarks column)
4	In case the Bidder is proposing any additional product category that is not listed in this section, he may use additional sheets.
5	Wherever **minimum requirements** are specified, it is **mandatory** to indicate with a YES or NO, whether the solution being offered **complies to the minimum requirements** stated. In case of non-compliance, Details/remarks must be provided.
6	It is mandatory to fill up the "Bidder's Response" column against all the listed parameters / features.
7	**Incomplete/ missing information or information not adhering to the prescribed format may not be considered during evaluation of bid and/or for award of marks.**
8	The bidder is advised not to make any changes to any information in the functional requirements. For example, insert a row or delete a row or modify any other information like change the functionality required, etc. In case the bidder modifies any information the response would be rejected.

Section 5 - A
Minimum Software Requirements Specifications

#	Description
1	Nirbhaya Portal
2	Business Intelligence (BI), Reporting & Analytics
3	Enterprise Management System (EMS)
4	Identity Management Software (IMS)
5	Email Solution
6	E-Learning Software
7	Anti-Virus
8	Case Record Management (CRM)
9	Directory Services
10	Interanet Web Portal
11	Virtual Machine
12	Code Review

Nirbhaya Portal						
Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS products/ component if relevant	Bidder's Comments
NPOR.REQ.001	General requirement	The Portal should be hosted at the data center infrastructure being installed by the bidder				
NPOR.REQ.002	General requirement	The Portal should be state of the art with user friendly interface,informative, interactive and easily accessible.				
NPOR.REQ.003	Citizen Registration	The Portal should be able to register citizens on the website.				
NPOR.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/increase on later stages.				
NPOR.REQ.005	Citizen Registration	The information collected from the registration should be verified with one time password on the Citizen mobile number.				
NPOR.REQ.006	Citizen Registration	Once the Citizen has registered, the Citizens would be prompted to download the mobile application				
NPOR.REQ.007	Search Functionality	The Portal should be searchable to query registration patterns, users, regional specifics etc.				
NPOR.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 purchaser				
		Access to various literature related to rules and regulations				
		Feedback and RSS feed.				
		News Section				
		Contact us				
		Link for administrators for various modules/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				
		MIS reports for citizen, Purchaser and identified stakeholders.				
		The Portal shall be linked to social media sites (Facebook, twitter etc.) and count should be displayed of no. of likes of the Nirbhaya 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/ non-emergency numbers etc.				
NPOR.REQ.009	Chat Window	The Portal should be integrated with Chat Window functionality where citizen can do the chat with call center agent. Citizen should be able to initiate the chat after giving the location of the chat location, citizen name and contact number.				

Nirbhaya Portal						
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Requirement available (Yes/ No)**	**Standard/ Customized/ Bespoke**	**Provide Name of COTS products/ component if relevant**	**Bidder's Comments**
NPOR.REQ.010	Webmail Access	The Portal should be integrated with webmail solution of the internal users where Purchaser users can access the email with their login id and password.This access is not for citizens.				
NPOR.REQ.011	Common requirements of Portal	The portal should meet and compliant the web deisgn and security guidelines of Govt. of India				
		The system should adhere to Best/Standard programming practices and OWASP-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.				
NPOR.REQ.012	Portal Administrator	The Portal should have administrator console where administrator can manage the content, users and can create portal dynamic menus (a common navigation bar should be included on all pages)				
		The Portal administrator should be able to modify/ design custom look and feel of the portal with minimal change in software code.				
NPOR.REQ.013	Portal Administrator - Publishing	The system should allow the authorized user to publish Emergency Helpline news, articles, events etc.				
NPOR.REQ.014	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				
		· News room				
		· News search key word				
		· News main content				
		The system should allow the user to attach image related to news				
NPOR.REQ.015	Multimedia Support	The system should adhere to automatically format images and other rich media based on predefined standards for resolution, size etc.				
NPOR.REQ.016	Security	The system shall ensure virus check for all files that are uploaded in Solution e.g. detect malicious executables.				
NPOR.REQ.017	Security	Where ever documents are involved, the system should allow the user to assign a note/annotation to a document image.				
NPOR.REQ.018	Security	The system shall support provide support for HTTPs/SSL for secured data transfer and session timeouts.				
NPOR.REQ.019	Audit Trail	The system shall display the date and time of last login when the user logs in.				

Nirbhaya Portal						
Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS products/ component if relevant	Bidder's Comments
NPOR.REQ.020	Portal Content Management	The system should allow the authorized user, through a user friendly GUI, to manage/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.				
NPOR.REQ.021	Portal Content Management	The front end user interface must be integrated with content management solution for easy management and change of theme design.				
NPOR.REQ.022	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.				
NPOR.REQ.023	Portal Content Management	The system should allow the authorized user, through a user friendly GUI, to create meta tag search of each web page.				
NPOR.REQ.024	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				
NPOR.REQ.025	Portal Content Management	The system should allow the authorized user, through a user friendly GUI.				
NPOR.REQ.026	Search Content	The system should be able to search the Fire, Medical, Police and other databases as per requriment.				
NPOR.REQ.027	Reporting access	All reports from BI/Reporting engine should be available to authorized users. There should be user access control on Nirbahya portal				
NPOR.REQ.028	General Requirement	Portal should be able to handle 10000 concurrent users with response time of one second				
NPOR.REQ.029	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.				

Business Intelligence (BI), Reporting And Analytics

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS products/ component if relevant	Bidder's Comments
BIRA.REQ.001	General Requirement	The system shall be provided in high availability configuration to avoid any single point of failure				
BIRA.REQ.002	Auto 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 delivery of both manually generated and scheduled reports to a file directory or folder				
BIRA.REQ.003	Archiving	It should be possible to archive/store certain data for more than one year. Such selected data could be electronically flagged to enable easy classification and then separate storage also.				
BIRA.REQ.004	Predictive Analytics	The software should have the capability to perform predictive analytics which can help in extracting information to predict trends like deployment the police officials around a certain area within a state on the basis of emergency/non-emergency calls made over a period of time etc.				
BIRA.REQ.005	Pattern Analytics	The software should have a capability to perform the pattern analytics which can help in extracting the information to pattern trends like Crime pattern like robbery, women cases w.r.t state, district and city level etc.				

Business Intelligence (BI), Reporting And Analytics

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS products/ component if relevant	Bidder's Comments
BIRA.REQ.006	General Requirement	The following daily, Weekly,monthly and yearly trending reports must be provided by system. The given below reports are for reference purpose only.It may update and can increase on later stages.Reports should be categorised into State/District/City level also. 1. Average Speed of Answer 2. Service Level Percentage 3. Calls Offered 4. Calls Handled 5. Abandoned Call Rate 6. Average Talk Time 7. Average Hold Time 8. Average Handle Time 9. Longest Delay Before Answered 10. Outbound Call Volume 11. Outbound Call Duration 12. Average Delay before Abandon 13. Longest Delay before Abandon 14. Number of calls exceeding threshold (i.e. calls waiting in queue longer than given time) 15. Average time in queue by call type 16. After Call Work (Wrap Up) 17. Operator Hours Report 18. Staffing Distribution Report 19. Number of instances the operator found busy 20. Calls made / referred to stakeholder institutions 21. Call type 22. Development of suitable Management Information System (MIS) for reporting periodical progress in redress of public grievances 23. Category/Sub-Category-wise complaint registration/resolution status 24. Category/Sub-Category-wise Complaint escalation status 25. Area wise problem based (emergency and non-emergency) analytical report on monthly/quarterly basis based on call data base. Prepare and submit problem based schematic maps for districts/groups of districts 26. Vehicle distance travelled to the caller/user location				

Business Intelligence (BI), Reporting And Analytics

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS products/ component if relevant	Bidder's Comments
BIRA.REQ.007	Tools for Analysis on GIS map	It should be possible to analyse crime and criminals in. at least , the following ways: 1. Hot Spot Analysis 2. Trend Analysis 3. Suspect Analysis 4. Crime forecasting 5. Journey to crime 6. Response time 7. Repeat Callers 8. Change over Time mapping 9. Neighbourhood Analysis 10. Serial sex offender tracker 11. Patrol Charts 12. Crime against women etc. This list is for reference purpose and may update/increase on later stages.				
BIRA.REQ.008	Dataware House And Searching	Datawarehouse should be cretaed to manage all BI and reporting system reports.System should have functionality to search structured data,unstructured data, video and images as well in the system				
BIRA.REQ.009	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.				
BIRA.REQ.010	Application Integration	It should be integrated with other application of purchaser for data analysis and reporting				
BIRA.REQ.011	Exception Reporting	The ability to generate reports as a result of critical event/scenario such as system capacity utilization nearing threshold or average handle time of a call falls below defined threshold for a call operator				
BIRA.REQ.012	Architecture	The data components of the architecture should include the internal and external sources of structured and unstructured data that users/stakeholders will need to access and analyse to meet their requirements				
BIRA.REQ.013	Data Integration	The BI software should have data integration tools available that seamlessly and natively integrate with other applications				
BIRA.REQ.014	Data Quality Tool	Data quality tools and methodologies to support the preparation of data for business intelligence applications and reporting				

Business Intelligence (BI), Reporting And Analytics

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS products/ component if relevant	Bidder's Comments
BIRA.REQ.015	Master Data Management	Master Data Management tools and methodologies to support the preparation of a system of record for business intelligence applications and reporting				
BIRA.REQ.016	Metadata Management	Metadata Management – Tool should enable the creation, consolidation , ongoing auditing and reporting on the metadata				

Enterprise Management System (EMS)

Sr. No.	Item	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
EMS.REQ.001	Enterprise Management System	Bidder should quote tool for monitoring services, & SLA along with Helpdesk tool for the Department along with all the necessary Hardware, DB, OS, etc.				
EMS.REQ.002	Enterprise Management System	Solution should be scalable and open to third party integration.				
EMS.REQ.003	Enterprise Management System	Should support Web / Administration Interface.				
EMS.REQ.004	Enterprise Management System	Should provide compatibility to standard RDBMS.				
EMS.REQ.005	Enterprise Management System	The Service Management solution namely Service desk (incident and problem mgmt.), Change, and SLA management should have shared configuration database with a unified architecture.				
EMS.REQ.006	Enterprise Management System	Offered solution should provide for future scalability of the whole system without major architectural changes.				
EMS.REQ.007	Enterprise Management System	Enterprise Management System should provide for end to end performance, availability, fault and event and impact management for all enterprise resources that encompasses the heterogeneous networks, systems, applications, databases and client infrastructure present in the enterprise.				
EMS.REQ.008	Enterprise Management System	The agent and agentless monitor should be able to collect & manage event/fault, performance and capacity data and should not require separate collectors.				
EMS.REQ.009	Enterprise Management System	The solution should reduce manual customization efforts and should speed-up problem identification and resolution of the IT performance anomalies with intelligent events.				
EMS.REQ.010	Enterprise Management System	The solution should accelerate problem isolation through accurate analysis of probable cause through end-to-end correlation.				
EMS.REQ.011	Enterprise Management System	The solution should have the capability to identify probable root cause using a variety of filtering and statistical correlation methods to determine their relevance to the issue being researched.				
EMS.REQ.012	Enterprise Management System	The solution should possess capabilities that deliver self-learning capabilities to virtually eliminate the effort of manual threshold, rule, and script maintenance.				
EMS.REQ.013	Enterprise Management System	The agent and agentless monitor should be able to collect & manage event/fault, performance and capacity data and should not require separate collectors.				
EMS.REQ.014	Enterprise Management System	The solution should have predictive analytics and intelligence in-built into it so as to detect any anomaly before it could potentially hit the threshold thereby giving enough lead time to users to resolve the issues before the threshold is breached.				

Enterprise Management System (EMS)

Sr. No.	Item	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
EMS.REQ.015	Enterprise Management System	The solution should carry out automated probable cause analysis by picking up feeds from every infrastructure component being monitored and automating the correlation of these alarms/events to point out the probable cause of an infrastructure error.				
EMS.REQ.016	Enterprise Management System	Solution should carry out probable cause analysis thereby helping operators to identify the root cause without having to write complex rules for correlation.				
EMS.REQ.017	Enterprise Management System	Solution should be able to score the events and display the highest impacting events in descending order or any other order as customized by the administrator.				
EMS.REQ.018	Enterprise Management System	The Solution should offer the ability to monitor any				
EMS.REQ.019	Enterprise Management System	custom/home-grown applications for which the monitoring areas have been defined.				
EMS.REQ.020	Enterprise Management System	The solution should be extensible enough to support capacity planning and optimization with data collected through the deployed performance management agent or from agentless data collectors.				
EMS.REQ.021	Enterprise Management System	Should be able to monitor/ manage large heterogeneous systems environment continuously.				
EMS.REQ.022	Enterprise Management System	Servers: Should be able to monitor the server instances, database and instance status, initialization parameters, CPU usage, parallel processing, and SQL tracing.				
EMS.REQ.023	Enterprise Management System	Should be able to monitor performance statistics reported as timings and throughput values for such operations as reads, writes, and recursive calls.				
EMS.REQ.024	Enterprise Management System	Should be able to monitor statistics reports as averages and percentages for such items as data caches hits, queue waits, disk sorts, and rollbacks.				
EMS.REQ.025	Enterprise Management System	The Network Management should monitor performance across heterogeneous networks having multiple categories of devices like firewall, switches etc. across Department including the DC, DR site.				
EMS.REQ.026	Enterprise Management System	It should proactively analyze problems to improve network performance.				
EMS.REQ.027	Enterprise Management System	The Network Management function should create a graphical display of all discovered resources.				
EMS.REQ.028	Enterprise Management System	Should monitor various operating system parameters such as processors, memory, files, processes, file systems etc. where applicable using agent /agentless on the servers to be monitored.				

Enterprise Management System (EMS)

Sr. No.	Item	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
EMS.REQ.029	Enterprise Management System	Provide performance threshold configuration for all the agents to be done from a central GUI based console that provide a common look and feel across various platforms in the enterprise. These agents could then dynamically reconfigure the performance monitors to use these threshold profiles they receive.				
EMS.REQ.030	Enterprise Management System	**IT Service Management**				
EMS.REQ.031	Enterprise Management System	Centralized IT helpdesk for technical and functional support should be maintained to respond to queries and solve issues of the users.				
EMS.REQ.032	Enterprise Management System	The Helpdesk should be accessible through various communication channels viz. Telephone, web based facility and email. The helpdesk should be able to respond to the queries/problems in the time limits as specified in Service Level Agreement.				
EMS.REQ.033	Enterprise Management System	Online Helpdesk system should be deployed and would be used for management and support activity. Service desk is envisaged as a tool that will facilitate the end-to-end service support for users. The proposed system should include required hardware and software and should have sufficient analyst licenses to meet the requirement of Project.				
EMS.REQ.034	Enterprise Management System	The Solution should have the complete ITIL process flow for Incident, problem, Change and release Management.				
EMS.REQ.035	Enterprise Management System	The solution should have Service Management Process Model in built based on ITIL v3 best practices.				
EMS.REQ.036	Enterprise Management System	At each stage in the cycle of the incident, the system should prompt users on the status and the missing information that is required to complete the flow.				
EMS.REQ.037	Enterprise Management System	In case any process step is missed, the system prompts users to complete that step before they move to the next step.				
EMS.REQ.038	Enterprise Management System	Solution should support reporting on the process flow to allow management to understand how organization is performing in terms of process adherence.				
EMS.REQ.039	Enterprise Management System	Solution should support multi-tenancy with complete data isolation as well as with ability for analysts based on access rights to view data for one, two or more organizational units.				
EMS.REQ.040	Enterprise Management System	Solution should automatically provide solutions from the knowledge base.				

Enterprise Management System (EMS)

Sr. No.	Item	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
EMS.REQ.041	Enterprise Management System	Workflow should be able to perform notification via email, SMS and the have provision to interface with other communication modes. The solution should provision the administrator to create new or modify existing workflow by using actions like set fields, push fields, SQL query etc.				
EMS.REQ.042	Enterprise Management System	The solution should provide the functionality of executing searches to the entire database.				
EMS.REQ.043	Enterprise Management System	**Incident/Problem Management**				
EMS.REQ.044	Enterprise Management System	Flexibility of logging incidents via various means - web interface, email, phone. Service Desk solution should allow detailed multiple levels/tiers of categorization on the type of incident being logged.				
EMS.REQ.045	Enterprise Management System	Service Desk solution should provide classification to differentiate the criticality of the security incident via the priority levels, severity levels and impact levels.				
EMS.REQ.046	Enterprise Management System	It should allow SLA to be associated with a ticket based on priority, severity, incident type, requestor, asset, location or group individually as well as collectively.				
EMS.REQ.047	Enterprise Management System	Solution should support fast service restoration leveraging previous incident data.				
EMS.REQ.048	Enterprise Management System	It should be possible for agent to view the 'Health of a selected asset' from within the ticket.				
EMS.REQ.049	Enterprise Management System	The health view should be consistent across platform (Windows & flavors of UNIX / Linux).				
EMS.REQ.050	Enterprise Management System	Should support automatic assignment of ticket to the right skilled resource based on business priority Ex - Database crash issue need not be assigned to a DBA unless the business service is completely down.				
EMS.REQ.051	Enterprise Management System	Asset causing the business failure and business service that has failed should be automatically related to the ticket.				
EMS.REQ.052	Enterprise Management System	It should be possible to architect a decentralized service operations (across OS, database and application versions).				
EMS.REQ.053	Enterprise Management System	For integrations with other EMS/NMS tools, various options for integration should be provided - APIs, web services, SDKs.				
EMS.REQ.054	Enterprise Management System	It should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues. Should support full text search capabilities.				
EMS.REQ.055	Enterprise Management System	**Change Management**				

Enterprise Management System (EMS)

Sr. No.	Item	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
EMS.REQ.056	Enterprise Management System	Should support Change Impact and change collision detection based on affected CIs from CMDB.				
EMS.REQ.057	Enterprise Management System	Solution should provide for Change Calendar with periodical views.				
EMS.REQ.058	Enterprise Management System	Should support self-service change request and fulfilment with standard change requests via service catalogue.				
EMS.REQ.059	Enterprise Management System	Should support Incident & problem driven change-release-deployment activities. End to End Release Management workflows should be supported with in-built rollback capabilities.				
EMS.REQ.060	Enterprise Management System	Should support unified change and release tools (planning, risk assessment, scheduling, and execution tools) for complete enterprise across virtual & physical environments, applications, etc.				
EMS.REQ.061	Enterprise Management System	**Configuration Management**				
EMS.REQ.062	Enterprise Management System	The Configuration Management Database should support multiple datasets with federation and reconciliation facilities so as to get data from various discovery tools and also through manual import process.				
EMS.REQ.063	Enterprise Management System	The Configuration Management should support Definitive Software and Media Library with content updates on a periodic basis.				
EMS.REQ.064	Enterprise Management System	Normalization of data should be possible along complete definitive media library – software, hardware with standardization on attributes.				
EMS.REQ.065	Enterprise Management System	Reconciliation of data should be possible with multiple data providers based on common attributes and ability to define precedence rules on attributes.				
EMS.REQ.066	Enterprise Management System	Federation of external data sources should be possible with ability to store common attributes inside CMDB and getting other attributes from external data sources in real time.				
EMS.REQ.067	Enterprise Management System	Should provide best in class integration capabilities with CMDB compliant APIs.				
EMS.REQ.068	Enterprise Management System	Should Provide a single shared view of services supporting Service Design, Transition and Operations stages of the lifecycle.				
EMS.REQ.069	Enterprise Management System	Should Provide a Service catalogue so as to establish a framework for Service definitions based on IT and business alignment.				
EMS.REQ.070	Enterprise Management System	Should Provide Service blueprints to describe functional and deployment models for the Service definitions.				
EMS.REQ.071	Enterprise Management System	Should automatically create Service models to describe how IT infrastructure supports business services.				

Enterprise Management System (EMS)

Sr. No.	Item	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
EMS.REQ.072	Enterprise Management System	Manage services consistently across heterogeneous Primary site & DR site and cloud environments.				
EMS.REQ.073	Enterprise Management System	**Service Level Management / Monitoring**				
EMS.REQ.074	Enterprise Management System	The SLA Monitoring function of the EMS is by far the most important requirement of the Integrated Project. This is on account of the fact that commitment of the projects to the citizens is dependent on an effective and continuous monitoring of the timelines within which citizens are served at the Portal or GSKs. In this context, the SLA Monitoring will have to possess the following capabilities:				
EMS.REQ.075	Enterprise Management System	Response times of Portal;				
EMS.REQ.076	Enterprise Management System	Transaction handling capacity of application server in terms of number of concurrent connects;				
EMS.REQ.077	Enterprise Management System	Should compile the performance statistics from all the IT systems involved and compute the average of the parameters over a month, and compare it with the SLA metrics laid down in the RFP;				
EMS.REQ.078	Enterprise Management System	Have a consolidated, automated graphical report for SLA compliance with ability to drill down to reason for non-compliance.				
EMS.REQ.079	Enterprise Management System	Manage service levels for delivery and support of business services.				
EMS.REQ.080	Enterprise Management System	Fast, repeatable process for defining and capturing service level measurements.				
EMS.REQ.081	Enterprise Management System	Real-time visualization of service level targets, agreement compliance data, penalties and rewards.				
EMS.REQ.082	Enterprise Management System	Deliver service level information and alerts directly to IT Operations and Service Support consoles.				
EMS.REQ.083	Enterprise Management System	Should support compliance and cost trending to assist in identifying areas for process and operational improvements.				
EMS.REQ.084	Enterprise Management System	**Service Request Management**				
EMS.REQ.085	Enterprise Management System	Should support single service catalogue for requestable services				
EMS.REQ.086	Enterprise Management System	Should provide for Service Requests Workflows and Fulfilment definitions for commonly used IT/non-IT services.				
EMS.REQ.087	Enterprise Management System	Catalog based on User profile				
EMS.REQ.088	Enterprise Management System	Ability to position both Custom-made and Standard Requests				

Enterprise Management System (EMS)

Sr. No.	Item	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
EMS.REQ.089	Enterprise Management System	Should send notifications to Customers based on the status				
EMS.REQ.090	Enterprise Management System	Should have the ability to extend and create new service request				
EMS.REQ.091	Enterprise Management System	Should have predefined catalogues that cover specific use cases				
EMS.REQ.092	Enterprise Management System	Should be completely web based and should be accessible from an portal				
EMS.REQ.093	Enterprise Management System	The services should be integrated to SLAs and should be auto measured for adherence.				
EMS.REQ.094	Enterprise Management System	**Reporting**				
EMS.REQ.095	Enterprise Management System	Should provide for Reports for Service Support and Service Delivery processes through a unified portal.				
EMS.REQ.096	Enterprise Management System	Should have ability to have a consolidated view of data collected from different types of operations (Eg - SLA compliance for a selected service, it's dependent SLAs, OLA and UPCs, it's changes by priority, open incidents by priority and status, it's assets and individual asset compliance, patches installed and compliance to patches etc.) and displayed in a universal portal				
EMS.REQ.097	Enterprise Management System	Provide users (based on role) to drill down to specific report/data on a need basis				
EMS.REQ.098	Enterprise Management System	Provide detailed reports on a specific area as per the need of the user				
EMS.REQ.099	Enterprise Management System	Should support multiple views with flexible structure along with role based access.				
EMS.REQ.100	Enterprise Management System	The Service Desk / Helpdesk & SLA Monitoring tool shall have software application which is ITIL compliant				

Identity Management Software (IMS)

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
IMS.REQ.001	General Requirement	The Identity Manager architecture should be an N Tier Architecture to allow portability between Operating systems and Application servers.				
IMS.REQ.002	General Requirement	Solution must be comprehensive with user provisioning, de-provisioning and password management tools				
IMS.REQ.003	General Requirement	Solution should be able to authenticate platforms proposed by the Bidder as part of the solution				
IMS.REQ.004	General Requirement	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. Bidder should own the responsibility for the Identity & 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				
IMS.REQ.005	General Requirement	The solution for identity lifecycle management should support Web Services standards				
IMS.REQ.006	General Requirement	Provisioning tool must support and provide business role based provisioning.				
IMS.REQ.007	General Requirement	Solution must support “Delegated” model of administration to support user administration based on department, type of user (intranet / extranet), location etc.				
IMS.REQ.008	General Requirement	Solution should use Workflow engine to define workflow to the user management processes.				
IMS.REQ.009	General Requirement	Solution must provide flexibility to allow users(only internal) to self register for less sensitive applications / modules with a pre-defined workflow. Solution must also allow users to reset their passwords on those applications / modules that they have accounts on without the intervention of the administrators / helpdesk.				
IMS.REQ.010	General Requirement	Must provide password management capabilities like, password resets, password synchronization				
IMS.REQ.011	General Requirement	Solution should support for delegation of authority and mechanisms to review delegations				
IMS.REQ.012	General Requirement	It is required that all provisioning activities are tracked by the provisioning tool for subsequent analysis if the need arises.				
IMS.REQ.013	General Requirement	Solution should support generation of audit reports without the target resources being available				
IMS.REQ.014	General Requirement	Solution should support offline reporting. Reporting should be available for target systems where provisioning is done even when the target systems are not available.				
IMS.REQ.015	General Requirement	Support for automatic detection of accounts which haven't been used / not owned by anyone etc.				

Identity Management Software (IMS)

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
IMS.REQ.016	General Requirement	Historical data should be readily available with minimal customization. Support historical reports such as who has/had what, when why and how, privilege reports, Access Reports, delegations, exceptions etc.				
IMS.REQ.017	General Requirement	Solution for single sign on should integrate with LDAP server and products that are part of solution.				
IMS.REQ.018	General Requirement	Solution should support agentless or agent based Single Sign On facility.				
IMS.REQ.019	General Requirement	Solution should be comprehensive to include both web based and client server applications				
IMS.REQ.020	General Requirement	The solution must provide central configuration of client.				
IMS.REQ.021	General Requirement	The Solution should provide integrated Identity Management, smart provisioning, business role management, access management (web single sign-on), OS access Management, client server single sign-on				
IMS.REQ.022	General Requirement	Solution should provide real-time visibility into the end-to-end operation of Access Management infrastructure. It should monitor the availability, health and performance of web agents, policy servers and back end data stores that are used by the access management solution.				
IMS.REQ.023	General Requirement	The solution should monitor web access management infrastructure around the clock, detect availability and performance problems proactively, and enable quick analysis when issues arise. The solution should provide comprehensive, real-time metrics such as: - Agent availability - Agent performance per operation - Agent cache status - Policy server availability, policy server performance per operation, policy server queue, thread, socket, and cache - Errors generated by back end data stores - Performance of calls to back-end data stores The solution should collect this information and provides a single view that enables administrators to gain visibility into their access management operations and take action when problems arise.				
IMS.REQ.024	General Requirement	Solution provide capabilities to define password policies e.g. password expiration, composition etc.				

Identity Management Software (IMS)						
Sr. No.	**Nature of Requirement**	**Minimum Requirement Description**	**Requirement available (Yes/ No)**	**Standard/ Customized/Bespoke**	**Provide Name of COTS product/ component if relevant**	**Bidder's Comments**
IMS.REQ.025	General Requirement	Solution should monitor Policy Server and Agent performance and availability, correlates Web application performance with access management performance, and determines if access management solution is impacting application performance				
IMS.REQ.026	General Requirement	The solution should provide Monitoring and management and various reports and metrics for administrators like success/failed logins , response time etc.				
IMS.REQ.027	General Requirement	The solution should provide for SLA management including: - Define service levels - Single view of SLA compliance, service status, performance, and usage - Manage system availability and performance from single dashboard				
IMS.REQ.028	General Requirement	Solution should have facilities for enforced-change of password after first-time login including after password reset, automatic password outage after a fixed period of time, maintenance of unique passwords that neither resemble login ID nor any of the previously used passwords (last 3 passwords), a combination of upper & lower cases, numbers and special characters, etc.				
IMS.REQ.029	General Requirement	Solution should have ability to detect and report in near real-time local administrator account maintenance (creation, deletion, changes) made directly on local resources natively.				
IMS.REQ.030	General Requirement	Solution should have ability to notify designated personnel of access-rights changes made outside the provisioning Solution				
IMS.REQ.031	General Requirement	Solution should allow customization of the “Look and Feel” of the User Interfaces. Solution should also allow customization of the user entry screens which determine the fields and the layout of each task screen.				
IMS.REQ.032	General Requirement	System shall provide web access management should provide a centralized Single Sign-On for web users requesting for accessing various modules as per their roles and policy.				
IMS.REQ.033	General Requirement	Solution should support for the latest Web standards, such as Transport Layer Security (TLS), SOAP transactions and Web Services Security.				
IMS.REQ.034	General Requirement	Solution should provide OS security hardening and extra levels of access control to the platform.				
IMS.REQ.035	General Requirement	Solution should provide protection against Back Doors and Trojan Horses				
IMS.REQ.036	General Requirement	Solution should allow administrators to construct logical host groups and deployment rules for streamlined policy deployment				
IMS.REQ.037	General Requirement	Solution must be able to centrally manage policy				

Identity Management Software (IMS)						
Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
IMS.REQ.038	General Requirement	Solution should provide centralized security policy enforcement of user entitlements by leveraging role- and rule-based access control				
IMS.REQ.039	General Requirement	Solution must control the number of sessions a user may have open simultaneously on one or more workstations				
IMS.REQ.040	General Requirement	Solution should be able to prevent highly privileged users, including application DBAs and others, from accessing sensitive applications and data in the databases outside their authorized responsibilities. For e.g. Central data store that consolidates system audit information and reports for IT auditing				
IMS.REQ.041	General Requirement	Solution should provide high availability and failover capabilities to eliminate any single point of failure				
IMS.REQ.042	General Requirement	Solution should use multiple load-balanced policy servers, policy agents, and directory instances to do so				
IMS.REQ.043	General Requirement	Bidder should provide an integrated solution to deliver authentication, authorization, federation, Single Sign on & web services security				
IMS.REQ.044	General Requirement	Solution should support multi-factor authentication technologies (tokens, certificates etc.)				
IMS.REQ.045	General Requirement	Out of the box reports should be available for user creation, deletion, assignment of access, approvals done, pending violations, password resets etc.				
IMS.REQ.046	General Requirement	Solution should provide real time fraud and risk management including but not limited to behavioural analysis, key loggers, Trojans and should allow monitoring on transactions and raise alerts in case of suspicious activities as defined by the security policy of organization.				

Email Solution

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
ES.REQ.001	Webmail	System should allow access to email from any web browser, like Internet Explorer or Mozilla Firefox, without needing to install any email software on client computer.				
ES.REQ.002	Search and save	System should auto-save mails in draft folders for mails not sent				
ES.REQ.003	Search and save	System should include built-in Search, providing users with the ability to find email messages quickly.				
ES.REQ.004	Shared Calendaring	Shared calendaring - allowing users to track all meetings, view other calendars, and share their calendar with others from within e-mail application.				
ES.REQ.005	Company Directory	The company directory is populated with contact information and can be accessed by all employees.				
ES.REQ.006	Contacts	The contact manager allows users to store address book information for an unlimited number of contacts and groups—all information is accessible from within email application.				
ES.REQ.007	Task Lists	Task lists will allow users to create multiple task lists, quickly add tasks from anywhere in webmail, and sort tasks by complete or incomplete.				
ES.REQ.008	Control Panel	The control panel allows email administrators to manage their account settings, create, modify, and delete mailboxes, setup aliases, and much more.				
ES.REQ.009	Control Panel	Statistics for users like Bandwidth Usage, Space Usage, Mail Sent & Received				
ES.REQ.010	Control Panel	Set preferences of Individual Mail Users about password change facility				
ES.REQ.011	Control Panel	Modify Mail Quota and Attachment Size for Individual Mail Users				
ES.REQ.012	POP3 / IMAP / SMTP	These are standard protocols that allow users to use desktop software like Outlook and Thunderbird and wireless devices such as Blackberry and Treo. Email application should support these protocols.				
ES.REQ.013	Spam Filtering	Protects users from spam and allows administrators and users to blacklist and safe list senders, and control the filtering sensitivity.				
ES.REQ.014	Spam Filtering	Reduce spam more effectively using appropriate spam control mechanism				
ES.REQ.015	Spam Filtering	Easy spam administration at the system, domain, or user level				
ES.REQ.016	Virus Scanning	Virus protection should incorporate multiple anti-virus (atleast 3 Level) scanners for maximum protection from computer viruses and security threats.				
ES.REQ.017	Size of Mailboxes	Folder auto-clean allows easy control over the size of folders				
ES.REQ.018	SSL and TLS Encryption	Provides SSL encryption for POP/IMAP/SMTP/Webmail in order to encrypt user data so that others cannot view it. This is very important for passwords and confidential emails. Email application could allow for classification of emails by confidentiality				
ES.REQ.019	User Groups	User can create as many user groups as needed, each of which can forward to a total of 50 email accounts. Up to four of those recipients can be sent to external email accounts.				
ES.REQ.020	Domain Aliases	User can create atleast 50 domain aliases. When an email is sent to a domain alias, the email is automatically directed to the corresponding email account in the original domain.				

Email Solution

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
ES.REQ.021	BCC Archiving	BCC archiving allows email administrators to archive all incoming and outgoing emails, storing them in a third party email account.				
ES.REQ.022	Auto-responders	Out-of-office and auto-responder facilities can be configured by users				
ES.REQ.023	User preference management	Ability to create user-defined folders				
ES.REQ.024	Email Gateway	Email gateway to authorize and authenticate emails in the system on requirement basis				
ES.REQ.025	User preference management	User level configuration such as templates, signatures, archival etc.				

E-Learning

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
EL.REQ.001	E-Learning	The agents 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	E-Learning	Quality monitoring evaluation data shall be used to assign targeted learning.				
EL.REQ.003	E-Learning	E-learning software should be pre-integrated with Work force management to schedule the training based on skill assessment of the agents				
EL.REQ.004	E-Learning	E-Learning software should allow access for scheduled training assignments while listening to a recorded interaction.				
EL.REQ.005	E-Learning	Integrated Scorecard should be able to aid in automatic lesson assignments when a KPI falls below an excepted goal				
EL.REQ.006	E-Learning	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	E-Learning	The E-Learning software should support remote access.				
EL.REQ.008	E-Learning	The E-Learning content development software should allow adding and or recording narration directly into the application without additional software requirement				

Anti-virus Solution

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if	Bidder's Comments
AVS.REQ.001	General Requirement	Anti-virus shall have auto update feature, it shall be able to push signature from the centralized server to all the clients / workstations				
AVS.REQ.002	General Requirement	Bidder shall ensure that the scan logs are made available for review.				
AVS.REQ.003	General Requirement	The solution must support mass mailing virus detection.				
AVS.REQ.004	General Requirement	The solution must support mail attachment virus detection.				
AVS.REQ.005	General Requirement	The solution must support Malformed Mail format detection.				
AVS.REQ.006	General Requirement	The solution must have a built in Safe Stamp feature.				
AVS.REQ.007	General Requirement	The solution must have its own Updated Recommended Virus Extensions.				
AVS.REQ.008	General Requirement	The solution must support Heuristics-based mail header detection for Spam.				
AVS.REQ.009	General Requirement	The solution must support Heuristics-based scanning of the mail body for Spam.				
AVS.REQ.010	General Requirement	The solution must support administrator defined Anti-Spam exception list (approved list).				
AVS.REQ.011	General Requirement	The solution must support administrator-defined non-approved list of known spammers.				
AVS.REQ.012	General Requirement	The solution shall be able to detect Spam based on multiple categories (such as general, commercial email, Get rich quick, pornography etc.).				
AVS.REQ.013	General Requirement	The solution shall be able to take action based on the category in which Spam is detected.				
AVS.REQ.014	General Requirement	The solution must be able to take different action based on the different sensitivity level of Spam detection.				
AVS.REQ.015	General Requirement	The solution must provide alerts based on action taken on the Spam mail.				
AVS.REQ.016	General Requirement	The solution must support Encrypted Mail Detection.				
AVS.REQ.017	General Requirement	The solution must support Password Protect Zip Detection.				
AVS.REQ.018	General Requirement	The solution must have a Secure SSL Web Management Console.				
AVS.REQ.019	General Requirement	The solution must be able to prevent System Denial of Service (‘DoS’) Attack.				
AVS.REQ.020	General Requirement	Bidder shall propose the required hardware for the entire solution				
AVS.REQ.021	General Requirement	Bidder shall provide requisite licenses for all the software required for the Anti-virus and Anti-spam Solution.				

Case Record Management (CRM)

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
CRM.REQ.001	All Communication Channel	The CRM software should be capable to receive call (Mobile, Landline),SMS, chat, email, VOIP (like Skype to Skype),social media like Facebook, Twitter, IOT (internet of things) like sensors, panic button and mobile apps to create an appropriate case and send the relevant case to the dispatcher after case assessment.				
CRM.REQ.002	Communication Channel - Call	The software should be able to display caller name, caller number and caller address on agent desktop. Data from Location Detection Interface: Automatic display of data on CRM screen Manual Data of the location: Agent should be capable to enter the location of the caller on CRM Screen				
CRM.REQ.003	Communication Channel - SMS	The software should be able to automatically create a case using SMS data (Phone No. & Message) and display on the agent desktop				
CRM.REQ.004	Communication Channel - SMS	The agent should be able to assess the SMS case and send the case to Outbound call agent/ Dispatcher after assessment				
CRM.REQ.005	Communication Channel - Email	The software should be able to automatically create a case using Email data (Email content) with attachment (not more than 7 MB) if any and display on the agent desktop.				
CRM.REQ.006	Communication Channel - Email	The software should be able to send the case to Outbound dialer/ Dispatcher after assessment.				
CRM.REQ.007	Communication Channel - VOIP	The software should be able to integrated with VOIP channel like Skype where agent can speak with the users on skype and can do chat on Skype and agent can create a case into CRM based on case assessment.				
CRM.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 agent desktop. This will also include integration of IOTs system designed by goverment agencies like MoRTH etc.				
CRM.REQ.009	Communication Channel - IOT	The agent should be able to send the case to the Outbound dialer/Dispatcher after assessment				

Case Record Management (CRM)

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
CRM.REQ.010	Communication Channel - Chat	The software should have a functionality where agent can receive the chat which is initiated by the web user in real time through Nirbhaya portal. If the user initiates the chat through personal messenger i.e. GTalk, Yahoo Messenger and other two messenger (to be decided later), then chat should be received into the CRM screen of the particular agent. The agent should be able to chat with the user in real time with the user.				
CRM.REQ.011	Communication Channel - Chat	If the agent is offline then the user should be able to send the messages to chat window and message should be received as an email to the CRM agent software				
CRM.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 agent desktop				
CRM.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 dialer/ Dispatcher after assessment.				
CRM.REQ.014	Communication Channel - Social Media	The CRM should be able to create case with data received from Facebook, Twitter and any two more open source API of social networking site. These other two open source API will be decided at later stage. This case will be created manually by agent into CRM software				
CRM.REQ.015	Communication Channel - Mobile Application	The CRM software should be integrated with Mobile Apps (registered with Purchaser) to receive location of the caller and caller number.				
CRM.REQ.016	Call Classification	The agent 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. Purchaser can add more classification at later stage.				
CRM.REQ.017	Call Transfer/Call Forward	CRM agent should be capable to transfer the call to the call center agent in other states / same state / transfer to dialled number by the agent Caller's Call should not be disconnected during call forwarding/ Transferring into the system				
CRM.REQ.018	SMS Case Transfer	A case to be considered where SMS is sent in Hindi and can't be read by the agent. Provision for profile of agents to be available to forward the SMS to appropriate agent				

Case Record Management (CRM)

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
CRM.REQ.019	Duplicate Calls	An incident may attract more than one call but each call is important as it may give details about eye witnesses 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.				
CRM.REQ.020	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 of Case. Whenever a call is merged, the system should not generate a new dispatch.				
CRM.REQ.021	Duplicate Calls	The software should alert the voice agent, Dispatcher, and Supervisor about the possibility of a single incident - Duplicate call situation				
CRM.REQ.022	Voice Recording	All calls should be recorded and tagged with the concerned event. They should be easily retrievable. The call should be recorded as it enters the system i.e. if a call is transferred from one agent to other agent, the recording should continue and be stored for the desired period.				
CRM.REQ.023	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.				
CRM.REQ.024	Case creation and Appraisal	System should facilitate Case creation, by providing 'a drop down menu' for various functions like creation of an Case, files attachment, location of nearby Case and other information related to an Case should be recorded and updated.				
CRM.REQ.025	Soft Phone Integration	The software should have a capability of a Telephone window allowing agents 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. Soft phone should have a feature to select the state for call forwarding/transferring/ conference call.				
CRM.REQ.026	Emergency Call	The software should have capabilities to create Hot Calls like fire in a building, disaster emergency. The agent should fill minimum information for a Hot call. Dispatcher and Supervisor should receive the alert / notification for the same. Dispatcher should be able to initiate action for quick response. To facilitate quick response to emergency calls / hot call, there should be special and dedicated hot call button in the agent software.				
CRM.REQ.027	Case Status Display And Search	The voice and non voice agent 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 no, Date & Time, Case Type etc.				

Case Record Management (CRM)

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
CRM.REQ.028	Location of Interest (LOI)	Once a Location of the incident is marked in the map, The agent shall have the facility to see for various 'Location of Interest (LOI)' in the vicinity of an case location like nearest Hospital, Blood Bank, Fire brigade. (Applicable in dispatcher module also).				
CRM.REQ.029	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, whenever a new case is created to save precious time in effective response to a distress call.				
CRM.REQ.030	Update Existing Case	The software should allow the agent to update / 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.				
CRM.REQ.031	Alert Notification	Software should have capability to alert an agent or supervisor if a case is not attended in pre-defined time duration.				
CRM.REQ.032	Pre-defined Q&A	A freely configurable structured query script should be available within the software to assist both agent (Voice agent and Non Voice agent) 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 both agent (Voice and Non Voice agent) should be prompted.				
CRM.REQ.033	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.				
CRM.REQ.034	Case Cancel/Close	The Case like raily 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/ Cancel/postponed the Case manually into the system				
CRM.REQ.035	Call back	Voice agent should be able to call back the caller with the click of the mouse.				
CRM.REQ.036	Caller Address conflict handling	It should be possible to find the numbers whose subscriber information and caller information recorded by the Voice agent are different and generate a report for the concerned agency.				
CRM.REQ.037	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 IVRS system / email / SMS to Non Emergency helpline				
CRM.REQ.038	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.				
CRM.REQ.039	Incident scheduling and Mapping	The Scheduled Case feature should allow operators to create, edit, delete, and search for a scheduled Case.				

Case Record Management (CRM)						
Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
CRM.REQ.040	Language Support	It should be possible to switch between English, Hindi or any other regional language. Every State should have support for Hindi, English and one regional language				
CRM.REQ.041	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.				
CRM.REQ.042	Call Conference	Agent should be able to do conference call with agents in same call center and other state call center agents (Voice agent or non voice agent , Dispatcher and Supervisor) / Other dialled number by the agent. Caller's Call should not be disconnected during the conference call by the system				
CRM.REQ.043	Other Agent Status For Call Conference / Forward Call	Agent should be able to see the agents status (like busy/ Free) with agent extension of the same state or other state and agent language (like agent can speak Hindi, English or any other native language) to forward/transfer/ conference call with the caller				
CRM.REQ.044	Outbound Call	Agent should be able to see any type of call like Missed call/Drop Call Case and can call back from the application.				
CRM.REQ.045	Outbound Call	Agent should be able to dial the international number in case of international caller is in distress and contact to the proposed system.				
CRM.REQ.046	General Requirement	System shall merge or split (Case for Service) CFS depending upon the situation				
CRM.REQ.047	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 like dial 100, 1091 etc.				
CRM.REQ.048	General Requirement	System supports the ability to put a case that has not been accepted into the system on hold so that a higher priority Case can be handled like unknown Number case.				
CRM.REQ.049	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.				
CRM.REQ.050	Standard Operating Procedures (SOP's)	The software should have capabilities to set the Standard Operating Procedures (SOP) for agents. The same needs to be invoked during Case creation by the Voice and Non Voice agent. It should also be possible to remodel the Case, Case sub types, priorities and type of service required by using a remodelling tool.				
CRM.REQ.051	Location History Storage and Optimization	The software should store/update the location history of the caller in CRM database. This history should be gradually increased and optimized in the system as per requirement				
Messaging						

Case Record Management (CRM)

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
CRM.REQ.052	Messaging	The CRM software should have an ability for messaging between agents (with in call center and other state call center)				
CRM.REQ.053	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.				

Directory Server

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
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	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	Genreal 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				
DS.REQ.007	Synchronization	Support for data synchronization with third party identity stores (Active directory etc.)				
DS.REQ.008	Standards	Adherence to LDAP Standards RFC 2696, RFC 3671 etc.				
DS.REQ.009	Failover mechnism	Support for server failover and failback				
DS.REQ.010	Security	Support for protection against any kind os 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				

Intranet Web Portal

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
IP.REQ.001	General Requirement	The intranet portal is required to manage the all kind of documents at one place in the system and a web portal required is required to access those documents in the system				
IP.REQ.002	General Requirement	The portal should have access, upload, view, delete functionality for the documents				
IP.REQ.003	General Requirement	The portal should have functionality to categorize the documents in the portal like deliverable documents, Development documents, Invoice etc.				
IP.REQ.004	General Requirement	The portal should have provision to provide the access to different kind of user to read, edit and update the documents				
IP.REQ.005	General Requirement	The portal should have a admin console to manage the complete portal with GUI, Data on the portal and management of the documents				
IP.REQ.006	General Requirement	The portal should have a functionality to show all kind of version of the uploaded/modified documents				
IP.REQ.007	General Requirement	The portal should have audit functionality to keep the track changes by the user in the system				
IP.REQ.008	General Requirement	The portal should have a user friendly GUI to access the features of the portal				
IP.REQ.009	General Requirement	The portal should be integrated with Single sign on in the system				
IP.REQ.010	General Requirement	If any document gets removed from the system through portal then a email alert should be sent to the administrator about the documents with user detail, document detail, Date , time etc.				
IP.REQ.011	General Requirement	These are some of the features which require in the portal, Some of the features can be added by the purchaser on later stages of the project				

Virtual Machine

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
Grade 1						
VM.REQ.001	vCPU	1 vCPU				
VM.REQ.002	RAM	4 GB				
VM.REQ.003	Storage	150 GB				
Grade 2						
VM.REQ.004	vCPU	2 vCPU				
VM.REQ.005	RAM	8 GB				
VM.REQ.006	Storage	200 GB				
Grade 3						
VM.REQ.007	vCPU	4 vCPU				
VM.REQ.008	RAM	32 GB				
VM.REQ.09	Storage	250 GB				
Grade 4						
VM.REQ.010	vCPU	8 vCPU				
VM.REQ.011	RAM	128 GB				
VM.REQ.012	Storage	300 GB				
Grade 5						
VM.REQ.013	vCPU	12 vCPU				
VM.REQ.014	RAM	512 GB				
VM.REQ.015	Storage	1 TB				
VM.REQ.016	Operating System	Red Hat Linux 7.1 server version for x86-64				
Grade 6						
VM.REQ.013	vCPU	4 vCPU				
VM.REQ.014	RAM	256 GB				
VM.REQ.015	Storage	1 TB				
VM.REQ.016	Operating System	Red Hat Linux 7.1 server version for x86-64				
Grade 7						
VM.REQ.013	vCPU	8 vCPU				
VM.REQ.014	RAM	512 GB				
VM.REQ.015	Storage	1 TB				
VM.REQ.016	Operating System	Red Hat Linux 7.1 server version for x86-64				

Code Review

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
CR.REQ.001	General Requirement	Environment: JAVA,J2EE,PHP,ASP,ASP.NET,VB,VB.NET,VBScript,JavaScript				
CR.REQ.002	General Requirement	Operating System				
		Windows, Linux				
		Databases:				
		Oracle, Microsoft SQL, MYSQL, Postgre				
		Web Server:				
		IIS, Apache Tomcat				
CR.REQ.003	Enterprise Version	Should be available as a solution deployable in enterprise mode				
CR.REQ.004	Enterprise Version	Should provide centralized management				
CR.REQ.005	Enterprise Version	Should provide ability to create different users with different access privileges for management and code scanning.				
CR.REQ.006	Enterprise Version	Should support remote management over a secure channel				
CR.REQ.007	Analysis Criteria and standards support	Should analyze for vulnerabilities compatible with industry standards				
CR.REQ.008	Analysis Criteria and standards support	Should analyze and report set of classes of software security weaknesses and detect critical vulnerabilities in the source code of applications such as: Un-validated Input Improper Error handling API abuse Secure Password storage Memory leakage/buffer overflow				
CR.REQ.009	Analysis Criteria and standards support	The solution should be flexible to add updates for new attacks				
CR.REQ.010	Analysis Criteria and standards support	The solution should have low false positives				
CR.REQ.011	Analysis Criteria and standards support	The solution should do Application source code scan with a high degree of accuracy and minimal false negative ratio				
CR.REQ.012	Analysis Criteria and standards support	Provide details on the analysis methodology being used in the proposed solution				

Code Review

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
CR.REQ.013	Configuration and Administration	The solution should have ability to provide comprehensive features for ease of management in terms of user Management, access control, rule configuration, automatic vulnerability scanning and reporting.				
CR.REQ.014	Configuration and Administration	The solution should provide customizable Dashboard Display support				
CR.REQ.015	Configuration and Administration	The proposed solution should provide customization support				
CR.REQ.016	Configuration and Administration	The solution should not report a weakness instance that is suppressed in order to reduce false positives				
CR.REQ.017	Configuration and Administration	The solution should support Customizing Rule set i.e. creation/alteration of rule set as per the user specific needs.				
CR.REQ.018	Configuration and Administration	The solution should provide event-logging mechanism.				
CR.REQ.019	Remediation	The solution should provide suggestive remediation for fixing highlighted vulnerabilities as per the recommended industry standard				
CR.REQ.020	Remediation	The solution should provide complete traceback from attack entry point to the final exploit point along with the location and path details				
CR.REQ.021	Environment Compatibility	The solution should be compatible with the following programming and scripting languages: Java, J2EE ASP, ASP.NET, VB, VB.NET, C# PHP (Linux)/PHP (Windows) XML, HTML VBScript, JavaScript				
CR.REQ.022	Environment Compatibility	The proposed solution should support the use of the following databases: Oracle, Microsoft SQL, PostGresSQL and MySQL.				
CR.REQ.023	Environment Compatibility	The proposed solution should support IIS/Apache Tomcat web Servers.				
CR.REQ.024	Environment Compatibility	The proposed solution should have IDE Plugin Support				
CR.REQ.025	Environment Compatibility	The proposed solution should support at least the following frameworks: J2EE/EJB Struts				

Code Review

Sr. No.	Nature of Requirement	Minimum Requirement Description	Requirement available (Yes/ No)	Standard/ Customized/ Bespoke	Provide Name of COTS product/ component if relevant	Bidder's Comments
CR.REQ.026	Multiplatform Licensing Support	The proposed solution should support multiple Operating environments such as Windows and Linux.				
CR.REQ.027	Multiplatform Licensing Support	The proposed solution should have license support for both Windows and Linux operating environments.				
CR.REQ.028	Reporting and Logging	The solution should report the location of any weaknesses by providing the directory path, filename and line number.				
CR.REQ.029	Reporting and Logging	The solution should provide both selective and consolidated reporting at granular levels				
CR.REQ.030	Reporting and Logging	Report of selected vulnerability category/severity				
CR.REQ.031	Reporting and Logging	Complete consolidated Report				
CR.REQ.032	Reporting and Logging	The solution should support report customization to meet user specific needs				
CR.REQ.033	Reporting and Logging	The solution should have the ability to generate and export reports in HTML and PDF formats.				
CR.REQ.034	Reporting and Logging	The solution should report the traced vulnerable issues with detailed and effective remediation mechanism.				
CR.REQ.035	Others	The solution should have CLI Support				
CR.REQ.036	Others	The solution should support Multiple Scanning of application project				
CR.REQ.037	Others	The solution should have Delta Analysis (comparison of last two scans) Support				
CR.REQ.038	Others	The Solution should provide Web Services (Web2.0/AJAX) Support				
CR.REQ.039	Others	The Solution should have audit trail mechanism service				

Instructions for filling Section 5 B	
1	It is **mandatory** to fill up **all sheets** provided under this **Section 5 B**
2	Bidder should fill up the specification sheets in the given format using MS-Excel.
3	Bidder should ensure that none of the listed parameters are modified, deleted and no additional parameter is added. (Remarks, if any, should be indicated separately in the Remarks column)
4	In case the Bidder is proposing any additional product category that is not listed in this section, he may use additional sheets.
5	In case the software proposed by the Bidder has multiple modules/components that are priced and sold separately, the Bidder should use additional sheets for each such module/component and include the licensing policy and number of licenses proposed for the same in the respective sheets. The same should also be reflected in the Commercial Bid format as new line items with the above said references.
6	Wherever **minimum requirements** are specified, it is **mandatory** to indicate with a YES or NO, whether the solution being offered **complies to the minimum requirements** stated. In case of non-compliance, Details/remarks must be provided.
7	It is mandatory to fill up the "Bidder's Response" column against all the listed parameters / features.
8	**Incomplete/ missing information or information not adhering to the prescribed format may not be considered during evaluation of bid and/or for award of marks.**
9	The Bidder is advised not to make any changes to any information in the functional requirements. For example, insert a row or delete a row or modify any other information like change the functionality required, etc. In case the bidder modifies any information the response would be rejected.

Section 5 B
Minimum Technical Requirements Specifications - Hardware

Item	Minimum Description
1	Managed Access Switch
2	UPS
3	Desktop
4	IP Phone Device
5	Lasr Jet Printer
6	Mobile Data Terminal Devices (MDT)
7	LED TV for Conference Room
8	Cloud Hosting Specification
9	Video Wall Projection Type

Managed Access Switch

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
MAS.REQ.001	Switch Architecture and Performance	Switch should have 24 Nos. 10/100/1000Base-TX auto-sensing plus 4x1G SFP uplinks.		
MAS.REQ.002	Switch Architecture and Performance	Should support stacking using dedicated stacking ports with up to 80Gbps throughput		
MAS.REQ.003	Switch Architecture and Performance	Switch should support link aggregation across multiple switches in a stack.		
MAS.REQ.004	Switch Architecture and Performance	Should support stacking of minimum of eight switches		
MAS.REQ.005	Switch Architecture and Performance	Switch should have non-blocking wire-speed architecture.		
MAS.REQ.006	Switch Architecture and Performance	Switch should support IPv4 and IPv6 from day One		
MAS.REQ.007	Switch Architecture and Performance	Switch should have non-blocking switching fabric of minimum 56 Gbps or more		
MAS.REQ.008	Switch Architecture and Performance	Switch should have Forwarding rate of minimum 41 Mpps.		
MAS.REQ.009	Layer 2 Features	IEEE 802.1Q VLAN tagging.		
MAS.REQ.010	Layer 2 Features	802. 1Q VLAN on all ports with support for minimum 255 active VLANs and 4k VLAN ids		
MAS.REQ.011	Layer 2 Features	Support for minimum 8k MAC addresses		
MAS.REQ.012	Layer 2 Features	Spanning Tree Protocol as per IEEE 802.1d		
MAS.REQ.013	Layer 2 Features	Multiple Spanning-Tree Protocol as per IEEE 802.1s		
MAS.REQ.014	Layer 2 Features	Rapid Spanning-Tree Protocol as per IEEE 802.1w		
MAS.REQ.015	Layer 2 Features	Self-learning of unicast & multicast MAC addresses and associated VLANs		
MAS.REQ.016	Layer 2 Features	Jumbo frames up to 9000 bytes		
MAS.REQ.017	Layer 2 Features	Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.		
MAS.REQ.018	Layer 2 Features	Port mirroring functionality for measurements using a network analyzer.		
MAS.REQ.019	Layer 2 Features	Switch should support IGMP v1/v2/v3 as well as IGMP v1/v2/v3 snooping.		
MAS.REQ.020	Quality of Service (QoS) Features	Switch should support classification and scheduling as per IEEE 802.1P on all ports.		
MAS.REQ.021	Quality of Service (QoS) Features	Switch should support DiffServ as per RFC 2474/RFC 2475.		
MAS.REQ.022	Quality of Service (QoS) Features	Switch should support four queues per port.		
MAS.REQ.023	Quality of Service (QoS) Features	Switch should support QoS configuration on per switch port basis.		
MAS.REQ.024	Quality of Service (QoS) Features	Switch should support classification and marking based on IP Type of Service (TOS) and DSCP.		
MAS.REQ.025	Quality of Service (QoS) Features	Switch should provide traffic shaping and rate limiting features (for egress as well as ingress traffic) for specified Host, network, Applications etc.		
MAS.REQ.026	Quality of Service (QoS) Features	Strict priority queuing guarantees that the highest-priority packets are serviced ahead of all other traffic.		

Managed Access Switch

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
MAS.REQ.027	Security Features	Switch should support MAC address based filters / access control lists (ACLs) on all switch ports.		
MAS.REQ.028	Security Features	Switch should support Port as well as VLAN based Filters / ACLs.		
MAS.REQ.029	Security Features	Switch should support RADIUS and TACACS+ for access restriction and authentication.		
MAS.REQ.030	Security Features	Secure Shell (SSH) Protocol, HTTP and DoS protection		
MAS.REQ.031	Security Features	IP Route Filtering, ARP spoofing, DHCP snooping etc.		
MAS.REQ.032	Security Features	Should support DHCP snooping, DHCP Option 82, Dynamic ARP Inspection (DAI)		
MAS.REQ.033	Security Features	Should support a mechanism to shut down Spanning Tree Protocol Port Fast-enabled interfaces when BPDUs are received to avoid accidental topology loops.		
MAS.REQ.034	Security Features	Should support a mechanism to prevent edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.		
MAS.REQ.035	Security Features	Switch should support static ARP, Proxy ARP, UDP forwarding and IP source guard.		
MAS.REQ.036	Security Features	Switch should Support Ipv6 First hop Security with the following functions: IPv6 snooping, IPv6 FHS binding, neighbor discovery protocol (NDP) address gleaning, IPv6 data address gleaning, IPv6 dynamic host configuration protocol (DHCP) address gleaning, IPv6 device tracking, neighbor discovery (ND) Inspection, IPv6 DHCP guard, IPv6 router advertisement (RA) guard		
MAS.REQ.037	Management, Easy-to-Use Deployment and Control Features	Switch should have a console port with RS-232 Interface for configuration and diagnostic purposes.		
MAS.REQ.038	Management, Easy-to-Use Deployment and Control Features	Switch should be SNMP manageable with support for SNMP Version 1, 2 and 3.		
MAS.REQ.039	Management, Easy-to-Use Deployment and Control Features	Switch should support all the standard MIBs (MIB-I & II).		
MAS.REQ.040	Management, Easy-to-Use Deployment and Control Features	Switch should support TELNET and SSH Version-2 for Command Line Management.		
MAS.REQ.041	Management, Easy-to-Use Deployment and Control Features	Switch should support 4 groups of embedded RMON (history, statistics, alarm and events).		
MAS.REQ.042	Management, Easy-to-Use Deployment and Control Features	Switch should support system and event logging functions as well as forwarding of these logs to multiple syslog servers.		
MAS.REQ.043	Management, Easy-to-Use Deployment and Control Features	Switch should support on-line software reconfiguration to implement changes without rebooting. Any changes in the configuration of switches related to Layer-2 & 3 functions, VLAN, STP, Security, QoS should not require rebooting of the switch.		

Managed Access Switch

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
MAS.REQ.044	Management, Easy-to-Use Deployment and Control Features	Support for Automatic Quality of Service for easy configuration of QoS features for critical applications.		
MAS.REQ.045	Management, Easy-to-Use Deployment and Control Features	Support for Unidirectional Link Detection Protocol (UDLD) to detect unidirectional links caused by incorrect fiber-optic wiring or port faults and disable on fiber-optic interfaces		
MAS.REQ.046	Management, Easy-to-Use Deployment and Control Features	Switch should have comprehensive debugging features required for software & hardware fault diagnosis.		
MAS.REQ.047	Management, Easy-to-Use Deployment and Control Features	Layer 2/Layer 3 trace route eases troubleshooting or equivalent feature supporting IEEE 802.1 AG, IEEE 802.3 AH identifying the physical path that a packet takes from source to destination.		
MAS.REQ.048	Management, Easy-to-Use Deployment and Control Features	Should support DHCP Server feature to enable a convenient deployment option for the assignment of IP addresses in networks that do		
MAS.REQ.049	Management, Easy-to-Use Deployment and Control Features	not have without a dedicated DHCP server.		
MAS.REQ.050	Management, Easy-to-Use Deployment and Control Features	Switch should support Multiple privilege levels to provide different levels of access.		
MAS.REQ.051	Management, Easy-to-Use Deployment and Control Features	Switch should support NTP (Network Time Protocol)		
MAS.REQ.052	Management, Easy-to-Use Deployment and Control Features	Switch should support FTP/ TFTP		
MAS.REQ.053	Standards	RoHS Compliant.		
MAS.REQ.054	Standards	IEEE 802.1x support.		
MAS.REQ.055	Standards	IEEE 802.3x full duplex on 10BASE-T and 100BASE-TX ports.		
MAS.REQ.056	Standards	IEEE 802.1D Spanning-Tree Protocol.		
MAS.REQ.057	Standards	IEEE 802.1p class-of-service (CoS) prioritization.		
MAS.REQ.058	Standards	IEEE 802.1Q VLAN.		
MAS.REQ.059	Standards	IEEE 802.3u 10 BaseT / 100 Base Tx /1000 Base Tx.		
MAS.REQ.060	Compliance	The switch should be IPV6 complaint		

UPS

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
UPS10.REQ.001	Capacity	10 KVA, 20 KVA and 60 KVA		
UPS10.REQ.002	Technology	True ONLINE (Double Conversion) PWM technology using IGBTs for switching at high frequency (>15 KHz)		
UPS10.REQ.003	Connector	SNMP Connectivity		
UPS10.REQ.004	Electrical Input	Single Phase, 230 V AC with an option to select three phase		
UPS10.REQ.005	Electrical Input	Voltage Range 155 – 280 V on Full Load Voltage Range 110 – 280 V on less than 70% Load		
UPS10.REQ.006	Electrical Input	Frequency Range 45 – 55 Hz		
UPS10.REQ.007	Electrical Input	Efficiency AC to AC: > 85% (AC to AC)		
UPS10.REQ.008	Electrical Output	230V AC		
UPS10.REQ.009	Electrical Output	Frequency: 50 Hz + 0.25Hz (free running); + 2Hz (sync mode)		
UPS10.REQ.010	Electrical Output	Voltage Regulation: +1% on mains/batteries		
UPS10.REQ.011	Electrical Output	Overload Capacity: 125% for 5 min., 110% for 10 mins.		
UPS10.REQ.012	Electrical Output	Waveform; Pure Sine wave		
UPS10.REQ.013	Protection	Electronic Overload Sensing, and circuit breaker protection.		
UPS10.REQ.014	Protection	Over heating, Output short circuit, low battery, input over/under voltage etc.		
UPS10.REQ.015	Battery Type	Sealed Maintenance Free Battery, Mains & Battery with necessary indicators, alarms and protection with proper battery storage stand		
UPS10.REQ.016	Backup Time	Minimum 2 hour backup on rated load		
UPS10.REQ.017	DC Voltage	MIN. : 240 V		
UPS10.REQ.018	Charging Features	Adjusted to about 10% of battery capacity for fast charging. 1. Boost/trickle charging facility 2. Uncontrolled rectifier with high efficiency and reliability. 3. Low battery protection to avoid deep discharging of batteries. 4. Self test diagnostic feature		
UPS10.REQ.019	Other Features	UPS Bypass Automatic on Overload or UPS Failure		
UPS10.REQ.020	Other Features	Monitoring panel with LCD display to provide following information:- 1. Input/output voltage 2. Input/output frequency 3. Load current 4. Charging current LED display for:- UPS on, battery operation, bypass, alarm, battery charge level, etc. Alarms for :- Mains failure, low battery, overload etc.		

UPS

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
UPS10.REQ.021	Other Features	RS 232 Standard Interface port in conjunction with UPS monitoring software provides information about UPS health, status, battery backup,etc.		
UPS10.REQ.022	Environmental	Temperature 0-400C operating, -10 to + 60 deg C		
UPS10.REQ.023	Environmental	Humidity 0 – 95% RH non-condensing		
UPS10.REQ.024	Environmental	Audible noise < 50 dB (A)		
UPS10.REQ.025	Mandatory Compliance	Safety certified to IEC standards or as per applicable in Indian law		
UPS10.REQ.026	Mandatory Compliance	EMC certified to IEC standards.		
UPS10.REQ.027	Mandatory Compliance	ISO 9001:2000 and ISO 14001 certified ETDC/ERTL test reports for above specifications.		
UPS10.REQ.028	Mandatory Compliance	Dimension Light Weight/Smaller Footprint		

Desktop - State Call Center

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
For Agent				
DSK.REQ.001	Processor	Intel Core i7 , 64bit x86 Processor @ 3.2 GHz or more,4MB L3 cache, Memory support DDR3 or better specifications		
DSK.REQ.002	Motherboard & Chipset	OEM Motherboard		
DSK.REQ.003	Video	Integrated Graphic controller		
DSK.REQ.004	Network	Integrated 10/100/1000 Gigabit Ethernet controller		
DSK.REQ.005	Ports	1 HDMI port (Preferable), 2x USB 2.0 and 2 x USB 3.0 (Preferable) , 10 USB ports external - with minimum 4 ports USB 3.0 Front I/O includes (2 or more) USB 2.0 ports Rear I/O includes (2 or more) USB 3.0 ports, (2 or more) USB 2.0 ports, serial port, Parallel port, PS/2 mouse and keyboard ports, RJ-45 network interface, DisplayPort 1 VGA and 3.5mm audio in/out jacks; 4 in 1 Media Card Reader (Preferable)		
DSK.REQ.006	HDD Controller	Integrated dual port SATA-II controller		
DSK.REQ.007	Memory	16GB DDR III 1333MHz or higher expandable up to 8 GB or more		
DSK.REQ.008	Storage	1TB @ HDD 7200 RPM		
DSK.REQ.009	Optical Drive	22X DVD writer or higher and the corresponding software		
DSK.REQ.010	Monitor	21" TFT LCD monitor minimum 1920 x 1080 resolution with 5 ms response time or better specifications, TCO 03 or higher certified **CRM operations per desktop total 1 monitors to be provided**		
DSK.REQ.011	Keyboard	107 or more Keys Keyboard		
DSK.REQ.012	Mouse	2 / 3 button USB Optical Scroll Mouse with anti-static mouse pad resolution of Optical 1000 cpi, Complying to CE and FCC norms		
DSK.REQ.013	Power Management and DMI	System with Power management features & Desktop Management Interface implementation		
DSK.REQ.014	Operating System	U Buntu Linux 14.04.2 LTS Desktop version for x86-64 bit		
DSK.REQ.015	Power input	100 -240V AC		
For Dispatcher				
DSK.REQ.016	Processor	Intel Core i7, 64bit x86 Processor @ 3.2 GHz or more,4MB L3 cache, Memory support DDR3 or better specifications		
DSK.REQ.017	Motherboard & Chipset	OEM Motherboard		
DSK.REQ.018	Video	Integrated Graphic controller		
DSK.REQ.019	Network	Integrated 10/100/1000 Gigabit Ethernet controller		
DSK.REQ.020	Ports	1 HDMI port (Preferable), 2x USB 2.0 and 2 x USB 3.0 (Preferable) , 10 USB ports external - with minimum 4 ports USB 3.0 Front I/O includes (2 or more) USB 2.0 ports Rear I/O includes (2 or more) USB 3.0 ports, (2 or more) USB 2.0 ports, serial port, Parallel port, PS/2 mouse and keyboard ports, RJ-45 network interface, DisplayPort 1 VGA and 3.5mm audio in/out jacks; 4 in 1 Media Card Reader (Preferable)		
DSK.REQ.021	Additional Graphics Card 1	Graphics Card with 1GB memory (non shared) PCIe Graphics Card or equivalent or higher with two display port		
DSK.REQ.022	HDD Controller	Integrated dual port SATA-II controller		
DSK.REQ.023	Memory	16 GB DDR III 1333MHz or higher expandable up to 8 GB or more		
DSK.REQ.024	Storage	1TB @ HDD 7200 RPM		
DSK.REQ.025	Optical Drive	22X DVD writer or higher and the corresponding software		

Desktop - State Call Center

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
DSK.REQ.026	Monitor	21” TFT LCD monitor minimum 1920 x 1080 resolution with 5 ms response time or better specifications, TCO 03 or higher certified **CAD operations per desktop total 3 monitors to be provided**		
DSK.REQ.027	Keyboard	107 or more Keys Keyboard		
DSK.REQ.028	Mouse	2 / 3 button USB Optical Scroll Mouse with anti-static mouse pad resolution of Optical 1000 cpi, Complying to CE and FCC norms		
DSK.REQ.029	Power Management and DMI	System with Power management features & Desktop Management Interface implementation		
DSK.REQ.030	Operating System	U Buntu Linux 14.04.2 LTS Desktop version for x86-64 bit		
DSK.REQ.031	Power input	100 -240V AC		
Desktop - Thin Client For SOC and NOC				
DSK.REQ.032	Graphics	Intel HD Graphics		
DSK.REQ.033	Monitor	21” Or higher “TFT OEM color monitor. TCO Monitor. Same brand as Desktop		
DSK.REQ.034	Keyboard	104 Keys, USB keyboard		
DSK.REQ.035	Mouse	2 button Optical scroll Mouse		
DSK.REQ.036	Operating System	Linux and upgradable		
DSK.REQ.037	Power	320 W or less, 80 PLUS		
DSK.REQ.038	Certifications	UL, ROHS, EPEAT Gold, Energy Star		

IP phones with headset for each agent desk

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
IPP.REQ.001	General Requirement	The IP phones with compatible wireless headset should be supplied by the bidder. Wireless headset should be compatible with soft Phone in desktop also. Wireless headset should have a provision to switch between soft phone and IP Phone.Wireless headset should have echo cancellation.		
IPP.REQ.002	General Requirement	The IP Phone shall have an interactive and user-friendly alphanumeric display to make use of the key phone very simple.		
IPP.REQ.003	General Requirement	The IP Phone shall provide at least 6 programmable keys along with fixed feature buttons for Hold, Redial, Volume Up and Down, Mute, Hands free, Directory, Voice Message. There shall be possible to configure agent Login, Logout and Break keys on the IP Phone/Client Desktop.		
IPP.REQ.004	General Requirement	The IP Phone shall include a two port (100/1000BaseT interface) switch for connecting PC/workstations.		
IPP.REQ.005	General Requirement	The IP Phones shall support connection of Headset.		
IPP.REQ.006	General Requirement	The IP Phone shall have LED/LCD Indicator for Call Waiting and Message Waiting.		
IPP.REQ.007	General Requirement	The IP Phone shall support Dynamic Host Configuration Protocol (DHCP) based as well as statically configured IP address assignment.		
IPP.REQ.008	General Requirement	The IP Phone shall have minimum 2.5"X2.0", high resolution graphical grayscale LCD display.		
IPP.REQ.009	General Requirement	It shall be possible to create Local Phone book with at least 50 contacts as well as pull information from the directory (Integration with directory like Active directory Contact details etc.).		
IPP.REQ.010	General Requirement	The IP phones shall support industry standard audio codec viz. G.711 (A-law and Mu-law), G.729 (including G.729 A and G.729 B), G.722 audio codec.		
IPP.REQ.011	General Requirement	The IP Phone shall support Voice Activity Detection, Silence Suppression and Echo Cancellation.		

IP phones with headset for each agent desk

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
IPP.REQ.012	General Requirement	The display shall provide features such as Date and Time, Calling Party Number and Digits Dialled.		
IPP.REQ.013	General Requirement	IP phones shall be able to work on SIP/H.323 protocols.		
IPP.REQ.014	General Requirement	There shall be provision to provide electrical power to the IP phones either through power adapter or via PoE (IEEE 802.3af) enabled Ethernet port.		
IPP.REQ.015	General Requirement	The IP phones shall support for POE Class 1 or POE Class 2		
IPP.REQ.016	General Requirement	The Phones shall have configurable Abbreviated Dial & Speed Dial.		
IPP.REQ.017	General Requirement	The firmware of IP phones shall be upgradable using HTTPS or FTP or TFTP or SFTP.		
IPP.REQ.018	General Requirement	It shall be possible to view call history for at least last 10 missed calls, 10 dialled calls and 10 received calls for each call taker desk.		
IPP.REQ.019	General Requirement	It shall be possible to set preferences such as Display Contrast and Ring Types.		
IPP.REQ.020	General Requirement	The IP Phones shall be SNMP manageable (SNMP v1, SNMP v2c and/or SNMPv3 protocols) directly or through the PBX server. IP Phones or PBX server shall be able to send IP phone related SNMP traps to the configured Network Management System (NMS). Bidder shall provide generic as well as vendor/OEM specific SNMP MIBs of the equipment for monitoring/management through standard NMS systems along with the equipment.		
IPP.REQ.021	Features	Mobile-Phone style menu with access to most often used features like call forwarding, Park, Settings etc. On screen status indication for activated features like call forwarding		
IPP.REQ.022	Message Waiting Indicator	used as ringing call alert indicator		
IPP.REQ.023	Mounting	Desk or wall mountable with optional wall mount adapter.		

Laser Jet Network Printer (Duplex)				
Sr. No.	**Item**	**Requirement Description**	**Compliance (Yes / No)**	**Deviations / Remarks**
LJN.REQ.001	Print speed, black	30 ppm or more		
LJN.REQ.002	Print resolution, black	1200 x 600 x 2 dpi or more		
LJN.REQ.003	Print technology	Laser		
LJN.REQ.004	Monthly duty cycle	8000 pages or more		
LJN.REQ.005	Memory, standard	32 MB or higher		
LJN.REQ.006	Print languages, standard	Host-based printing, PCL 5e		
LJN.REQ.007	Duplex printing (printing on both sides of paper)	Automatic (standard)		
LJN.REQ.008	Media sizes, standard	A4 , letter		
LJN.REQ.009	Media sizes, custom	250-sheet input tray: 5.8 x 8.27 to 8.5 x 14 in; priority feed slot: 3 x 5 to 8.5 x 14 in preferable		
LJN.REQ.010	Network ready	Standard (built-in Ethernet)		
LJN.REQ.011	ENERGY STAR® Qualified	Yes		

Mobile Data Terminal (MDT) Device				
Sr. No.	**Item**	**Minimum Requirement Description**	**Compliance (Yes / No)**	**Deviations / Remarks**
Rugged Devices				
For 4 Wheeler				
MDT.REQ.001	Processor	at least Dual core, 1 GHz		
MDT.REQ.002	Memory	RAM at least 2 GB or better		
MDT.REQ.003	Storage	At least 16 GB or higher		
MDT.REQ.004	Operating System	Android v 4.1 and above		
MDT.REQ.005	Generation	2G and 3G support		
MDT.REQ.006	GSM	Yes		
MDT.REQ.007	Screen size	minimum 8" with Multi touch support i.e. Multiple finger touch parallel		
MDT.REQ.008	Voice	Voice recording should be possible, built-in microphone, built-in Speaker		
MDT.REQ.009	Camera & Video	at least 2MP Front & 5 MP rear with LED Flash (integrated)		
MDT.REQ.010	Feature	Should work as AVLS device for AVLS/CAD application, Supports Turn by Turn Navigation and install auto updates for CAD, GIS and other relevant application		
MDT.REQ.011	Screen luminosity	Min. 500 nits, Daylight readable		
MDT.REQ.012	Ruggedness	IP 55 certified (water and dust protected)		
MDT.REQ.013	Speakerphone	Hands free Support		
MDT.REQ.014	Keyboard	Virtual on Screen		
MDT.REQ.015	Integration Support	Should be able to integrate with CAD,GIS and other application like MDT security etc.		
MDT.REQ.016	GPS	Yes and support for GLONASS		
MDT.REQ.017	Audio Playing Format	MP3,wav files format etc.		
MDT.REQ.018	Enviornment Specification	5°C to 50°C, Humidity 95% RH,Non Condensing		
MDT.REQ.019	Ports	Micro USB * 1 version 2.0 and above and same for charging and OTG,Headset port etc.		
MDT.REQ.020	Expansion Slots	Integrated		
MDT.REQ.021	Power Supply	230V, 50 Hz AC Supply		
MDT.REQ.022	Bluetooth	Yes		
MDT.REQ.023	Adapter	AC Input:100-240V;DC Output:5V/2A		
MDT.REQ.024	Battery	minimum 4000 mAh and above		
MDT.REQ.025	Charger	Suitable charger shall be supplied, Built-in rechargeable battery pack/battery.Electric Charger,USB Charger, Convertor required in case of no USB port in vehicle, Headset Port etc.		
MDT.REQ.026	Tablet Case	Rugged case		
MDT.REQ.027	Mounting	On Vehicle Dashboard		
MDT.REQ.028	Tablet case	Rugged Case		
MDT.REQ.029	Wireless	Yes		
MDT.REQ.030	IPv6 Compliant	Yes		
MDT.REQ.031	Security Features	Password Security		
Non Rugged Devices				
For 4 Wheeler				
MDT.REQ.032	Processor	at least Dual core, 1 GHz		
MDT.REQ.033	Memory	RAM at least 2 GB or better		
MDT.REQ.034	Storage	At least 16 GB or higher		
MDT.REQ.035	Operating System	Android v 4.1 and above		
MDT.REQ.036	Generation	2G and 3G support		

Mobile Data Terminal (MDT) Device				
Sr. No.	**Item**	**Minimum Requirement Description**	**Compliance (Yes / No)**	**Deviations / Remarks**
MDT.REQ.037	GSM	Yes		
MDT.REQ.038	Screen size	minimum 8" with Multi touch support i.e. Multiple finger touch parallel		
MDT.REQ.039	Feature	Should work as AVLS device for AVLS/CAD application, Supports Turn by Turn Navigation and install auto updates for CAD, GIS and other relevant application		
MDT.REQ.040	Screen luminosity	500 nits, Daylight readable		
MDT.REQ.041	Voice	Voice recording should be possible, built-in microphone, built-in Speaker		
MDT.REQ.042	Camera & Video	at least 2MP Front & 5 MP rear with LED Flash (integrated)		
MDT.REQ.043	Speakerphone	Hands free Support		
MDT.REQ.044	Keyboard	Virtual on Screen		
MDT.REQ.045	Integration Support	Should be able to integrate with CAD,GIS and other application like MDT security etc.		
MDT.REQ.046	GPS	Yes and support for GLONASS		
MDT.REQ.047	Audio Playing Format	MP3,wav files format etc.		
MDT.REQ.048	Enviornment Specification	5°C to 50°C, Humidity 95% RH,Non Condensing		
MDT.REQ.049	Ports	Micro USB * 1 same for charging and OTG,Headset port etc.		
MDT.REQ.050	Expansion Slots	Integrated		
MDT.REQ.051	Bluetooth	Yes		
MDT.REQ.052	Power Supply	230V, 50 Hz AC Supply		
MDT.REQ.053	Adapter	AC Input:100-240V;DC Output:5V/2A		
MDT.REQ.054	Battery	minimum 4000 mAh and above		
MDT.REQ.055	Charger	Suitable charger shall be supplied, Built-in rechargeable battery pack/battery.Electric Charger,USB Charger, Convertor required in case of no USB port in vehicle, Headset Port etc.		
MDT.REQ.056	Tablet Case	Rugged case		
MDT.REQ.057	Mounting	On Vehicle Dashboard		
MDT.REQ.058	Wireless	Yes		
MDT.REQ.059	IPv6 Compliant	Yes		
MDT.REQ.060	Security Features	Password Security		
For 2 Wheeler				
MDT.REQ.061	Processor	at least Dual core, 1 GHz		
MDT.REQ.062	Memory	RAM at least 2 GB or better		
MDT.REQ.063	Storage	At least 16 GB or higher		
MDT.REQ.064	Operating System	Android v 4.1 and above		
MDT.REQ.065	Generation	2G and 3G support		
MDT.REQ.066	GSM	Yes		
MDT.REQ.067	Screen size	minimum 5.5" with Multi touch support i.e. Multiple finger touch parallel		
MDT.REQ.068	Size/ Dimensions	Handheld		
MDT.REQ.069	Feature	Should work as AVLS device for AVLS/CAD application, Supports Turn by Turn Navigation and install auto updates for CAD, GIS and other relevant application		
MDT.REQ.070	Voice	Voice recording should be possible, built-in microphone, built-in Speaker		
MDT.REQ.071	Camera & Video	at least 2MP Front & 5 MP rear with LED Flash (integrated)		
MDT.REQ.072	Screen luminosity	500 nits, Daylight readable		
MDT.REQ.073	Speakerphone	Hands free Support		

Mobile Data Terminal (MDT) Device

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
MDT.REQ.074	Keyboard	Virtual on screen		
MDT.REQ.075	Integration Support	Should be able to integrate with CAD,GIS and other application like MDT security etc.		
MDT.REQ.076	GPS	Yes and support for GLONASS		
MDT.REQ.077	Audio Playing Format	MP3,wav files format etc.		
MDT.REQ.078	Enviornment Specification	5°C to 50°C, Humidity 95% RH,Non Condensing		
MDT.REQ.079	Ports	Micro USB * 1 same for charging and OTG,Headset port etc.		
MDT.REQ.080	Expansion Slots	Integrated		
MDT.REQ.081	Bluetooth	Yes		
MDT.REQ.082	Adapter	AC Input:100-240V;DC Output:5V/2A		
MDT.REQ.083	Power Supply	230V, 50 Hz AC Supply		
MDT.REQ.084	Battery	minimum 4000 mAh and above		
MDT.REQ.085	Charger	Suitable charger shall be supplied, Built-in rechargeable battery pack/battery and USB cable		
MDT.REQ.086	Tablet case	Rugged Case		
MDT.REQ.087	Carrying Pouch	Yes		
MDT.REQ.088	Mounting	Should be able to be fixed on the bike with facility to charge		
MDT.REQ.089	Wireless	Yes		
MDT.REQ.090	IPv6 Compliant	Yes		
MDT.REQ.091	Security Features	Password Security		
Mobile Data Terminal Device Security and Monitoring Features for 2 Wheelers and 4 wheelers devices				
MDT.REQ.092	Password Security	Mobile Device should be password protected. Password of the MDT device should be reset by the Monitoring Center IT helpdesk		
MDT.REQ.093	Security	Should have multi level security for MDT devices remotely accessing the application. E.g. strong passwords, access to only predefined IPs / MAC numbers, etc.		
MDT.REQ.094	General Requirement	Should have ability to detect jail-broken, and rooted devices		
MDT.REQ.095	Mobile Device Monitoring	Should have a capability to provide the device health check report like CPU usage , Memory usage, storage usage etc. and should be integrated with Enterprise Management system (EMS) solution		
MDT.REQ.096	Mobile Device Monitoring	Should provide the access User Status and Statistics / ability to review mobile user and mobile environment activity, such as: # of sent/received items, last connection time, etc.		
MDT.REQ.097	Mobile Device Monitoring	Should support the ability to disable access to public App Stores based on a policy configuration		
MDT.REQ.098	Mobile Device Monitoring	Should have configuration Policies to allow individual components of the mobile device to be enabled or disabled.		
MDT.REQ.099	Login/logout Support	Should support login/logout support and provide a secured access through unique user name and password.		
MDT Certification				
MDT.REQ.100	Certification	MDTs should be certified by Bureau of Indian Standards (BIS) , PMA for rugged and non rugged devices.		
MDT.REQ.101	Charger Certification	Travel Charger should comply with: IEC 60950, IS13252:2010.UL Certified, ROHS		

LED TV for Conference Room

Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
LCD.REQ.001	Screen Type	LED		
LCD.REQ.002	LED Panel Viewable Area	Minimum 65"		
LCD.REQ.003	HD Technology & Screen	Full HD, 1920 x 1080		
LCD.REQ.004	Front Control	Power On/Off with LED		
LCD.REQ.005	USB	2 (Minimum)		
LCD.REQ.006	HDMI	3 (Minimum)		
LCD.REQ.007	WiFi	Built In		
LCD.REQ.008	Backlight Module	LED		
LCD.REQ.009	Scan System	Automatic NTSC/PAL; 31.5 ~ 80 KHz (Horizontal) ; 56 ~ 75 Hz (Vertical)		
LCD.REQ.010	Video Connectors	BNC (Composite Video) – 2 channels (looping); 4-Pin Mini DIN (Y/C Video) DVI-I, 15-pin D-Sub for VGA/SXGA Audio Inputs PC Audio (mini jack) Video Audio (2 channels RCA - looping), HDMI 4 (Rear),		
LCD.REQ.011	Power Input	AC Input – 100 to 240V ~ 0.5A, 50/60Hz		
LCD.REQ.012	Power Cord	Detacheable		
LCD.REQ.013	Display Mode	DVI-I/SXGA/XGA/VGA		
LCD.REQ.014	Display Colours	16.7 Million		
LCD.REQ.015	Viewing Angle	140º horizontal, 160º vertical		
LCD.REQ.016	Operating Temperature	41° to 104° F (5° to 40° C)		
LCD.REQ.017	Operating Humidity	30% to 80% relative, non-condensing		
LCD.REQ.018	Emmission	FCC: Part 15, Class B		
LCD.REQ.019	Hardware	Suitable mounting fixture/ stand to be provided		
LCD.REQ.020	Support	The system should not be an end of life / end of service product.		

Cloud Hosting Specification

Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
CHS.REQ.001	Infrastructure as a Service (IAAS)	• Provide scalable, redundant, dynamic computing and storage capabilities or virtual machines. • Purchaser can procure cloud services via the Internet or via VPN		
CHS.REQ.002	Hosting Services	• Purchaser can securely load applications and data onto the provider's service remotely from VPN or secure connection. • Configuration is enabled via a web browser over the VPN or secured connection		
Scalability & Provisioning				
CHS.REQ.003	On demand self service	Automatic Provisioning & Deprovisioning of virtual machines.		
CHS.REQ.004	Elasticity	Manual Provisioning & Deprovisioning of virtual machines.		
Security				
CHS.REQ.005	Infrastructure Security Incident Monitoring	Design, implementation, configuration, modification, and management of infrastructure and software are consistent with defined system security policies to enable authorized access and to prevent unauthorized access.		
CHS.REQ.006	Infrastructure & Application Security Incident Remediation	Design, implementation, configuration, modification, and management of infrastructure and software are consistent with defined processing integrity and related security policies.		
CHS.REQ.007	Data Integrity & Data Protection	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.		
CHS.REQ.008	Identity & Access Management Credential Lifecycle / Provision Management	User access policies and procedures shall be established in consultation with purchaser and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management.		
CHS.REQ.009	Infrastructure & Virtualization Security VMM Security - Hypervisor Hardening	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering,		
CHS.REQ.010	Security Incident Management & Cloud Forensics	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.		

CHS.REQ.011	Threat and Vulnerability Management Anti-Virus / Malicious Software	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.		
Audit				
CHS.REQ.012	Audit Assurance & Compliance Audit Planning	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits. System security is periodically reviewed and compared with the defined system security policies. Process to identify and address potential impairments to the entity's ongoing ability to achieve its objectives in accordance with its defined system security policies.		
CHS.REQ.013	Audit Assurance & Compliance	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations. System security is periodically reviewed and compared with the defined system security policies. Process to identify and address potential impairments & ongoing ability to achieve its objectives in accordance with its defined system security policies.		
Interoperatibility				
CHS.REQ.014	Interoperability & Portability	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.		
Back Up & Recovery				
CHS.REQ.015	Back up & Recovery	A. Back Up process of copying computer data from a registered server to a Backup Vault. B. "Backup Agent" software installed on a registered server to enable the registered server to Back Up or Restore one or more Protected Items. C. Register one or more Items for Backup. D. Collection of data, such as a volume, database, or virtual machine that has been scheduled for Backup to the Backup Service. E."Recovery" or "Restore" of restoring computer data from a Backup Vault to a registered server.		
Log Retention				
CHS.REQ.016	Log Retention	Log Collection facility should be available		
Reporting Requirements				
CHS.REQ.017		Daily Weekly Monthly Yearly Report		
Data Retention Time				
CHS.REQ.018		Data should be retained as per defined policy		
Other requirements				
CHS.REQ.019	General Requirement	Bandwith should be dedicated between data centers		
CHS.REQ.020	General Requirement	DCs should be connected on fiber		
CHS.REQ.021	General Requirement	Cloud services should have dedicated SOC and NOC services with 24*7 operations		
CHS.REQ.022	General Requirement	Deployment Should support vendor supplied software with out modification or additional scripting		

CHS.REQ.023	General Requirement	it should allow batch jobs to scheduled for execution at later stage		
CHS.REQ.024	General Requirement	No unauthorize to access the data		
CHS.REQ.025	General Requirement	each vCPU should have a speed of minimum 1Ghz and above		

Video Wall (For NOC & SOC)

Sr. No.	Nature of Requirement	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
VWCCC.REQ.001	Display Wall	The large display wall shall be consisting of multiple rear projection modules in(2) rows and (3)columns configuration and behaving as a single logical screen.		
VWCCC.REQ.002	Projection Technology	Display Unit/Rear Projection Module must be based on Single Chip DLP-based Rear Projection Technology 3 separate colour (Red, Green & Blue) LED lit, without any colour wheel.		
VWCCC.REQ.003	Architecture	The display unit/rear projection modules shall have in-built illumination system		
VWCCC.REQ.004	Display size	The diagonal size of each visual display unit/rear projection module shall be 60".		
VWCCC.REQ.005	Native Resolution per cube	1920 X 1080 pixels (Full HD)		
VWCCC.REQ.006	Aspect Ratio	16:9 for each projection module		
VWCCC.REQ.007	Lamp Type	LED - RGB (1 each of 12 sqmm surface area). Multiple LED's of each colour to achieve 12 sqmm area is not acceptable		
VWCCC.REQ.008	Display redundancy	In case of failure of any 1 or 2 LED lamp, it should be possible to display the Image with available 1 or 2 to continue the display and automatically switch the original display colour into other available colours.		
VWCCC.REQ.009	Cooling Mechanism	Cooling by means of heat pipe		
VWCCC.REQ.010	Brightness	should be minimum 500 lumens		
VWCCC.REQ.011	Brightness Uniformity	≥ 95%		
VWCCC.REQ.012	Contrast ratio	≥1500:1		
VWCCC.REQ.013	Dynamic contrast ratio	>600,000:1		
VWCCC.REQ.014	Luminance	The screen should have adjustable low inter screen gap <1mm to give seamless viewing experience.		
VWCCC.REQ.015	Color gamut	125% of NTSC / 165%of EBU		
VWCCC.REQ.016	Color	shall offer in excess of 16.7 million colors.		
VWCCC.REQ.017	Screen	Burn free, shall have Glass Backing to prevent deformation		

VWCCC.REQ.018	Viewing Angle	full viewing angle should be 180 degrees		
VWCCC.REQ.019	Half Gain Angle	Horizontal : ±35 degrees		
VWCCC.REQ.020		Vertical: ±27 degrees		
VWCCC.REQ.021	Internal Splitter	Inbuilt internal splitter which can provide a complete computer or Video image with loop in loop out		
VWCCC.REQ.022	Pedestals	Should be customized as per project requirements		
VWCCC.REQ.023	RGB, DVI - D timing compatibility	720x400/70Hz, 85HZ VGA/60Hz, 72Hz, 75Hz, 85Hz SVGA/60Hz, 70Hz, 75Hz, 85Hz XGA/60Hz, 70Hz, 75Hz, 85Hz WXGA(1280x768)/60 Hz SXGA+/60 Hz,70 Hz,75Hz WUXGA+/60 Hz UXGA/60 Hz,65Hz,75Hz QXGA/60Hz(reduced blanking)		
VWCCC.REQ.024	Auto detection	System shall automatically search the source which has input signal after signal plug- in.		
VWCCC.REQ.025	Source Redundancy	System should able to switch to secondary DVI input if primary DVI input not available.		
		System should also automatically switch back to primary DVI from secondary DVI input as soon as primary DVI input is available again.		
VWCCC.REQ.026	Video feature	10 bit motion adaptive interlacing for HD and SD		
		Detail enhancement (H, V peaking).		
		Adaptive detail enhancement featuring sharpness and texture enhancement (STE)		
		Enhanced noise reduction with Mosquito noise reduction (MNR)and Block Artifact Reduction(BAR)		
VWCCC.REQ.027	Component Life-LED	>80,000 Hours		
VWCCC.REQ.028	LED Control	Dynamic control		
VWCCC.REQ.029	Startup	Instant hot restart		
VWCCC.REQ.030	Operating Temperature	system shall be operate properly under 5ºC to 50ºC Temperature		
VWCCC.REQ.031	Storage Temperature	-10°C to +60°C		

VWCCC.REQ.032	Operating Relative Humidity	10% to 90%		
Video Wall Controller				
VWC.REQ.001	Display Controller	Controller to control Display module in a matrix of (3) x (2) with outputs , video inputs and Universal inputs along with necessary softwares		
VWC.REQ.002	Processor	Single or Dual Quad Core Intel® Xeon 64-bit 2.0 GHz CPU		
VWC.REQ.003	RAM Capacity	Min 8GB and Should be upgradable up to 192 GB 1333 DDR3 ECC Registered memory		
VWC.REQ.004	Expansion Slots	7 slots PCI-E 2.0		
VWC.REQ.005	HDD	Min 500 GB Hard Disk		
		Minimum Support up to 4 Hard disk should be available		
		Hard disk Capacity should be upgradable		
VWC.REQ.006	RAID	RAID 0, 1, 5, 10 support (Windows)		
VWC.REQ.007	Networking	Dual-port Gigabit Ethernet Controller inbuilt		
		Support for Add on Network adapters		
		Support for Optical Fiber interface Adapters		
VWC.REQ.008	Input/ Output supported	Serial ATA * Six Serial ATA ports * Six SATA hard drives supported		
		IDE * Single EIDE channel supports up to two UDMA IDE devices (IDE-M, IDE-S) including CF(Compact Flash) Card		
		IDE-S) including CF(Compact Flash) Card * Supports UDMA Mode 5, PIO Mode 4, and ATA/100		
		LAN * 2x RJ45 LAN ports * 1x RJ45 Dedicated IPMI LAN port		
		USB * 6x USB rear ports * 1x USB on-board * 2x USB internal headers (3 ports) * Total 10 USB 2.0 Compliant		

		VGA * 1x VGA Port Keyboard / Mouse * PS/2 keyboard and mouse ports Serial Port / Header Serial Port / Header * 1 Fast UART 16550 serial port * 1 Fast UART 16550 serial header (Option)		
		IEEE 1394a * 2x IEEE 1394a ports (1x header)		
VWC.REQ.009	Power Configurations	* ACPI Power Management		
		* Main Switch Override Mechanism		
		* Wake-On-Ring (WOR) header		
		* Wake-On-LAN (WOL) header		
		* Power-on mode for AC power recovery		
		* Internal / External modem remote ring-on		
Video Wall Management Software				
VWS.REQ.001	Client & Server based Architecture	Should supports Multi client/Console control the Wall layouts		
VWS.REQ.002	Scaling and display	Software enable user to display, multiple sources up to any size and anywhere on the display wall.		
VWS.REQ.003	Controls	Software should support to control the Brightness, Contrast, Saturation, Hue, filtering, Crop and Rotate function as per user requirement		
VWS.REQ.004	RS232, TCP/IP	RS232 & TCP/IP support should be available for other interfaces		
VWS.REQ.005	Remote Control	Wall can be control from Remote PC through LAN		
VWS.REQ.006	Auto Source Detection	Software should support for auto source detection		
VWS.REQ.007	Layout Management	Should support for Video, RGB, DVI, ,Internet Explorer, Desktop Application and Remote Desktop Monitoring Layouts		
VWS.REQ.008	Scenarios	Software should able to Save and Load desktop layouts from Local or remote machines		
VWS.REQ.009	Layout Scheduler	All the Layouts can be scheduled as per user convince.		
		Software should support auto launch of Layouts according to specified time event by user		
VWS.REQ.010	Protocol	VNC		

VWS.REQ.011	Interface	LAN		
VWS.REQ.012	Resolution	At least 4k x 2k		
VWS.REQ.013	Scaling and display	Display of multiple sources up to any size, everywhere on the wall		
VWS.REQ.014	Console View	Software enable user to select following view		
		Primary Display		
		Secondary Display		
		Full Desktop		
		Selected region		
		Selected application		