CRIME & CRIMINAL TRACKING NETWORK AND SYSTEMS (CCTNS)

Tender Reference

ELCOT/PROC/OT/33384/CCTNS 2.0 (SCRB)/ 2020-21

Request for Proposal

For

Selection of System Integrator for Supply, Design, Development, Implementation and Maintenance of CCTNS 2.0

Volume I

Tender Document

Table of Contents

1. Glossary and List of Abbreviations

ADGP	Additional Director General of Police
AMC	Annual Maintenance Contract
API	Application Programming Interface
BG	Bank Guarantee
BOM	Bill of Material
CAPEX	Capital Expenditure
CCTNS	Crime & Criminal Tracking Network and System
DC	Data Center
DMT	District Mission Team

DRC	Disaster Recovery Center
ELCOT	Electronics Corporation of Tamilnadu
EMD	Earnest Money Deposit
GOI	Government of India
HIPS	Host Intrusion Prevention System
HQ	Head Quarter
IO	Investigation Officer
IT	Information Technology
MFP	Multi-Functional Printer
MHA	Ministry of Home Affairs
OEM	Original Equipment Manufacturer
OPEX	Operational Expenditure
PBG	Performance Bank Guarantee
PS	Police Station
RFC	Request for Clarification
RFP	Request for Proposal
SAN	Storage Area Network
SCRB	State Crime record Bureau
SDC	State Data Center
SI	System Integrator
SLA	Service Level Agreement
SMT	State Mission Team
SPOC	Single Point of Contact
TIA	Tender Inviting Authority
TNSDC	Tamil Nadu State Data Centre
UTR	Unique Transaction Reference

2. Request for Proposal - Process

2.1 Preamble

Electronics Corporation of Tamil Nadu Limited (ELCOT), a wholly owned Government of Tamil Nadu Undertaking is the Optional Procurement Agency of the Government of Tamil Nadu for procurement of IT/ ITES related products like Computers, Printers, other peripherals and software as per G.O.Ms.No.58 of Finance (BPE) Department dated 16.2.1999 with latest amendments. ELCOT is procuring various IT/ ITES related products and services for all the State Government Departments / Boards / Autonomous Bodies, etc. As part of the procurement activities, ELCOT inviting bids for Selection of System Integrator for Supply, Design, Development, Implementation and Maintenance of CCTNS 2.0 on behalf of SCRB. ELCOT has undertaken the role of State Project Management Consultant (SPMC) for Bid Process Management for Selection of System Integrator for the implementation of CCTNS 2.0 and the post tendering processes shall be executed by SCRB.

2.2 Tender/RFP Schedule

1	Tender Inviting Authority, Designation and Address	The Managing Director, ELCOT,II Floor, MHU Complex, 692, Anna Salai, Nandanam, Chennai-600035. www.elcot.in, md@elcot.in
2	Tender Accepting Authority	Board of Directors of ELCOT
2	Name of the Work	Supply, Design, Development, Implementation and Maintenance of CCTNS 2.0 for SCRB
3	Tender/RFP Reference	ELCOT/PROC/OT/33384/CCTNS 2.0 (SCRB)/ 2020-21
4	Downloading of Tender/RFP Documents	Tender documents can be downloaded from **https://tntenders.gov.in**, **www.elcot.in** and **www.tenders.tn.gov.in** till closing date and time of the Tender.

5	Tender Fee	Tender Fee of Rs.10,000/- (Rupees Ten Thousand only) should be paid electronically through their respective internet banking enabled account via NEFT / RTGS to the account of ELCOT: **Account Number: 6681528770** **Indian Bank, Nandanam Branch, Chennai – 600 035.** **IFSC Code: IDIB000N078.**
6	Earnest Money Deposit (EMD)	Rs. 1,00,00,000/- (Rupees One Crore Only) should be paid electronically through their respective internet banking enabled account via NEFT / RTGS to the account of ELCOT: **Account Number: 6681528770** **Indian Bank, Nandanam Branch, Chennai– 600 035.** **IFSC Code: IDIB000N078.**
7.	Tender/RFP Submission	Two part Tender/RFP comprising of Technical Proposal and Commercial Proposal should be submitted electronically through e-tender portal **https://tntenders.gov.in**
8.	Bid/Proposal Signing	Bidders should possess valid Class 3-Signing and Encryption Digital Signature Certificates for signing the bids/Proposals.
9	Pre-Bid meeting Date & Location	09.02.2021 @ 11:00 AM. ELCOT,II Floor, MHU Complex, 692, Anna Salai, Nandanam, Chennai-600035.
10	Due Date, Time and place of submission of Tender/RFP	02.03.2021 @ 3:00 PM through the portal mentioned in Row (7) above
11	Date, Time and place of Opening of Technical Proposals	02.03.2021 @ 4:00 PM through the portal mentioned in Row (7) above Opening of the bids/Proposals will be at ELCOT, Nandanam, Chennai-600035.
12	Date, Time and Place of opening of Commercial Proposals	Will be intimated to the Technically Qualified bidders only.

2.3 General Instructions

1. This RFP process is governed by the Tamil Nadu Transparency in Tenders Act 1998 and The Tamil Nadu Transparency in Tenders Rules, 2000 as amended from time to time.

2. The Bidders are requested to examine the instructions, terms and conditions and specifications given in the Tender. Failure to furnish all required information in every aspect will be at the Bidder's risk and may result in the rejection of bid.

3. It will be imperative for each Bidder(s) to familiarize itself with the prevailing legal situations for the execution of contract. ELCOT shall not entertain any request for clarification from the Bidder regarding such legal aspects of submission of the Bids.

4. The Proposal and all related correspondence including the documents shall be written in English only.

5. ELCOT shall respond to the accepted queries and the same will be released as corrigendum to the RFP. This corrigendum would be released on the Tamil Nadu Tenders Portal (www.tntenders.gov.in) or (www.elcot.in).

2.4 Structure of the RFP

Electronics Corporation of Tamil Nadu (hereafter referred as "ELCOT") invites the eligible parties (hereafter referred as "Bidder") for appointment as System Integrator to Supply, Install, Commission and Maintenance of Hardware Items and Design, Develop, Implement and Maintain the "CCTNS 2.0 Software" by providing a comprehensive solution as specified in the RFP.

This Request for Proposal (RFP) document comprises of the following volumes:

1. **Volume I:** Instructions on the Bid process for the purpose of responding to this RFP. This broadly covers:
    a. General instructions for bidding process.
    b. Bid process management details.

c. Bid evaluation process including the parameters for Pre-qualification evaluation, Technical evaluation and Commercial evaluation to facilitate SCRB in determining bidder's suitability as the System Integrator.
d. Bid submission formats.
e. Proposed BoM, Pricing Bid Format & Minimum Technical specification.

2. **Volume II:** Functional and Technical Requirements of the project. The contents of the document broadly cover the following areas:
   a. About the project and its objectives.
   b. Scope of Work.
   c. Minimum Functional and Technical requirements.
   d. Implementation & Payment Schedule.

3. **Volume III:**
   a. Master Service Agreement (MSA) template outlining the contractual, legal terms & conditions applicable for the proposed Project.
   b. Service Level Agreement (SLA).
   c. Non-Disclosure Agreement (NDA).
   d. Change Control Note.

2.5 Instruction to Bidders

i. The Bidders are expected to examine all instructions, forms, terms, Project requirements and other information in the RFP document. Submission of a proposal in response to this notice shall be deemed to have been done after careful study and examination of this document with full understanding of its terms, conditions and implications. Failure to furnish all information required as mentioned in the RFP document or submission of a Proposal not substantially responsive to the RFP document in every aspect will be at the Bidder's risk and may result in rejection of the Proposal and forfeiture of the EMD.

ii. Bidders are requested to comply with the below instructions without fail

1. Any bidder from a country which shares a land border with India will be eligible to bid in this tender only if the bidder is registered with the Competent Authority. The Competent Authority for the purpose of registration under this tender shall be

   a) The Registration Committee constituted by the Department for Promotion of Industry and Internal Trade (DPIIT). OR

   b) The Registration Committee constituted by Government of Tamil Nadu consisting of the following members: -
      1) Managing Director & Chief Executive Officer, Guidance (as Chairman)
      2) Additional Chief Secretary to Government (Finance), or his representative
      3) Additional Chief Secretary to Government (Information Technology) or his representative
      4) Principal Secretary to Government (Public Works Department) or his representative
      5) Industries Commissioner and Director of Industries and Commerce.

Definitions:

1. "Bidder" for the purpose of the tender(including the term 'tenderer', 'consultant', 'vendor' or 'service provider' in certain contexts) means any persons or firm or company, including any member of a consortium or joint venture (that is an association of several persons, or firms or companies), every artificial juridical person not falling in any of the descriptions of bidders stated hereinbefore, including any agency branch or office controlled by such person, participating in a procurement process.

2. Bidder from a country which shares a land border with India" for the purpose of this tender means-
   a. An entity incorporated, established or registered in such a country; or
   b. A subsidiary of an entity incorporated, established or registered in such a country; or
   c. An entity substantially controlled through entities incorporated, established or registered in such a country; or

d. An entity whose beneficial owner is situated in such a country; or
e. An Indian (or other) agent of such an entity; or
f. A natural person who is a citizen of such a country; or
g. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above.

However, there are no restrictions in case of procurement of goods or services from the bidder from those Countries (even if sharing a land border with India) to which the Government of India has extended lines of credit or in which the Government of India is engaged in development Projects.

3. The "Beneficial owner "for the purpose of (ii) above will be as under:

i. In case of a company or Limited Liability Partnership, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person(s), has a controlling ownership interest or who exercises control through other means.

Explanation –

1. "Controlling ownership interest" means ownership of, or entitlement to, more than twenty-five percent of shares or capital or profits of the company;

2. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions, including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

ii. In case of a partnership firm, the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership of entitlement to more than fifteen percent of capital or profits of the partnership;

iii. In case of an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals;

iv. Where no natural person is identified under (i) or (ii) or (iii) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

v. In case of a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

vi. An 'agent' for the purpose of this tender is a person employed to do any act for another, or to represent another in dealings with third person.

vii. The successful bidder shall not be allowed to sub-contract works to any contractor from a country which shares a land border with India unless such contractor is registered with the Competent Authority. The definition of a 'Contractor' from a Country which shares a land border with India' shall be as detailed in paragraph (2) above.

Each Bidder shall have to submit the Undertaking as per Annexure 7

Where applicable, the bidder shall have to submit the Certificate of Registration from the Competent Authority.

2.6 Pre – Qualification Criteria

SNo.	Qualification Criteria Type	Pre-Qualification Criteria	Documentary Proof to be submitted
PQ-1	**Legal Entity**	The Bidder should be a Company registered under Companies Act, 1956 or 2013, and existing from past 10 years as on 31.3.2020	Copy of Certificate of Incorporation and Fresh Certificate of Incorporation in case of Name Change
PQ-2	**Tax Registration**	The Bidder should be Registered Entity in India and should be Registered with the Tax Authorities	1. Copy of PAN 2. Copy of GST Registration Certificate
PQ-3	**Power of Attorney**	Power of Attorney (POA) to sign, submit the bid, Execute the Contract Agreement (if selected)	Copy of Power of Attorney (PoA) by Authorized Signatory of Bidder authorizing a staff of Bidder to sign and submit the bid, execute the Contract Agreement (if selected) on behalf of the Bidder.

SNo.	Qualification Criteria Type	Pre-Qualification Criteria	Documentary Proof to be submitted
PQ-4	**Blacklisting**	The Bidder must not be under a declaration of in-eligibility for corrupt, fraudulent or any other unethical business practices and should not be debarred or blacklisted by State/ Central Government/ Public Sector Undertaking/ Statutory Boards/ Local Bodies of any State for any reason in the last 3 years from the date of the response to this Tender.	A self-certified letter signed by the Authorized Signatory of the Bidder which is included in the Letter of Undertaking
PQ-5	**Sales Turnover**	The Bidder should have a minimum average annual turnover of INR 200 Crores over the last 3 audited financial years (FY 2019-20, 2018-19, 2017-18) as on 31/03/2020 from IT / ITES such as (Software application development / System Integration/ Supply of hardware and Support / Operations and maintenance services for IT infrastructure)	Certificate from the statutory auditor of the Bidder on IT / ITES turnover for the last 3 audited financial years (FY 2019-20, FY 2018-19, FY 2017-18)
PQ-6	**Net worth**	**6.1** The Bidder should have positive net worth and should be a profit-making company for each of the last three audited financial years	Certificate from the statutory auditor of Bidder ascertaining Total Net Worth and Profit after Tax for the last 3 audited financial years (FY 2019-20,

SNo.	Qualification Criteria Type	Pre-Qualification Criteria	Documentary Proof to be submitted
		(FY 2019-20, FY 2018-19, FY 2017-18) **6.2.** The Bidder should have positive net worth of at least INR 25 crores for the last audited FY 2019-20	FY 2018-19, FY 2017-18).
PQ-7	**Technical Competency - IT Infrastructure Services & System Integration**	The Bidder should have delivered "Supply, Installation and Commissioning of Hardware Items (Desktop, Printers and Servers) and "Application Development" scope along with at least 3 of the following services through a single/ multiple (Not more than 3) contract in India for any State / Central Government / Quasi Government / PSU Clients with a minimum value of INR 75 Crore during the last 10 years (as on 31st March 2020). The Bidder should have also successfully completed at least 3 years of Operation and Maintenance phase post the successful completion of the Implementation phase for the same project 1. Application Development Support and	Copy of the Work order/ Contract confirming year and date (Dated on or after 1st April 2010) for the System Integration services as specified along with the Completion certificate* for the successful completion of the project. The supporting documents shall clearly indicate the scope of work as required in the criteria. *UAT Signoff / Completion/ Performance certificate issued by the client alone will be accepted. In case the project is in Operation and Maintenance phase, the bidder can submit certificate issued by the client mentioning that at least 3 years of Operation and Maintenance has been successfully completed.

SNo.	Qualification Criteria Type	Pre-Qualification Criteria	Documentary Proof to be submitted
		Maintenance 2. Operation & Maintenance of Hardware Items 3. Help Desk Services 4. Training & Capacity building	
PQ-8	**OEM Authorization**	The Bidder should have obtained direct authorization from Original Equipment Manufacturer (OEM) for supply, installation, commission of Desktop, Printers, UPS, Inverters, External Hard Drive, Servers and Network Switch	Manufacturer's Authorization Form for Desktop, Printers, UPS, Inverters, External Hard Drive, Servers and Network Switch
PQ-9	**Presence in Tamil Nadu**	**9.1** The Bidder should have a local office in Chennai, Tamil Nadu.	Copy of the Sale deed/ Rental/ Lease Agreement/ latest Landline Telephone bills signed by Authorized Signatory of the Bidder shall be submitted

SNo.	Qualification Criteria Type	Pre-Qualification Criteria	Documentary Proof to be submitted
		9.2 If the Bidder does not have an office in Chennai as on date of submission of bid, the Bidder if selected, will be required to open an office within 30 days from the date of issuance of Letter of Acceptance (LOA)	Undertaking for setting up the local office in Chennai, Tamil Nadu within 30 days shall be submitted.
PQ-10	**Manpower Strength**	The Bidder should have a minimum number of 500 technically qualified IT professional Staff (B.E/ B.Tech/ M.E./ M.Tech/ MBA/ MCA) with experience in Software development, IT Infrastructure, System & Database Administration, Project Management experience) as on 31st March 2020 on its rolls in India.	Certificate from authorized person in HR Department of the Bidder for exact number of technically qualified IT professional on rolls of the company as on 31st March 2020 as per format provided in Annexure 8.3 (6) of this RFP
PQ-11	**Accreditations**	The Bidder should have the following valid certifications as on date of bid submission. a) SEI CMMI Level 3 or higher b) ISO 27001 certification or higher or equivalent (Information Security Management)	1. Copy of the SEI CMMI Level 3 or higher, ISO 27001 certification or higher or equivalent and ISO 20000 certification or equivalent Certificate(s) of the Bidder shall be submitted 2. Copy of ISO 9001:2008 certification or higher or equivalent (Quality Management) from OEM of

SNo.	Qualification Criteria Type	Pre-Qualification Criteria	Documentary Proof to be submitted
		c) ISO 20000 certification or equivalent (IT Service Management) d) ISO 9001:2008 certification or higher or equivalent (Quality Management)	Desktop, Printers, UPS, Inverters, External Hard Drive, Servers, Electrical cabling, Patch panel, Information outlet, CAT 6 with cabling, Patch cords and Network Switch shall be submitted.
PQ-12	**Declaration of no Conflict of Interest**	The Bidder should not be bound by any conflict of interest in delivering the scope of the project	The Bidder shall furnish an affirmative statement as to the existence of, absence of, or potential for conflict of interest on the part of the Bidder, due to prior, current, or proposed contracts, engagements, or affiliations with the Department

2.7 Technical Qualification Criteria

S.No.	Evaluation Parameter	Scores
A	Organization Strength	30
B	Prior Project Experience	30
C	Approach & Methodology	20

D	Proposed Team and Governance Structure	20
	Total	**100**

Note:

The bidder should score a minimum cutoff score of 50% in each of the above sections and overall cutoff score of 70% (min 70 marks out of 100) to be qualified for commercial evaluation.

SNo.	Evaluation Criteria	Evaluation Parameter	Maximum Score	Documentary Proof
A	**Organization Strength**		**30**	
1	Bidders Average Sales turnover for the last 3 audited financial years FY 19-20; 18-19; 17-18 as on 31-3-2020 should be minimum INR 200 Crores	The Bidder having an average sales turnover for the last 3 audited financial years will be awarded scores as below: a. INR 200 – 300 Cr – 4 marks b. INR 300 – 400 Cr – 6 marks c. INR 400 – 500 CR – 8 marks d. INR 500 Cr & Above – 10 marks	10	Certificate from the statutory auditor of the Bidder for the last 3 audited financial years (FY 2019-20, FY 2018-19, FY 2017-18)
2	Bidders Average turnover from Supply, Installation and Commissioning of Hardware	The Bidder having an average turnover from Supply, Installation and Commissioning of Hardware	10	Certificate from the statutory auditor of the Bidder for turnover from Supply, Installation and Commissioning of

	Items (Desktop, Printers and Servers) and "Application Development" should be minimum INR 75 Crores in the last three FY Years 19-20; 18-19; 17-18 as on 31-3-2020	Items and "Application Development" for the last 3 audited financial years will be awarded scores as below: a. INR 75 – 125 Cr – 4 marks b. INR 125 – 175 CR – 6 marks c. INR 175 – 225 CR – 8 marks d. INR 225 Cr & Above – 10 marks		Hardware Items and "Application Development" for the last 3 audited financial years (FY 2019-20, FY 2018-19, FY 2017-18)
3	Bidders net worth in the last 3 audited financial years FY 19-20; 18-19; 17-18 should be minimum INR 25 Crores	a. INR 25 – 75 Cr – 2 mark b. INR 75 – 125 Cr – 3 marks c. INR 125 Cr & Above – 4 marks	4	Certificate from the statutory auditor of Bidder ascertaining Total Net Worth for the last 3 audited financial years (FY 2019-20, FY 2018-19, FY 2017-18)
4	Bidders manpower strength on technically qualified IT professionals as on 31st March 2020 with minimum 500 IT professionals	a. 500 – 750 nos.– 1 mark b. 751 – 1000 nos.– 2 marks c. Greater than 1000 nos. – 3 marks	3	Certificate from authorized person in HR Department of the Bidder for exact number of technically qualified IT professional staff on the rolls of the company along with their Educational Degree as on 31st March 2020 as per format provided in Annexure 8.3 (6) in this Volume 1 of RFP

5	Valid CMMI Certification with a minimum level of CMMI Level 3	a. CMMI level 3 – 1.5 marks b. CMMI level 5 – 3 marks	3	1. Copy of valid Certificate as on Bid Submission Date.
B	**Prior Project Experience**		**30**	
1	Bidders to have implemented IT System Integration Project with a Minimum Contract Value of INR 75 crores with at least 3 of the following services through a single/ multiple (Up to 3 only) contract in India for any State / Central Government / Quasi Government / PSU Clients in last 10 years (as on 31st March 2020) The Bidders should have successfully completed at least one year of Operations and Maintenance post the successful	Marks will be provided based on the combined project value of maximum 3 projects a. INR 75 – 100 Crores – 2 marks b. INR 100 – 125 Crores – 4 marks c. INR 125 – 150 Crores – 6 marks d. INR 150 – 175 Crores – 8 marks e. Greater than INR 175 Crores – 10 marks	10	1. Work Orders and Completion certificates issued by the client for completed projects 2. In case the project is in Operation and Maintenance phase, the bidder can submit Work Order and a certificate issued by the client mentioning that at least 1 year of Operation and Maintenance has been successfully completed. 3. Project summary details to be provided as per format provided in Annexure 8.4 (1) of this volume of RFP

	completion of the Implementation phase for the same project 1. Procurement Supply Installation and Commissioning of Hardware Items (Desktop, Printers and Servers) 2. Operation & Maintenance of Hardware Items (Desktop, Printers and Servers) 3. Application Development Support and Maintenance 4. Help Desk Services 5. Training & Capacity building			1. Work Orders and Completion certificates issued by the client for completed projects 2. In case the project is in Operation and Maintenance phase, the bidder can submit Work Order and a certificate issued by the client mentioning that at least 1 year of Operation and Maintenance has been successfully completed. 3. Project summary details to be provided as per format provided in Annexure 8.4 (1) of this volume of RFP 4. Manufacturer's Authorization Form obtained for hardware in prior projects shall also be submitted

2	Prior project experience in application development / customization and maintenance for any Government Projects in India with minimum contract value of each project worth of INR 10 Crores in the last 10 years (as of 31st March 2020).	a. 1 project – 2 marks b. 2 projects – 4 marks c. 3 projects – 6 marks a. INR 10 Cr- 15 Cr – 2 marks b. Greater than INR 15 Cr – 4 marks If any one of the projects exceeds 15 Cr, the bidder shall be eligible for 4 marks above.	6 4	1. UAT Signoff/ Completion/ Performance certificate/ Work Order/ Contract issued by the client for completed projects 2. In case the project is in Operation and Maintenance phase, the bidder can submit Work Order/ Contract and a certificate issued by the client mentioning that at least 1 year of Operation and Maintenance has been successfully completed. 3. Project summary details to be provided as per format provided in Annexure 8.4 (1) of this volume of RFP
3	Previous project experience in working with Police Departments in India with minimum contract value of each project worth of INR 10 crores. Scope of work should include any 3 of the following services 1. Supplying, installation	Marks would be awarded based on cumulative project value of maximum 4 projects. a. INR 10 to 20 Crores – 2 marks b. INR 20 to 30 Crores – 3 marks c. INR 30 to 40 Crores – 4	5	1. UAT Signoff/ Completion/ Performance certificate/ Work Order/ Contract issued by the client for completed projects 2. In case the project is in Operation and Maintenance phase, the bidder can submit Work Order/ Contract and a certificate issued by the client mentioning that at

	and commissioning of Hardware 2. Application Development / customization / Maintenance 3. Operations and Maintenance 4. Training & Capacity Building	marks d. Greater than 40 Crores – 5 marks		least 1 year of Operation and Maintenance has been successfully completed. 3. Project summary details to be provided as per format provided in Annexure 8.4 (1) of this volume of RFP
4	Prior Project Experience in providing training & capacity building to minimum 500 Government officials of State / Central Government / Public Sector Undertaking in India.	a. 500 – 1000 – 2 marks b. 1001 – 1500 – 4 marks c. Greater than 1500– 5 marks	5	Work Order/ Completion certificate issued by the client.
C	**Approach & Methodology**		**20**	
1	Understanding of the technical requirements of the project covering the overall Scope of Work.		3	Solution architecture for overall system including application architecture, database architecture, security architecture shall be submitted.
2	1. Approach and Methodology towards application development 2. Approach and Methodology for Site Preparation		1 1	Strategy (covering module wise application development strategy, site

	3. Approach and Methodology for Hardware Supply & Installation	1	inspection plans, distribution plans across districts etc.) for Implementation Roll Out shall be submitted
3	Methodology for Operations and Maintenance (Software + Hardware)	2	Overall strategy to meet SLA requirements, setting up of helpdesk and resource deployment plan for helpdesk shall be submitted
5	Plan & Methodology for procurement of EMS tool and setting up of Helpdesk for Asset monitoring and incident management.	2	
6	Project Plan with detailed activities, sequencing, dependencies among activities	2	Project plan to also include week wise activities with work breakdown structure, milestones, RACI matrix, dependencies etc.
7	Resource planning & sizing during rollout and Operations & Maintenance	2	Approach for Setting up helpdesk to meet SLA requirements, ramp up plan in case of additional manpower requirement in future to be included
8	Understanding of SLA Measurements & Strategy for adherence to SLA Compliance.	2	Understanding of project SLA requirements, SLA management methodology and approach or carrying out the activities for expected output to be explained
9	Risk Management & Mitigation plan for overall project	2	Plan for risk mitigation and technical approach to address the risks to be

				detailed.
10	Technical Presentation of Project requirement as mentioned in this section (Section C of Technical Qualification)		2	Soft Copy of the Presentation to be submitted before the presentation.
D	**Proposed Team**		**20**	
1	Proposed Overall Governance Structure and Escalation Mechanism		4	1. The Bidder should provide CV (format provided in Annexure 8.4.3 (b) of all the below resources mentioning the projects handled along with experience meeting the requirements mentioned in Section 12 of Volume 2 of this RFP. Copy of documents confirming on roll status of the resources with bidder organization such as (Company ID Card, Aadhaar Card, EPF number, PAN, Email ID) 3. Flowchart and Detailed plan of resource deployment
2	Proposed profile for Project Manager (Refer Section 13 for detail of Volume II of this RFP)	Education Qual. / Experience – 2 marks Prior project experience in similar projects – 2 marks	4	
3	Proposed profile for Team Lead - Technical Architect / Application Development (Refer Section 13 for detail of Volume II of this RFP)	Education Qual. / Experience – 2 marks Prior project experience in similar projects – 2 marks	4	
4	Proposed profile for Team Lead - Data Center Management (Refer Section 13 for detail of Volume II of this RFP)	Education Qual. / Experience – 2 marks Prior project experience in similar projects – 2 marks	4	
5	Proposed profile for Team Lead -	Education Qual. / Experience – 2	4	

	Service Desk Management (Refer Section 13 for detail of Volume II of this RFP)	Prior project experience in similar projects – 1 Local Language knowledge (read / speak) – 1		
	Total		**100**	

Note: Fractional marking may also be awarded for the documents submitted for requirements in Section C & Section D of the Technical Qualification criteria.

2.8 RFP Document

The RFP document made available in the Tamil Nadu Tenders Portal www.tntenders.gov.in or www.elcot.in or https://tntenders.gov.in and can be downloaded free of cost.

2.9 Earnest Money Deposit (EMD)

i. An EMD amount of Rs. 1,00,00,000/- (Rupees One Crore only) as specified in the Tender Schedule shall be paid electronically through their respective internet banking enabled account via NEFT / RTGS to the account of ELCOT before the date and time of opening of the Tender:

Account Number: 6681528770

Indian Bank, Nandanam Branch, Chennai – 600 035.

IFSC Code: IDIB000N078

The EMD in the form of Bank Guarantee is not acceptable.

ii. The EMD of the unsuccessful Bidders will be returned to the Bidders only after the finalization of the tender. The EMD amount held by ELCOT until it is refunded to the unsuccessful Bidders will not earn any interest thereof.

iii. The EMD amount of the Successful Bidder shall be returned to the Bidder only after submission of Performance Bank Guarantee (PBG) as required, for the successful fulfilment of the Contract.

iv. The EMD amount will be forfeited by ELCOT, if the Bidder withdraws the bid during the bid validity period (180 Days) or the successful bidder fails to remit Security Deposit within the stipulated period.

3. Schedule of Bid and Bid Process

3.1 Pre – Bid Meeting

ELCOT will hold a Pre-Bid Conference as per the details mentioned in the Tender Schedule, which would primarily focus on addressing and responding the clarifications sought by the bidders with regard to the RFP document. The purpose of the conference is to provide Bidders with information regarding the RFP and the proposed solution requirements in reference to the RFP. The Pre-bid conference will also provide each Bidder with an opportunity to seek clarifications regarding any aspect of the RFP and the Project.

i. ELCOT will endeavor to provide a complete, accurate, and timely response to all queries / clarifications to all the Bidders. However, ELCOT makes no representation or warranty as to the completeness or accuracy of any response, nor does it undertake to answer all the queries that have been posed by the Bidders.

ii. All responses given by ELCOT will be published online and can be accessed by all the Bidders. ELCOT's responses will be made available to Bidders by the date mentioned in the 'Tender Schedule' as the corrigendum issued as a part of the RFP document.

iii. ELCOT reserves the right not to respond to any/all queries raised or clarifications sought if, in their opinion and at their sole discretion, they consider that it would be inappropriate to do so or do not find any merit in it.

3.2 Bid Validity Period

Bids shall be valid for a period of 180 days from the date of opening the technical proposals. A Bid valid for shorter period may be considered as non-responsive. In exceptional circumstances, at its discretion, Authority may solicit the bidder's consent for an extension of the validity period.

3.3 Queries/ Clarifications on the RFP

i. A prospective Bidder requiring any clarification in the Tender may notify ELCOT by letter or by Fax or by E-mail to gmproc@elcot.in with a copy to procurement@elcot.in in the format specified in Annexure 1 of this Volume of RFP. We encourage paper free e-mail communication.

ii. The responses to the clarifications will be notified in the websites by means of Corrigendum to the Tender Document. It would be advantageous to commence e-mail contact with procurement@elcot.in to register your e-mail id.

iii. The Bidders shall periodically check for the amendments or corrigendum or information in the websites till the closing date of this Tender. ELCOT will not make any individual communication and will in no way be responsible for any ignorance pleaded by the Bidders.

iv. No clarifications would be offered by ELCOT within 48 hours prior to the due date and time for opening of the Tender.

v. Before the closing of the Tender, ELCOT may amend the Tender document as per requirements or wherever ELCOT feels that such amendments are absolutely necessary. ELCOT at its discretion may or may not extend the due date and time for the submission of bids on account of amendments.

vi. ELCOT is not responsible for any misinterpretation of the provisions of this tender document on account of the Bidders failure to update the proposals on changes announced through the website.

3.4 Right to Terminate the Process

i. ELCOT may cancel the tender process at any time and without assigning any reason. ELCOT makes no commitments, expressed or implied, explicit or implicit, that this process will result in a business transaction with anyone.

ii. This RFP does not constitute an offer by ELCOT

iii. The RFP does not commit ELCOT to enter into a binding agreement in respect of the Project with the shortlisted Bidders.

3.5 Conflict of Interest

Successful Bidder shall furnish an affirmative statement as to the absence of, actual or potential conflict of interest on the part of the Bidder due to prior, current, or proposed contracts, engagements, or affiliations with NCRB/ MHA or State Government. Additionally, such disclosure shall address any and all potential elements (time frame for service delivery, resource, financial or other) that would adversely impact the ability of the Bidder to complete the requirements as given in the RFP. Declaration to this effect shall be submitted by the Bidder in the prescribed format given in the RFP.

3.6 Force Majeure

Neither ELCOT nor the Bidder shall be liable to the other for any delay or failure in the performance of their respective obligations except causes or contingencies beyond their reasonable control due to Force Majeure conditions such as:

a) Act of God, Natural Disaster such as lightening, earthquake, landslide, etc. or other events of natural disaster of rare severity.
b) Meteorites or objects falling from aircraft or other aerial devices, travelling at high speeds
c) Fire or explosion, chemical or radioactive contamination or ionizing radiation
d) Epidemic/ Pandemic
e) Act of war (whether declared or undeclared), threat of war, invasion, armed conflict or act of foreign enemy, unexpected call up of armed forces, blockade, embargo, revolution, riot, religious strife, bombs or civil commotion, sabotage, and terrorism.

A party affected by an event of force majeure should give a written notice with full details as soon as possible and in any event not later than seven calendar days of the occurrence of the cause relief upon. The other party to respond within a reasonable time of not later than fifteen days and issue an acknowledgement on the claim or force majeure applies then dates (period) by which performance obligations are schedule to be met, with extended for that period of time equal to the time lost due to any delay so caused.

3.7 Arbitration and Dispute Resolution

Any dispute or difference, whatsoever, arising between the parties to this contract arising out of or in relation to the terms of this contract shall be resolved by the parties mutually by acting in good faith towards fulfilling the contract and for this purpose the parties mutually agree to furnish or exchange all relevant documents, information and any other material within their special knowledge and thereby conclude their discussions between them / their representatives or officers within a period of time as may be mutually agreed to say the time of commencement of the move to resolve the dispute.

In case, the parties failed to resolve the disputes amicably within the time frame agreed and, in the manner, stated supra, the aggrieved party shall approach the Courts in Chennai City alone to the exclusion of all other Courts to adjudicate the unresolved dispute.

3.8 Withdrawal of Bids

Bidders can withdraw their bids submitted earlier, in case they do not want to participate in this RFP, before the bid closing date and time. Bidders should note that once withdrawn, bid cannot be submitted again for this RFP.

3.9 Resubmission of Bids

Bidders can resubmit the bids at any point of time either in technical bid or in price bid or both, before the bid submission end date and time and only the last content updated successfully will be available for bid opening, at the scheduled date and time.

4. Proposal Submission Instructions

4.1 Tender Procedure

i. ELCOT is using the e-Tendering system of Government of Tamil Nadu namely tntenders.gov.in which is developed and hosted by NIC. Bidders can go to the ELCOT tenders page directly by selecting the elcot - tntenders option from the home page of ELCOT site elcot.in

ii. The bidders should enroll themselves on the website https://tntenders.gov.in using the option "**Online Bidder Enrollment".** This enrollment is free at this point of time.

iii. Possession of a **Valid Class III Digital Signature Certificate (DSC) in the form of smart card/e-token with signing and encryption keys,** in the Company's name is a prerequisite for registration and participating in the bid submission activities through this web site

iv. Digital Signature Certificates can be obtained from the authorized certifying agencies, details of which are available in the web site https://tntenders.gov.in under the link **"Information about DSC".**

v. The web site also has user manuals with detailed guidelines on enrollment and participation in the online bidding process. The user manuals can be downloaded for ready reference.

vi. Bidders can also attend the **training/familiarization programme** on the e-tendering system conducted periodically by NIC.

vii. The bidders will be able to see the status of the tenders for which they have submitted bids in different stages and would also be informed of the status by E-Mail. For the bidders who have specified the Product Category through "Product Category" option, information of all the tenders published, under the selected product category, will be sent by E-Mail.

viii. Bidders should submit the bid well in advance before bid submission end date and time, instead of doing at the last minute, which may fail. In this case, the Tender

Inviting Authority is not responsible for the non-submission of bids at the bidder's end.

ix. Bidder should contact ELCOT helpdesk for any clarifications on the bid submission at any point of time at least one day before the bid submission, so that bid submission goes through smoothly. Bidders should not assume and do the steps and then get into issues which cannot be solved.

x. Bidders should go through the tender documents and get ready with all relevant documents in pdf/ xls/ rar formats as indicated and then have to be uploaded against each. In the technical bid, bidders may attach an index page wherever necessary, in the beginning, which indicates the details of the files/documents that follow the index page against each technical bid content indicated. This will also help for easy reference later.

xi. While scanning the bid documents to convert to pdf, bidders are asked to scan the page in 65 to 100 dpi mode, to get a readable page after scanning and also the size of the document will also be lesser. For pages in text, it is advised to use 65dpi mode and for pages with images, 100 dpi mode.

xii. Bidders can get ready the technical bid and price bid in filled form in advance instead of doing at the last moment and once ready in all aspects, they may chose the freeze option to submit the bid finally and thereafter they will get a bid acknowledgement receipt which is the final end indicating the successful submission of the bid submission process.

xiii. Bidders can do the resubmission of the bid any number of times, either technical bid or price bid or both till the end date and time of bid submission. The content of the last submitted bid alone will be opened at the time of tender opening.

xiv. Bidders can withdraw the submitted bid before the end of bid submission date and time with proper reasons and once it is withdrawn, bids cannot submit again for that tender.

xv. For all tender processing activities, the server time indicated at the top, while doing bid submission/tender opening activities is the final. The local system time will not be taken into account in this case.

xvi. Bidders may contact the ELCOT help desk by mail etendersupport@elcot.in or by mobile 9566003517 to get any clarifications on bid submission process well in advance.

4.2 Tender Fee

For each and every proposal submitted, a non-refundable tender fee as mentioned in tender schedule should be paid through NEFT/ RTGS in offline mode as per the details mentioned in electronically to the details mentioned in S.No. 5 of the Tender schedule. In case tender fee is paid in advance by the Bidder, but due to some reasons the proposals could not be uploaded, the tender fee paid earlier will not be refunded.

4.3 Updation of Payment Details

i. The payment particulars with respect to tender fee and EMD should be entered in the e-Tender Portal, the bidder should select NEFT / RTGS payments and then enter UTR No. and other details as required.

ii. The necessary hard copy of the acknowledgement of the payment made through NEFT/ RTGS should be submitted to ELCOT before due date and time of opening of the tender.

iii. At the time of opening of Technical proposals, the payments committed in the proposal should be factual and should match with the physically submitted hard copies of payments.

iv. Even though the payment particulars are entered in the Tender portal, if the Bidder fails to submit the hard copies of payment, their proposals are liable for rejection.

4.4 Proposal Submission

The EMD will be paid through NEFT / RTGS only as specified in the tender document. The procedure for submission of tender document is Two Part System and the details are as follows:

1. Technical Proposal.

   It comprises;

   a. Pre-qualification Criteria

   b. Technical Qualification Criteria

2. Commercial Proposal

All the documents (uploaded online) submitted by the Bidder should have page number and should be indexed in the prescribed format.

i. Technical Proposal Form (Pre-qualification Criteria and Technical Qualification Criteria):

   a. The content format of the Technical Proposal will be presented in the tender site and the bidder has to upload the relevant documents in the format, as asked in the tender against each item. The Bidder has to verify each uploaded document and then sign the same using the Digital Signature Certificate (DSC) before final submission.

   b. The Technical Proposal Form should not be changed or altered or tampered. If the Proposal form is tampered, the bids will be summarily rejected.

   c. The Technical Proposal Form should not contain any Price indications strictly; otherwise the Proposals will be summarily rejected.

   d. The Technical Proposal format as given in the RFP shall be filled, signed using the DSC and the scanned copy in the prescribed format shall be submitted.

   e. The supporting documents and other documents should be submitted in pdf in the Technical Proposal as indicated in Annexure 4.

ii. Commercial Proposal Form

a. The Commercial Proposal Form called Bill of Quantity (BOQ) will be in spread sheet format (xls). The original BOQ should be downloaded from the tender site, filled in at the appropriate places indicated in offline and then it has to be uploaded with the same name against the Commercial Proposal option. The BOQ has to be verified and then signed using the DSC before final submission.

b. The Commercial Proposal Form should not be changed or altered or tampered. If the Commercial Proposal form is tampered, the Proposals will be summarily rejected.

c. The Commercial Proposal Form should not contain any conditional offers or variation clauses; otherwise the Proposals will be summarily rejected.

d. The Prices quoted shall be in INDIAN RUPEES (INR) only. The RFP is liable for rejection if Commercial Proposal contains conditional offers.

e. The cost quoted by the Bidder shall include cost and expenses on all counts viz., cost of equipment, materials, tools, techniques, methodologies, manpower, supervision, administration, overheads, travel, lodging, boarding, in-station & outstation expenses, etc., and any other cost involved in the work.

f. In cases of discrepancy between the prices quoted in words and in figures, lower of the two shall be considered.

g. The cost quoted by the Bidder shall be kept firm for a period specified in the RFP from the date of opening of the RFP. The Bidder should keep the Price firm during the period of Contract including during the period of extension of the time if any. Escalation of cost will not be permitted during the said periods or during any period while providing services whether extended or not for reasons other than taxes payable to the Government of India within the stipulated delivery period. The Bidders should particularly take note of this factor before submitting the Bids.

h. The Prices finalized after negotiations should be kept valid during the Contract period and no escalation in the final price will be entertained including reasons due to Foreign Exchange fluctuations.

i. Exchange Rate fluctuations (Foreign Currency Rate Exchange) cannot be cited as reason for delay or dishonour of work order.

4.5 Prices and Price Information

i. The Bidder shall quote price for all the hardware items and for the software services as listed in this RFP.

ii. The Total Bid Price shall be inclusive of

a) Capital expenditure for Application Development.
b) Capital expenditure for Hardware Items in all three phases.
c) Operations & Maintenance expenses for developed application
d) Operations & Maintenance expenses for supplied hardware
e) Operations & Maintenance expenses for already existing hardware (UPS Units, UPS Batteries & Servers)
f) Item-wise unit cost for Site Infrastructure.
g) Unit Price for Anti-virus, HIPS, API, Web service development & Person Man month.

Note:

1. The exact Bill of Quantity for Site Infrastructure will be arrived only after conducting inspection and preparation of site inspection report. Hence unit price would be considered for arriving at the Total Bid Price.
2. API/web service for integration with existing systems would already be part of software development, the API/web service unit price here is for any new requirements post implementation and hence only unit price would be considered for arriving at the total bid price.

3. The price discovery component of Total Bid Value is excluded for the calculation of Total Contract Value. TCV = TBV – Price discovery for Site Infrastructure, Anti-virus, HIPS, API/ Web Services development and Person Man-month rate.

iii. The Total Bid Value & Total Contract Value should be inclusive of all costs including the costs towards packing, forwarding, insurance and transportation, delivery charges, travel / stay, daily allowance or any other allowances with respect to their staff deployed for the execution of this Project before or after the award of the Contract.

iv. The price quoted in the Commercial Proposal shall be the only payment, payable by SCRB to the successful Bidder for completion of the contractual obligations by the successful Bidder under the Contract, subject to the terms of payment specified as in the proposed commercial proposal or the one agreed between ELCOT and the Bidder after negotiations. The price would be inclusive of all taxes, duties, charges and levies as applicable.

v. The prices, once offered, must remain fixed for 2 years from date of signing of contract and must not be subject to escalation for any reason within that 2 years. A proposal submitted with an adjustable price quotation or conditional proposal will be liable for rejection.

vi. Bidder should provide all prices, quantities as per the prescribed format given in Annexure 5 for Bid Response – Commercial proposal. Bidder should not leave any field blank. In case the field is not applicable, Bidder must indicate “0” (zero) in all such fields.

vii. It is mandatory to provide the break-up of all components in the format specified for detailed Bill of Material. The commercial proposal should include the unit price and proposed number of units for each component provided in the Bill of Material. In case of a discrepancy between the Proposed Bill-of-Material and the Commercial

Proposal, the Proposed Bill-of-Material remains valid in terms of quantities and components to be provided under this Contract.

viii. In the event of any increase of the rate of taxes, duties or levies due to any statutory notification/s during the term of the MSA shall be borne by SCRB. In the event of any decrease of rate of taxes, duties or levies due to any statutory notification/s during the term of the MSA shall be passed on by System Integrator to SCRB.

ix. Any increase in Currency rate due to exchange variations shall be borne by the System Integrator.

x. All costs incurred due to delay of any sort, shall be borne by the Bidder.

xi. SCRB reserves the right to ask the Bidder to submit proof of payment against GST indicated within specified time frames.

4.6 Bid closing date and time

The Bids should be submitted not later than the date and time specified in the Tender Schedule or Corrigendum if published. The e-Tender portal will automatically lock exactly on the date and time. Even if the Bid submission is in halfway through during the closing date and time, submission would not be possible. Hence the Bidders should be cautious to submit the Bids well in advance to avoid disappointments.

4.7 Modification and Withdrawal of Proposals

No proposal shall be withdrawn during the bid validity period. Entire EMD shall be forfeited if any of the bidders withdraw their bid during the validity period.

4.8 Condition under which this RFP is issued

i. Bidders shall not make attempts to establish unsolicited and unauthorized contact with the Tender Accepting Authority, Tender Inviting Authority or Tender Scrutiny Committee after the opening of the Tender and prior to the notification of the Award and

any attempt by any Bidder to bring to bear extraneous pressures on the Tender Accepting Authority shall be sufficient reason to disqualify the Bidder.

ii. Notwithstanding anything mentioned above, the Tender Inviting Authority or the Tender Accepting Authority may seek bonafide clarifications from Bidders relating to the tenders submitted by them during the evaluation of tenders.

4.9 Non – Conforming Proposals

A Proposal may be construed as a non – conforming proposal and ineligible for consideration;

i. If it does not comply with the requirement of this RFP.
ii. If the proposal does not follow the formats requested in this RFP.

4.10 Disqualification/ Rejection of Proposal(s)

The proposal is liable to be disqualified in the following cases or in case bidder fails to meet the bidding requirements as indicated in this RFP:

i. Proposal not submitted in accordance with the procedure and formats prescribed in this document is treated as non-conforming proposal

ii. During validity of the proposal, or its extended period, if any, the bidder increases his quoted prices

iii. Proposals with Conditional Offers.

iv. The bidder not confirming to unconditional acceptance of full responsibility of providing services in accordance with the scope of work and Service Level Agreements of this RFP.

v. Proposal is received with suppression of information or incomplete information

vi. Proposal is not accompanied by all the requisite documents

vii. Proposal is not accompanied by the EMD

viii. If bidder provides quotation only for a part of the project

ix. Proposals from Consortium bidders

x. Information submitted in the Proposal is found to be suppressed, misrepresented, incorrect or false, accidentally, unwittingly or otherwise, at any time during the processing of the contract (no matter at what stage) or during the tenure of the contract including the extension period, if any.

xi. Bidder tries to influence the proposal evaluation process by unlawful/ corrupt/ fraudulent means at any point of time.

xii. In case any one bidder submits multiple proposals or if common interests are found in two or more bidders, the bidders are likely to be disqualified, unless additional proposals/bidders are withdrawn upon notice immediately

xiii. Bidder fails to deposit the Performance Bank Guarantee (PBG) or fails to enter into a contract within 21 working days from the date of Issuance of Letter of Acceptance.

xiv. While evaluating the proposals, if it comes to ELCOT's knowledge expressly or implied, that some bidders may have colluded in any manner whatsoever or otherwise joined to form an alliance resulting in delaying the processing of proposal then the bidders so involved are liable to be disqualified for this contract as well as blacklisted for the period of three years from participation in any of the tenders floated by ELCOT.

xv. If the information on price, pricing policy, pricing mechanism or any information indicative of the commercial aspects of the bid is mentioned anywhere other than the commercial proposal.

4.11 Site Visit by Bidder

The bidder may visit and examine any of the Police Stations to obtain all information on the existing processes and functioning of the stations for preparing the bid response document. The bidder may carry out such site visit only after obtaining written permission of SCRB through ELCOT.

The visit may not be used to raise questions or seek clarification on the RFP from the site personnel. All such queries or clarifications must be submitted in writing to the Tender Inviting Authority as part of Pre-Bid Clarification. The cost of such visits to the site(s) shall be at the Bidder's own expense and should not be included in the Commercial proposal.

5. Bid Opening and Proposal Evaluation Process

5.1 Suppression of facts and misleading information

i. It is the responsibility of the Bidder to submit the full copies of the proof documents to meet out the criteria. Otherwise, ELCOT at its discretion may or may not consider such documents. The bidders should note that any data in the supporting documents submitted by the bidders for proving their eligibility is found masked or erased, ELCOT shall have the right to seek the correct data or reject such bids.

ii. The RFP calls for full copies of documents to prove the bidder's experience and capacity to undertake the project.

5.2 Bid Opening Sessions

i. The representatives of the bidders are advised to carry their identity card and a letter of authority from the bidding firms for attending the opening of the Pre-Qualification Proposal, Technical Proposal and Commercial Proposal of the bid.

ii. The bidders' representatives who are present during the opening of Pre-Qualification Proposal, Technical Proposal and Commercial Proposal shall sign a register evidencing their attendance.

iii. In the event of the specified date of bid opening being declared a holiday for ELCOT, the Bids shall be opened at the same time and location on the next working day. However, if there is no representative of the bidder, ELCOT, shall go ahead and open the bid of the bidders.

iv. The Technical Bid will be opened online on the date and time as specified in the Tender schedule in the presence of those Bidders, who choose to be present against production of an authorization letter from the Bidding authority.

v. The technical qualification criteria would be evaluated only for those bidders who meet the Pre-Qualification criteria mentioned in Section 2.6 of Volume 1 of this RFP and submitted the requisite supporting documents as per the format provided in Annexures.

vi. The technically qualified bidders will be informed about the date and venue of the opening of the commercial proposals.

vii. The Commercial proposals of the Technically Qualified Bidders alone will be opened on the scheduled date and time in the presence of the Technically Qualified Bidders. The Bidders or their authorized representatives will be allowed to take part in the Price bid Opening

5.3 Sample Submission

i. For each hardware item quoted in the RFP, the samples should be submitted to ELCOT indicating the make, model number and brochures / specification of the items for testing by ELCOT as per Annexure 8.2 (Sample Submission Form) of this RFP.

ii. The pre – qualified bidders have to submit the samples within 7 days from the date of intimation from ELCOT unless any specific time given by ELCOT in writing.

iii. If the samples are not delivered within the time limit specified, the technical proposal would be treated as non-responsive and it is liable for rejection.

iv. Bidders shall also arrange for an evaluation/ trial/ demonstration of the tendered items (samples) to SCRB.

v. Technical compliance report for each sample should be given by the bidders as specified in Annexure 8.4.5, by filling up the Hardware compliance sheet.

vi. Sample evaluation for adherence to minimum technical specifications as per Annexure 8.4.5 will be conducted during technical proposal evaluation.

5.4 Bid Evaluation Process

1. Stage 1: Pre – Qualification

i. ELCOT shall validate the "Tender Fee & Earnest Money Deposit (EMD)".

ii. ELCOT will review the Pre-Qualification Proposal of the bidders to determine whether the requirements as mentioned in Pre-Qualification Criteria of the RFP are met. Each of the Pre-Qualification condition mentioned in the RFP is MANDATORY. Incomplete or partial Proposals are liable for rejection.

iii. All those Bidders whose Pre-Qualification Proposal meets the requirements would be selected for opening of the Technical Qualification Proposal opening.

2. Stage 2: Technical Proposal

i. Technical Proposals of the pre – qualified bidder (Stage -1) will alone be evaluated.

ii. ELCOT will review the Technical Qualification proposals of the Pre-Qualified bidders to determine whether their proposals are substantially responsive and to determine whether the requirements as mentioned in Technical Qualification criteria of the RFP are met. Bids that are not substantially responsive are liable for rejection.

iii. Proposal Presentations: ELCOT may invite each bidder to make a presentation to ELCOT, at a date, time and venue decided by ELCOT. The purpose of such presentations would be to allow the bidders to present their proposed solutions to the Technical Committee and orchestrate the key points in their proposals. **The team proposed for deployment shall make the presentation**.

iv. ELCOT shall assign a technical score to the bidders based on the Technical Qualification criteria detailed in this RFP. The Bidders are instructed to submit all relevant documents in support of the technical evaluation criteria as specified.

v. Bidders should submit the samples as per the terms specified in Section 5.3 "Sample Submission Clause" initially to ELCOT and to SCRB for testing/evaluation. Preliminary sample evaluation will be done at ELCOT and the samples will be forwarded to SCRB for further evaluation. Based on the sample acceptance report from SCRB, the Technically qualified bidders will be selected under this tender for further process i.e. on the satisfactory comments/feedback from SCRB, the bidder will be selected as technically qualified bidder. The samples of those Bidders, which do not conform to the technical specifications, the technical proposals of those Bidders will be rejected. The whole evaluation exercise would be done in the presence of the bidders in a transparent manner. Proposal without submission of samples are liable for rejection.

vi. At any time during the evaluation process, ELCOT/ SCRB may seek oral clarifications from the bidders.

vii. Bidders, those who score the minimum cut-off score of 70% in each section mentioned in Technical Qualification Criteria (Section 2.7) of the RFP will alone qualify for the evaluation of the commercial proposal.

3. Stage 3: Commercial Proposal

i. All the technically qualified bidders will be informed to participate in Commercial Bid opening process.

ii. The commercial proposals for the technically qualified bidders shall be opened on the notified date and time and reviewed to determine whether the commercial proposals are substantially responsive. Bids that are not substantially responsive are liable for rejection.

iii. Partial proposal shall be liable for rejection and hence the bidder has to quote for all the items.

iv. The Commercial Score of the bidder shall be calculated with respect to the lowest Total Price and shall be calculated for a maximum score of 100. The methodology for calculation of Commercial Score shall be as follows;

Commercial Score of the bidder under consideration = (Lowest Total Price out of all Commercial Bids / Total Price quoted in Commercial bid by the bidder under consideration) X 100

5.5 Total Bid Evaluation

i. The Total bid evaluation shall be based on Quality and Cost based Evaluation (QCBS). Technical Score shall have 70 % weightage and Commercial Score shall have 30% weightage.

ii. The Total Score of the bidder = 0.7*(Technical Score) + 0.3*(Commercial Score)

a. ***The bidder achieving the highest Total Score shall be invited for negotiations for awarding the contract.***

b. ***In case of a tie where two or more bidders achieve the same highest Total Score, the bidder with the higher Technical Score will be invited first for negotiations and for awarding the contract.***

iii. The evaluation, negotiation and Award of Contract will be done as per provisions of Tamil Nadu Transparency in Tenders Act, 1998 and The Tamil Nadu Transparency in Tenders Rules, 2000 as amended from time to time.

5.6 Evaluation Guidelines

i. The evaluation will be carried out for the compliance against the Pre-Qualification and Technical qualification criteria as defined in the RFP. The bidders are instructed to submit all required documents in support of the evaluation criteria specified.

ii. All the documentary proof shall be legible & readable otherwise the document shall not be considered for evaluation.

iii. The proposals that do not conform to the RFP conditions shall be liable for rejection.

iv. ELCOT reserves the right to do a reference check of the details provided by the bidder.

v. No content in the documentary proofs should be scored/ shaded/ deleted/ erased otherwise the document may not be considered for evaluation.

vi. No new documents (other than those mentioned in the proposal) will be accepted for evaluation after opening of the Pre-Qualification and Technical Qualification Criteria.

5.7 Negotiations with the Successful Bidder

ELCOT reserves the right to carry out negotiations with the Bidder who scores high in the total score. ELCOT/SCRB may further discuss the details of the Approach & Methodology, Bill of Quantity, Helpdesk Setup, Service level, Timelines, Delivery quality etc. to be adopted by the

bidder on the project over and above the minimum requirements of the RFP in the interest of the project.

6. Award of Contract

6.1 Award Criteria

Post evaluation process and negotiations, ELCOT will award the Contract to the bidder whose proposal has been determined to be technically responsive to the requirements of the RFP and has obtained the high score in total bid evaluation process will be considered as successful bidder and henceforth referred as 'System Integrator'.

6.2 Notification of Award and Letter of Acceptance

i. After the successful completion of negotiations, SCRB will issue Letter of Acceptance (LOA) to the successful bidder.

ii. The contract period will commence from the date of contract signing.

iii. Upon the identification of successful bidder, ELCOT shall notify unsuccessful bidders and will return their EMD.

iv. Upon the receipt of PBG from successful bidder, ELCOT shall return the EMD of the successful bidder.

6.3 Performance Bank Guarantee (PBG)

i. The successful bidder should submit the Performance Bank Guarantee (PBG), within 21 days from the Letter of Acceptance (LOA) received by the successful bidder.

ii. In case the successful bidder fails to submit PBG within the stipulated time, SCRB at its discretion may cancel the order placed to the successful bidder.

iii. The PBG for a value equivalent to 5% of the total contract value shall be submitted as per the format provided in this RFP from Scheduled Bank.

iv. The PBG shall be valid for a minimum period of 70 months.

v. SCRB shall invoke the PBG in case the successful bidder fails to discharge their contractual obligations during the period or SCRB incurs any loss due to the bidder's negligence in carrying out the project implementation as per the agreed terms & conditions and service level agreement.

6.4 Signing of Contract

After the Issuance of LOA by SCRB to the successful bidder and on submission of PBG by the Successful Bidder, the Successful Bidder shall enter into a contract with SCRB within 30 days, as mentioned in Volume III of this RFP. Once the contract is executed, the successful bidder shall be termed as "System Integrator".

ELCOT shall have the right to annul the award in case there is a delay of more than 30 days in signing of Contract from the date of Notification of Award/ Letter of Award by SCRB, for reasons attributable to the successful bidder.

6.5 Assigning Single Point of Contact (SPOC)

The Successful Bidder should nominate and intimate ELCOT/ SCRB, a Nodal Officer, for Single Point of Contact (SPOC), who should be responsible for effective delivery of work complying with all the terms and conditions. The Successful Bidder should ensure that the Nodal Officer is to be fully familiarized with the Tender Conditions, Scope of Work and deliverables.

6.6 Contract Period

The Contract will be valid during the implementation phase and the operation & maintenance phase (five years). In case of a delay during implementation phase for reasons attributable to the Selected System Integrator, the contract shall be extended accordingly without any additional cost.

6.7 Failure to Agree with the Terms and Conditions of the RFP

Failure of the System Integrator to agree with Terms & Conditions of the signed Contract at any stage of the Contract Period shall constitute sufficient grounds for termination of the contract and invoking of the Performance Bank Guarantee (PBG).

6.8 Return of PBG

The PBG will be returned to the System Integrator on completion of entire project (Go- Live + 5 years of operation & maintenance) subject to satisfaction of SCRB. Such completion would be arrived at when the entire scope is completed by the System Integrator as per the contract agreement signed between Selected System Integrator and SCRB.

6.9 Termination of Contract

This Contract may be terminated under the following conditions:

1. Termination for Convenience

By SCRB - By giving the System Integrator not less than 30 (thirty) days written notice of termination;

i. SCRB may at any time terminate the Contract for any reason by giving the System Integrator a notice of termination that refers to this clause.

ii. Upon receipt of the notice of termination under this clause, the System Integrator shall either as soon as reasonably practical or upon the date specified in the notice of termination:

   a. ceases all further work, except for such work as SCRB may specify in the notice of termination for the sole purpose of protecting that part of the System already executed, or any work required to leave the site in a clean and safe condition;

   b. removes all System Integrator's Equipment from the site, repatriate the all System Integrator's, remove from the site any wreckage, rubbish, and debris of any kind;

iii. in addition, the all System Integrator shall:

   a. delivers to SCRB the parts of the System executed by the all System Integrator up to the date of termination;

b. to the extent legally possible, assign to SCRB all right, title, and benefit of the System Integrator to the System, or Subsystem, as at the date of termination, and, as may be required by SCRB

c. deliver to SCRB all non-proprietary drawings, specifications, and other documents prepared by the System Integrator as of the date of termination in connection with the System.

Note:

On termination, the System Integrator shall be paid for the work completed and signed off as per the payment milestones.

2. Termination for default

By SCRB: -

i. If System Integrator commits any material breach of any term of this RFP and which in the case of a breach capable of being remedied has not been remedied upto the satisfaction of SCRB, within 30 days of written notice to remedy the same;

ii. If the System Integrator is not able to deliver the services as per the SLAs defined in RFP which translates into Material Breach, then SCRB may serve 30 days written notice for curing this Material Breach. In case the Material Breach continues, after the expiry of such notice period, SCRB will have the option to terminate this Agreement. Further, SCRB may offer a reasonable opportunity to the System Integrator to explain the circumstances leading to such a breach.

Note: On termination, the System Integrator shall be paid for the work completed and signed off as per the payment milestones.

Change of Ownership control at Bidder

i. In the event that Bidder undergoes such a change of control, SCRB may, as an alternative to termination, require a full Performance Guarantee for the obligations of Bidder by a guarantor acceptable to SCRB or its nominated agencies. If such a guarantee is not furnished within 30 days of SCRB's demand, the SCRB may

exercise its right to terminate this Agreement in accordance with this Clause by giving 15 days further written notice to the System Integrator.

ii. The termination provisions set out in this Clause shall apply mutatis mutandis to the Service Level Agreement.

3. Termination for bankruptcy

i. SCRB may serve written notice on Bidder at any time to terminate the MSA with immediate effect in the event of a reasonable apprehension of bankruptcy of the System Integrator.

ii. The Bidder shall in the event of an apprehension of bankruptcy immediately inform SCRB, well in advance (at least 4 months) about such a development;

Termination shall be without prejudice to any other rights or remedies a party may be entitled to hereunder or at law and shall not affect any accrued rights or liabilities of either party nor the coming into force or continuation in force of any provision hereof which is expressly intended to come into force or continue in force on or after such termination.

6.10 Effects of Termination

i. In the event that SCRB terminates this Agreement pursuant to failure on the part of the System Integrator to comply with the conditions as contained in this Clause and depending on the event of default, Performance Bank Guarantee furnished by System Integrator may be forfeited.

ii. The termination provisions set out in the MSA shall apply *mutatis mutandis* to the Service Level.

iii. Upon termination of the MSA, the parties will comply with the Exit management Schedule, as outlined in the MSA.

iv. Upon the expiration or termination of the MSA, System Integrator shall undertake the actions set forth in the MSA to assist SCRB to replace services as provided hereunder;

a. In respect of System Integrator third party Intellectual Property Rights, the System Integrator undertakes to secure such consents or licenses for SCRB from such third parties as are necessary to enable SCRB or its replacement System Integrator (any other agency that is selected for maintaining the system in place of the System Integrator, if applicable) to receive services substantially equivalent to the Services hereunder.

b. The System Integrator shall transfer to SCRB, in accordance with the terms of the MSA, Assets or Deliverables including the software, if any, (and including any data, ownership, source code and associated documentation which is the work product of the development efforts involved in the Implementation of Project) in which SCRB has the right, title and interest and that is in the possession or control of the System Integrator.

c. In the event of the MSA being terminated (as mentioned in Section 8.2 of Volume 3 of the RFP or due to Force Majeure) earlier than the planned Contract period, the System Integrator shall be eligible to receive payments as described in the Payment Schedule for the work completed and approved by SCRB.

d. The System Integrator's team and/or all third parties appointed by the System Integrator shall continue to perform all their obligations and responsibilities as stipulated under the MSA, and as may be proper and necessary to execute the scope of work under the MSA in terms of the MSA, the RFP and System Integrator's Bid, in order to execute an effective transition and to maintain business continuity.

e. In the event that SCRB terminates the MSA due to default or material breach of the MSA on the part of the System Integrator, then SCRB shall be entitled to invoke the Performance Bank Guarantee submitted for this Project and pursue such other rights and/or remedies that may be available to SCRB under law.

f. Notwithstanding anything contained herein above and without prejudice to the right to terminate the MSA, if the System Integrator fails to set up and operationalize the system at the designated locations, SCRB may in its sole discretion, engage another agency/System Integrator to fulfill the remaining obligations (or part of the remaining obligations) as may be decided, at the risk and cost of the System Integrator. The additional cost incurred by the SCRB shall be recoverable from the Performance

Bank Guarantee or any amount payable or due to the System Integrator, and in case such Performance Bank Guarantee or amount is not adequate, the System Integrator shall make good the shortfall.

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

h. The action as provided in this clause shall not be construed or treated as waiver of any right of the SCRB and the right to terminate the MSA shall subsist even if an action in accordance with this clause had been taken.

v. If the Contract is terminated by SCRB due to supply of substandard- services, system or hardware to the stations, the difference in cost of the items purchased through other Technically Qualified Bidders or any other alternative sources will be recovered from the System Integrator.

6.11 Assigning the Tender whole or in part

The System Integrator shall not assign or make over the contract, the benefit or burden thereof to any other person or persons or body corporate. The System Integrator should not underlet or sublet to any person(s) or body corporate for the execution of the contract or any part thereof without the written consent of SCRB.

6.12 Limitation of Liability

i. Neither party shall be liable to the other party for any indirect or consequential loss arising out of or relating to the Contract.

ii. In the case of **Gross negligence** or **Willful misconduct** on the part of the System Integrator/System Integrator's team or on the part of any person or firm acting on behalf of the System Integrator executing the work or in carrying out the services, the System Integrator, with respect to damage including to property and/or Assets/ Sales/ Revenue of SCRB or of any of the Stations shall regardless of anything contained herein, will be liable for any direct loss or damage that is less than or equal to **(A) the Total Contract**

Value of the Project or (B) the proceeds the System Integrator may be entitled to receive from any insurance maintained by the System Integrator to cover such a liability, whichever of (A) or (B) is higher.

For the purposes of this clause, "Gross Negligence" means any act or failure to act by a party which was in reckless disregard of or gross indifference to the obligations of the party under the MSA and which causes harmful consequences to life, personal safety or real property of the other party which such party knew, or would have known if it was acting as a reasonable person, would result from such act or failure to act. Notwithstanding the foregoing, Gross Negligence shall not include any action taken in good faith for the safeguard of life or property.

Gross Negligence will also mean- Loss of SCRB's revenue due to malfunctioning of system deployed by System Integrator as a part of this project.

Willful Misconduct means an intentional disregard of any provision of the MSA which a party knew or should have known if it was acting as a reasonable person, would result in harmful consequences to life, personal safety or real property of the other party but shall not include any error of judgment or mistake made in good faith.

iii. There shall be no limitation of liability in respect of the System Integrator in case of any damages for bodily injury (including death) and damage to real property and tangible personal property, other than as applicable under the relevant laws.

iv. The MSA does not grant or create any rights, benefits, claims, obligations or causes of action in, to or on behalf of any person or entity (including any third party) other than between the respective parties to the MSA, as the case may be.

v. Any claim or series of claims arising out of or in connection with the MSA shall be time barred and invalid if legal proceedings are not commenced by the relevant party against the other party within a period of 3 years from the date when the cause of action first arose or within such longer period as may be permitted by applicable law without the possibility of contractual waiver or limitation.

vi. SCRB shall be entitled to claim the remedy of specific performance under the MSA.

This right to claim for any damage shall be without prejudice to other rights and remedies available to SCRB under the contract and law. SCRB shall be entitled without prejudice to its other rights and remedies, to deduct from the price payable to the System Integrator and also to encash the PBG, provided the total amount recovered does not exceed the Total Contract Value or the insurance cover, whichever is higher.

7. Specification

1. New Hardware Items

1) Desktop:

SNo.	Parameters	Minimum Specification
1	Processor	Intel Core i5-10th generation (3.0 Ghz) or higher
2	Memory	8GB DDR4 SDRAM@2666 MHz with minimum 2 DIMM slots, upgradeable up to 32 GB, Onboard memory is not acceptable
3	Motherboard	OEM Motherboard
4	Slots	Min 2 PCI/PCI Express Slots
5	Network port	1000 BaseT, Gigabit Ethernet with remote booting facility, RJ45, Wi-Fi 802.11 AC or Above, Bluetooth 5.0 or Above.
6	USB Ports	Min 6 USB Ports (out of that 2 must be in front) with at least two with 3.0
7	Display Port	Display Port (DP), HDMI Port
8	Audio	Line/Mic In, Line-out/Speaker Out (3.5 mm)
9	Hard Disk Drive	Minimum 1 TB SATA Hard Disk @7200 RPM or higher
10	DVD Drive	DVD Writer
11	Keyboard	Minimum 104 keys Heavy Duty Mechanical Switch Keyboard (USB Interface). Rupee Symbol to be engraved.
12	Mouse	Optical with USB interface (same make as desktop)
13	Monitor	Minimum 21.5” diagonal LED Monitor with 1366x768 or higher resolution. (Same make as desktop). Must be TCO05 certified
14	Bays	2 Bays or more
15	General Certification	Hazardous - RoHS, Energy efficient - Energy star, Safety - CE / UL, Environment – EPEAT, MIL - STD 810G test passed, ISO 9001:2008 OEM certification or better
16	Operating System	Linux
17	Office Application	Open Office Suite

18	OS Compliance	Windows & Linux
19	OS Certification	MS Windows and Boss Linux.
20	Security	Discrete TPM 2.0(Hardware), Tool less Chassis with intrusion switch

2) Online UPS with Battery:

SNo.	Parameters	Minimum Specification	
1	Capacity	2 KVA TRUE ONLINE UPS	5 KVA TRUE ONLINE UPS
2	Back-up Time	60 Minutes with 70% Resistive Load	For code OL 5000-60 – 60 minutes
3	Inverter Type	IGBT (Make and current capacity to be specified by the tenderer)	IGBT (Make and current capacity to be specified by the tenderer)
	Input		
4	Input Voltage Range	150 - 270V AC, SINGLE PHASE	150 - 270V AC, SINGLE PHASE
5	Input power factor at Full Load	>0.9	>0.9
6	Input Frequency with Tolerance	40 Hz to 70 Hz	40 Hz to 70 Hz
7	Battery (Secondary Source)	Sealed maintenance free (SMF) type – AH and no. of Batteries shall be suitably selected for the respective minimum backup time of 70% Resistive Load, 60 Minutes – 3160 VAH.	Sealed maintenance free (SMF) type – AH and no. of Batteries shall be suitably selected for the respective minimum backup time of 70% Resistive Load, 60 Minutes – 7900 VAH
8	DC Bus voltage	To be specified by the tenderer	To be specified by the tenderer
9	Make of the Battery	Specify the Manufacturer Make, Model and enclose the technical specification sheet. The make and AH of the battery submitted for evaluation only will be accepted.	Specify the Manufacturer Make, Model and enclose the technical specification sheet. The make and AH of the battery submitted for evaluation only will be accepted.
10	Battery Storage Box	External Storage Box / MS-Rack for housing the Batteries.	External Storage Box / MS-Rack for housing the Batteries.
	Output		

11	Nominal Voltage	230V AC, Single Phase (+/-1%)	230V AC, Single Phase (+/-1%)
12	Frequency	50 Hz, +/-(0.2) Hz	50 Hz, +/-(0.2) Hz
13	Waveform	Pure Sine wave	Pure Sine wave
14	Load power factor at full load	0.7 lag to unity	0.7 lag to unity
	Others Features		
15	Overload Capacity	Overload Capacity: Withstand for 5 Minutes at 110% load (2200 Watts Resistive Load / 1540Watts Combinational Load).	Overload Capacity: Withstand for 5 Minutes at 110% load (2200 Watts Resistive Load / 1540Watts Combinational Load).
16	Total Harmonic Distortion	< 4% for Linear load and 5% for nonlinear load	< 4% for Linear load and 5% for nonlinear load
17	Efficiency	> 80%	> 85%
18	Ambient Temperature	To be specified by the tenderer (Preferable upto 50 Degree Celsius)	To be specified by the tenderer (Preferable upto 50 Degree Celsius)
19	Duty Cycle	Continuous	Continuous
20	Cooling	Forced air cooling	Forced air cooling
21	Protections	1) Input, Output – Low and High 2) Battery low and high voltage 3) Input, output – Fuse 4) Battery - MCB/Fuse 5) Short circuit 6) Overload 7) Lightening	1) Input, Output – Low and High 2) Battery low and high voltage 3) Input, output – Fuse 4) Battery - MCB/Fuse 5) Short circuit 6) Overload 7) Lightening
22	Controls	Manual By-pass Switch and static bypass switch to be provided with Indications	Manual By-pass Switch and static bypass switch to be provided with Indications
23	Power sockets	Power Sockets – 3 Nos. of 5A Socket.	1 No.32 Amps. Capacity Terminal Block
24	Trip Conditions	Indicators for AC Mains, Load on Battery, Fault, Load Level, Battery Low Warning, Inverter On, UPS on Bypass, Overload, etc.	Indicators for AC Mains, Load on Battery, Fault, Load Level, Battery Low Warning, Inverter On, UPS on Bypass, Overload, etc.
25	Alarms (Audio)	Battery low, Mains Failure, Over temperature, Inverter overload, Fault, Extreme battery low voltage.	Battery low, Mains Failure, Over temperature, Inverter overload, Fault, Extreme battery low voltage.

26	Meters	Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.	Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.
27	Manuals	Operating and User manual to be Provided	Operating and User manual to be Provided
28	Name Plate in the UPS	Name plate in UPS-Riveted metal plates / Stickers	Name plate in UPS-Riveted metal plates / Stickers
29	Isolation Transformer	Isolation Transformer must be provided internally / externally at input.	Isolation Transformer must be provided internally / externally at input.
30	Software	Software for automatic shutdown of the system compatible with Linux	Software for automatic shutdown of the system compatible with Linux
31	Certification	SAMEER / ETDC / NTH / ERTL / NABL's or any other Government authorized Testing Lab Certification for any back up of each UPS Category Mandatory for this specification (issued within last 6 years) ISO Certifications Mandatory - ISO 9001:2015 and ISO 14001:2015	SAMEER / ETDC / NTH / ERTL / NABL's or any other Government authorized Testing Lab Certification for any back up of each UPS Category Mandatory for this specification (issued within last 6 years) ISO Certifications Mandatory - ISO 9001:2015 and ISO 14001:2015
32	Integrated Stand	UPS along with the batteries should be accommodated in the existing integrated stand available at the respective locations. If the supplied device cannot be accommodated, then the UPS along with batteries should be supplied along with the integrated stand. The integrated stand should also have electrical panel to control the supply to UPS through a tripper switch and should have provision to tap the UPS supply.	UPS along with the batteries should be accommodated in the existing integrated stand available at the respective locations. If the supplied device cannot be accommodated, then the UPS along with batteries should be supplied along with the integrated stand. The integrated stand should also have electrical panel to control the supply to UPS through a tripper switch and should have provision to tap the UPS supply.
33	Other Features	SNMP Card - Provisions should be available Diesel Generator – Compatible	SNMP Card - Provisions should be available Diesel Generator – Compatible

3) Inverter:

SNo.	Parameters	Minimum Specifications
1	Capacity	3 KVA
2	Back-up Time	120 Minutes
	Input	
3	Under Voltage	150 +/- 10V
4	Over Voltage	285 +/- 10V
	Output	
5	Voltage (INVERTER Mode)	230 V Nominal
6	Frequency (Mains Mode)	Same as Input
7	Frequency (INVERTER Mode)	50 Hz. +/- 2%
8	Frequency (Mains Mode)	Same as Input (45-55 Hz)
9	Overload	> 110%
10	Transfer time	10 ms
	Battery	
11	Type	12 V/135 AH Tubular
12	Number	4 in Series
13	Typical Recharge Time	10-12 Hrs
14	Protection	Battery Deep Discharge, Reverse Polarity, DC Overvoltage
15	LED Displays	Inverter ON Battery Low Mains On Battery Charged Overload No load Over Temperature Short Circuit Under Battery Mode MCB Trip or Short Circuit under Mains Mode
16	Alarms	Low Battery Overload Short Circuit
	Environment	
17	Operating Temperature	0-45 degree C (32-113-degree F)
18	Storage Temperature	0-45 degree C (32-113-degree F)
19	Humidity	0-95% RH non-condensing
20	Certification	SAMEER / ETDC / NTH / ERTL / NABL's or any other Government authorized Testing Lab Certification for this specification (issued within last 6 years) ISO Certifications Mandatory - ISO 9001:2015 and ISO 14001:2015

21	Integrated Stand	Inverter along with the batteries should be accommodated in the existing integrated stand available at the respective locations. If the supplied device cannot be accommodated, then the inverter should be supplied along with the integrated stand. The integrated stand should also have electrical panel to control the supply to inverter through a tripper switch and should have provision to tap the inverter supply.

4) Printer MFP:

SNo.	Parameters	Minimum Specification
1	Printer type	Monochrome Laser
2	Printer Function	Print, Scan, Copy
3	RAM Size	256 MB or higher
4	Printer speed	Minimum 25 PPM or higher
5	Print Resolution	Up to 1200 x 1200 dpi
6	Duty cycle	Minimum 25000 pages or higher
7	Duplex	Automatic
8	Input Tray Capacity	Minimum 250 pages
9	Bypass Tray	1 Sheet or Higher
10	Paper size	A4, Letter, Legal
11	Paper Types	Plain paper, envelopes
12	Toner Type	Composite
13	Initial Toner(s) Yield	2500 pages & above
14	Scanner Type	Flatbed, ADF
15	Scan Resolution	Bidder to Specify

16	Scan file format	JPEG, PDF
17	Scan Mode	BW & Colour
18	Copy speed	Min. 25 ppm or higher
19	Copy Resize	25-400%
20	Copier Resolution	Up to 600 x 600 dpi or Higher
21	Interface/ Connectivity	USB and Ethernet 10/100
22	OS Compatibility	Windows, Linux

5) Printer LP:

SNo.	Parameters	Minimum Specifications
1	Printer type	Laser
2	Printer speed	Minimum 25 PPM
3	Resolution	Min 1200 x 1200 dpi
4	Memory	128 MB
5	Network	Ethernet 10/100 Mbps or above
6	Duty cycle	Minimum 25000 pages or higher
7	Duplex	Automatic
8	Input Tray Capacity	Minimum 250 pages
9	Paper size	A4, Letter, Legal
10	Paper Types	Plain paper, envelopes
11	Media Types	Paper (Plain, Envelopes, Labels & Card stock)
12	Interface/ Connectivity	USB and Ethernet
13	OS Compatibility	Windows and Linux

14	Toner cartridge – Yield	Yield of minimum 1500 pages

6) Ext. HDD:

SNo.	Parameters	Minimum Specifications
1	Capacity	1TB
2	Type	External
3	Interface	USB 3.0 & USB 2.0
4	Spindle Speed	5400 RPM
5	Transfer Rate	100-200 MB/s
6	OS Compatibility	Windows and Linux

7) Server Specifications

SNo.	Parameters	Minimum Recommendation
1	Processor	Latest series/ generation of 64-bit x86/ equivalent processor(s) with 16 or higher Cores Processor speed should be minimum 2.9 GHz and minimum 3.9 GHz turbo frequency, minimum 22MB Cache having SPEC Rate 2017_fp_base of 228 or Higher and SPEC Rate 2017_fp_base of 252 or Higher Minimum 2 processors per each physical server
2	RAM	16 x 32 GB RDIMM scalability upto 1 TB. Proposed memory should have ECC support.
3	Network interface	4 * 1 GB Ethernet Ports 2 * 10 GB Ethernet Ports 1* 16 Gbps Dual port FC HBA Card
4	Power supply	Hot-pluggable 1 + 1 redundancy
5	RAID support	12G SAS H/W Raid controller, which supports RAID: 0/1/5/10 with 2GB Flash Backed Cache
6	Hard Disk Drive	2X600GB 12G SAS 15K SFF Or Higher, Hot Plug expandable upto 8 Nos or Higher
7	Operating System	Licensed version of 64-bit latest version of Linux/ Unix
8	Form Factor	2U Rack Mountable
9	System Fans	Redundant & Hot Plug Fans
10	Interfaces/PCI Slots	Minimum 4 PCI slots
11	Pre-Failure Notification	Failure – Failure notification on HDD, Processor & Memory
12	Industry Standard Compliance	PCIe3.0 Compliant, PXE Support, USB 3.0 Support

13	Security	Power-on password / Keyboard password / Administrator's password, Hardware-based system security feature that can securely store information, such as passwords and encryption keys, which can be used to authenticate the platform.
14	Benchmarks	SPEC int benchmark for the quoted processor models should be submitted either along with the bid or shall be submitted within 15 days from the date of submission of Bid.
15	Virtualization	Shall support Industry standard virtualization hypervisor

8) CAT 6 Cables:

SNo.	Parameters	Specifications & Standards
1	Cable Type and support	4 Pair Twisted Cable, Support for Fast and Gigabit Ethernet, IEEE 802.3/5/12, Voice, ISDN, ATM 155 & 622Mbps. Should be Tested up to 550Mhz
2	Conductor	23 AWG Annealed bare solid copper
3	Insulation	High Density Polyethylene
4	Approx. Cable OD	6.3 mm.
5	Core Color	Fire Retardant PVC Compound (FRPVC) Pair 1: White – Blue Pair 2: White – Orange Pair 3: White – Green Pair 4: White – Brown
6	Pair Separator	4 twisted pairs separated by internal X shaped, 4 channel, polymer spine / full separator. Half shall not be accepted.
7	Sheath	Fire Retardant PVC Compound (FRPVC)
8	Sheath Colour	Grey / Blue
9	Flame Rating	60 deg. C As per UL 1685 CM
10	Operating Environment	Indoor
11	Electrical Specification	@ 250 MHz
12	Standards	TIA / EIA 568 C.2
13	Impedance	100Ohms +/- 15%
14	(NVP) Velocity	69% or more @ 250 MHz Approx.

	of Propagation	
15	Delay Skew	45 ns /100 mtrs. max. @ 20 deg. C, for 1 MHz~250 MHz Approx.
16	Propagation Delay	<=536 ns / 100 mtrs. max. @ 20 deg. C, @ 250 MHz
17	DC Resistance	<= 9.38 ohm / 100 mtrs. max. @ 20 deg. C
18	Mutual Capacitance	5.60 nF / 100 mtrs. max. Approx.
19	Safety	UL Listed

9) Connection Module:

SNo.	Specifications & Standards
1	RJ45 connection module of Category 6, for the establishing of transmission channels of class E with up to 4 plugged connections, complies with Category 6 requirements of the standards ISO/IEC 11801:2002, EN 50173-1: May 2007, DIN EN 50173-1: Dec. 2007 as well as ANSI/TIA/EIA 568-B.2-1, de-embedded tested in acc. with IEC 60603-7-4, interoperable and backwards compatible with Cat.5e and Cat.5.
2	Suitable for 10GBase-T applications in acc. with IEEE 802.3an up to 500 MHz and 55 m.
3	Parallel pair termination without crossover in acc. with EIA/TIA 568-A/B, gold-plated bronze contacts for >1000 mating cycles, IDC contacts with single-wire strain relief and >20 insertion cycles, contact resistance <50 m Ohm, dielectric strength >1000 Veff.
4	Maximum reliability through special contact design without internal transfer points.
5	Should have integral dust cover and integrated bend-limiting strain -relief unit for cable entry.
6	Should have IDC to hold conductor without using any tool for termination of cable.
7	Outlets should be of single metal piece design without any PCB to support the IDC / Contacts.
8	Should be reusable and tool less in design in terms of termination of solid wire installation cable AWG22-24 as well as stranded cables AWG 22/7 – 26/7.
9	Should be made of halogen free material and should be certified by third party like 3P or Delta or GHMT.

10) Patch Panel:

SNo.	Specifications & Standards
1	Patch panel with integrated cable tie shelf, 19" fastening kit, labeling field, accepting the snap-in type color coding clips in 8 colors.

2	Material: sub-rack made of sheet steel (DC01A) 1.5 mm, color blue achromatized, screen made of plastic (ABS), halogen-free, color medium gray (NCS 2502-B)
3	Complies with Category 6 requirements of the standards ISO/IEC 11801:2002, EN 50173-1: May 2007, DIN-EN 50173-1: Dec. 2007 as well as ANSI/TIA/EIA 568-B.2-1, de-embedded tested in acc. with IEC 60603-7-4, interoperable and backwards compatible with Cat.5e and Cat.5.
4	Suitable for 10GBase-T applications in acc. with IEEE 802.3an up to 500 MHz and 55 m in case of unshielded.
5	Each port should be individually terminated i.e. each Port should be individually replaceable & provide consistent port-to-port performance.
6	Each port should have an integral dust cover and integrated bend-limiting strain relief unit for cable entry.
7	Patch panels shall be modular in design and capable of supporting Cat 6 UTP/FTP and S/FTP modules on same port. The same panel should have the capability of terminating multimode and single mode fibers alongside the copper terminations.

11) Patch Cord:

SNo.	Parameters	Specifications & Standards
1	Type	Factory Crimped Cat6 UTP Patch cord with 24 AWG 7/32 Round stranded copper wire.
2	Length	1 Meter
3	Insulation	Polyethylene
4	Cable sheath	CM grade PVC Plug insertion
5	Durability	1000 mating cycles
6	Plug tensile strength	89 N, Plug insulation
7	resistance	>500MW
8	Contact resistance	10 mW

12) Network & Server Racks:

SNo.	Specifications & Standards

1	Feature: 42U 800W X 800D Modular Structures made from aluminum extruded profile, minimum extrusion wall thickness at all sides and corner- 2mm, along with following items: Top and Base Cover with cable enter Black Color.
2	Front/Rear Door: Front, Glass door, 800mm Wide, 42U, with Lock and hexagonal vent on the trims for thermal Management/ air cooling. 42U, 800mm W, Rear Steel Door, with 1/3 hexagonal vent at the base to allow proper air flow and thermal control, with Lock
3	Mounting Angles: 19" Mounting Angles, 19" mounting angles powder coated along with "U" marking
4	Side Panels: 2 Nos. of Removable Side Panels along with slam latch. 4 nos. of 100mm W, Reducing Cable channels on the sides to allow better cable management
5	Castors: Castors - For providing mobility to the rack. Two with foot operated brakes and Two without brakes, having a load carrying capacity of 100kg
6	Fan: 230V AC 90CFM Fan (4 nos. for each Rack) with Fan Housing Unit.
7	Cable Manager: 19", 1U, Horizontal Cable Manager, to allow proper cable routing
8	Cable Loops: 24U to help route the cable vertically
9	Power Supply: 10X 5 amps or 6 X 5 amps socket as per requirement
10	Castors: Castors as needed
11	Cable Storage: 2U cable storage shelf supported with 4 bobbins
12	Power Consumption: Not more than 5 KVA
13	Redundancy: Mechanical Devices such as Hard Disks, Fans and Power Units should be completely Hot Swappable and Redundant to ensure High Availability
14	Power Guaranteeing complete availability even on failure of any 2 power units across the enclosure. Sufficient Power to run a fully loaded enclosure in N+N redundant mode.
15	KVM/CD/USB/Floppy To be enabled Virtually over IP for Remote Access or Provided Locally.
16	Multi-platform Support: Enclosure should support Xeon & RISC/EPIC blade on the Same chassis. Enclosure should also support Unix, Linux and Windows Operating environment

13) Network Switch (Managed):

SNo.	Specifications & Standards
1	Interface Ports: 16 10/100/1000BASE-T Auto-negotiating, Auto-MDI/MDI-X ports with 802.3x Flow Control
2	Performance Switch Capacity: 32Gbps
3	Packet Forwarding Rate: 23.8Mpps or above
4	MAC Address Table Size: 8K

5	MAC Address Update: Up to 256 static MAC entries Enable/disable auto-learning of MAC addresses
6	Packet Buffer: 512KB
7	Power Input: 100 to 240 VAC 50/60Hz Internal power supply
8	Port Standards and Functions: IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Gigabit Ethernet (fiber) ANSI/IEEE 802.3 IEEE 802.3x Flow Control Auto-Negotiation 802.3af Power over Ethernet
9	LAYER 2 Features: IGMP v1/2 Snooping: supports 64 multicast groups 802.1D Spanning Tree Static Port Trunk (Link Aggregation): up to 6 group per device, up to 8 ports per group
10	VLAN: 802.1Q VLAN (VLAN Tagging) Up to 256 static VLAN groups Management VLAN Asymmetric VLAN
11	Quality of Service (QoS): 802.1p Priority Queues Up to 4 queues per port DSCP-based QoS
12	Security: 802.1X Port-based Access Control Broadcast Storm Control Trusted Host Cable Diagnostics function
13	Management: Web-based GUI SNMP v1 support DHCP Client Trap setting for destination IP, system events, fiber port events, twisted-pair port events. Port Access Control Web-based: Configuration backup/ restoration Web-based: Firmware backup/upload System Reboot using web-based interface

14) Network Switch (Unmanaged):

SNo.	Specifications & Standards

1	Standards: IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet ANSI/IEEE 802.3 NWay auto negotiation
2	Protocol: CSMA/CD
3	Data Transfer Rates: Ethernet: 10Mbps (half-duplex) 20Mbps (full-duplex) Fast Ethernet: 100Mbps (half-duplex) 200Mbps (full-duplex)
4	Network Cables: 10BASE-T: UTP Cat. 3, 4, 5 (100 m) EIA/TIA-586 100-ohm STP (100 m) 100BASE-TX: UTP Cat. 5 (100 m) EIA/TIA-568 100-ohm STP (100m max.)
5	Number of Ports: 10/100Mbps port x 16
6	Twisted-pair Rx Reverse Polarity: Auto-correction for each port
7	MAC Address Learning: Automatic update
8	RAM Buffer: 4MBits per device
9	Power Supply: 100 - 240 VAC, 50/60 Hz 0.3A Internal power supply

2. Existing Hardware Items

1) Online UPS Units:

SNo.	Parameter	Specifications
1	Capacity	2 KVA ONLINE UPS
2	Back-up Time	For code OL2000
3	Inverter Type	IGBT
4	INPUT - Mains Voltage Regulation	150 - 270V AC, SINGLE PHASE
5	INPUT - Input power factor	> 0.9
6	INPUT - Frequency with Tolerance	50 Hz, +/- 3 Hz
7	INPUT - Battery (Secondary Source)	Sealed maintenance free (SMF) type – AH and no. of Batteries shall be suitably selected for the respective minimum backup time of 70% Resistive Load.
8	INPUT - DC Bus voltage	72 v / 96 v
9	INPUT - Make of the Battery	Amararaja / Exide / Leoch / Rocket / BB
10	INPUT - Battery Storage Box	External Storage Box / MS-Rack for housing the Batteries.
11	Nominal Voltage	230V AC, Single Phase (+/-1%)
12	OUTPUT - Frequency	50 Hz, +/-(0.2) Hz

13	OUTPUT - Waveform	Pure Sine wave
14	OUTPUT - Load power factor	0.7 lag to unity
15	OTHER / GENERAL DATA - Overload Capacity	Overload Capacity: Withstand for 5 Minutes at 110% load

2) UPS Batteries:

SNo.	Parameter	Specification
1	Type	12V/42AH SMF Battery
2	Number	6
3	Typical Recharge Time	6 - 8 Hrs
4	Protection	Battery Deep Discharge, Reverse Polarity, DC Overvoltage

3) Servers:

SNo.	Specifications
1	Make: IBM systemX3550 M3 Model: 7944-D4A Processor: Intel(R) Xenon® E5620 @ 2.40 GHz (4Core*2 CPU=8 Core Processor) RAM: 64 GB Hard Disk: 2* 300 GB & 2* 1 TB, 4*1 TB
2	Make: IBM systemX3550 M3 Model: 7944-D4A Processor: Intel(R) Xenon® E5620 @ 2.40 GHz (4Core*2 CPU=8 Core Processor) RAM: 128 GB Hard Disk: 2*300 GB
3	Make: IBM systemX3850 M5 Model: E7-4870 Processor: Intel Xeon 10C E7-4870 130W 2.40GHZ (20 Core*4CPU=80 Core Processor) RAM: 64 GB Hard Disk: 4*146 GB, 4*600 GB
4	Make: IBM systemX3850 M5

	Model: E7-4870 Processor: Intel Xeon 10C E7-4870 130W 2.40GHZ (20 Core*4CPU=80 Core Processor) RAM: 128 GB Hard Disk: 4*146 GB
5	Make: Dell PowerEdge R530 Model: R530 Processor: Intel(R) Xenon® E5-2650V4 @ 2.20 GHz (12 Core*2 CPU=24 Core Processor) RAM: 256 GB Hard Disk: 8* 1 TB
6	Make: Dell PowerEdge R930 Model: R930 Processor: Intel(R) Xenon® E5-2650V4 @ 2.20 GHz (12 Core*2 CPU=24 Core Processor) RAM: 512 GB Hard Disk: 3*1 TB
7	Make: Dell PowerEdge R840 Model: R840 Processor: 2 x Intel Gold 6148 (20 Core) RAM: 512 GB Hard Disk: 3 x 600 GB SAS 10K SFF

8. Annexures

8.1 Annexure 1 – Request for Clarification

Pre-Bid Queries for RFP for Selection of System Integrator for Supply, Design, Development, Implementation and Maintenance of CCTNS 2.0

Name of Company (Bidder)					Mobile No:		
Contact Person Name:					Email ID:		
SNo.	RFP Reference				Description of the Clause	Amendment Requested	Reason for requesting the Amendment
	Volume No.	Page No.	Section No.	Clause No.			
1							
2							
3							
4							

Note: - The Pre-Bid Queries for RFP must be submitted through electronic mode in editable .xls/ .xlsx format only**.**

8.2 Annexure 2 - Sample Submission Form

Date of submission: __/___/____

Bidder Name:

Bidder Address:

Tender No.:

Sample Submitted On:

Tender Product Sl No.:

SNo.	Hardware Items	Item Description	Make	Model	Serial No. of the Item

Bidder	ELCOT
Bidding Company Name:	Name & Designation of the Person Receives the Sample:
Signature of the Representative:	Store I/C Name & Designation:
Name:	Signature:
Designation:	
Contact No.	

8.3 Annexure 3 – Pre – Qualification Proposal

1. Bidder should submit the Pre-Qualification Proposal, as per the below formats otherwise the proposal is liable for rejection.

2. Bidder shall provide requisite documentary proof for all proposal criteria otherwise the proposal is liable for rejection.

1. Format 1: General

a. Profile of the Bidder

Bidder should provide brief (maximum five page) description about their organization.

b. Contact Details

1	Name of the Company	
2	Address of the Company	
3	Name of the Authorized Signatory to whom all references shall be made regarding this RFP	
4	Designation of the Authorized Signatory	
5	Address of the Authorized Signatory	
6	Telephone/ Mobile of the Authorized Signatory	
7	E-mail ID of the Authorized Signatory	

2. Format 2: Power of Attorney

Power of Attorney (PoA) by Authorized Signatory of Bidder authorizing a staff to sign and submit the Bid and execute the Contract (if selected as a successful bidder) on behalf of the Bidder

<To be on non-judicial stamp paper of Rupees One Hundred Only (INR 100/-)>

Know by all men by these presents, We……. (Name of the Bidder and address of their registered office) do hereby constitute, appoint and authorize Mr. / Ms…… (name and residential address of Power of attorney holder) who is presently employed with us and holding the position of ……. as our Attorney, to do in our name and on our behalf, all such acts, deeds and things necessary in connection with or incidental to our Proposal for

Selection of System Integrator for Supply, Design, Development, Implementation and Maintenance of CCTNS 2.0 including signing and submission of bid, executing the contract (if selected as a Successful Bidder) and providing information / responses to ELCOT/ SCRB, representing us in all matters before SCRB in connection with our Proposal for the said Project.

We hereby agree to ratify all acts, deeds and things lawfully done by our said Attorney pursuant to this Power of Attorney and that all acts, deeds and things done by our aforesaid Attorney shall and shall always be deemed to have been done by us.

For

_____

Name:

Designation:

Date:

Time:

Seal:

Business Address:

Accepted,

…….. (Signature)

(Name, Title and Address of the Attorney)

3. Format 3: Blacklisting

Declaration of not being banned or blacklisted by State/ Central Government/ Public Sector Undertaking/ Statutory Boards/ Local Bodies of any State.

<To be printed on the Bidder's Letter head>

<Location, Date>

To,

The Managing Director

Electronics Corporation of Tamil Nadu Limited

692 Anna Salai, MHU Complex, II Floor,

Nandanam, Chennai-600035

Dear Sir,

Ref: Tender for Selection of System Integrator for Supply, Design, Development, Implementation and Maintenance of CCTNS 2.0.

Sub: Declaration of not being banned or blacklisted by State/ Central Government/ Public Sector Undertakings/ Statutory Boards/ Local Bodies of any State.

I, authorized representative of _____, hereby solemnly confirm that we are not under a declaration of in-eligibility for corrupt, fraudulent or any other unethical business practices and not debarred or blacklisted by State/ Central Government/ Public Sector Undertakings/ Statutory Boards/ Local Bodies of any State for any reason in the last 3 years from the date of the response to this Tender.

In the event of any deviation from the factual information/ declaration, ELCOT reserves the right to reject the proposal or SCRB reserves the right to terminate the Contract without any compensation.

Yours faithfully,

Signature of the Authorized Signatory:

Name and Designation of the Authorized Signatory:

Company Seal:

Place:

Date:

Business Address:

Note:

1. Declaration in the company's letter head should be submitted as per format given above.
2. If the bidding firm has been blacklisted by State/ Central Government/ Public Sector Undertakings/ Statutory Boards/ Local Bodies of any State earlier, then the details should be provided.

4. Format 4: OEM Authorization

(This form has to be provided by the hardware OEMs in their letter head)

<Location, Date>

To,

Managing Director

ELCOT, II Floor MHU Complex

692 Anna Salai, Nandanam,

Chennai-600035.

Dear Sir,

Ref: Tender for Selection of System Integrator for Supply, Design, Development, Implementation and Maintenance of CCTNS 2.0

Sub: Authorization of <company name of System Integrator> to provide services based on our product(s)

I/We, _____ who are established, and reputable manufacturers of hardware items (Desktop/Printers/UPS/Inverter/Ext. HDD/ Server). I/We do hereby authorize M/s _____ *(Name and address of Bidder)* to have due authorization from us to provide services that are based on our product(s) listed below as per Request for Proposal (RFP) document relating to Selection of System Integrator for Implementation for Design,

Development, Implementation and Maintenance of CCTNS 2.0, submit a Bid, and sign the contract with you against the above Bid Invitation.

We hereby extend our full guarantee and warranty for the hardware items supplied under this RFP. We will provide the necessary spares support in the event of replacement of any spare parts is necessitated during operation & maintenance phase or any Extended Period. We also hereby certify that the proposed products for this project are not end of life & we shall continue to support the supplied product till end of contract period of the _____(Name of the Bidder).

We hereby declare that we are not insolvent, in receivership, bankrupt or being wound up, our affairs are not being administered by a court or a judicial officer, our business activities have not been suspended and we are not the subject of legal proceedings for any of the foregoing.

We duly authorize the Bidder to act on our behalf in fulfilling all installations, Technical support and maintenance obligations required by the contract.

Yours faithfully,

Signature of the Authorized Signatory:
Name and Designation of the Authorized Signatory:
Company Seal:
Place:
Date:
Business Address:

Note: - This letter of authority should be on the letterhead of the manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer. The Bidder in its Bid should include it.

5. Format 5: Undertaking to establish local office in Chennai

<To be printed on the Bidder letter head>

<Location, Date>

To,

Managing Director
ELCOT, II Floor MHU Complex
692 Anna Salai, Nandanam,
Chennai-600035.

Dear Sir,

Ref: Tender for Selection of System Integrator for Supply, Design, Development, Implementation and Maintenance of CCTNS 2.0

Sub: Undertaking for setting up the local office in Chennai, Tamil Nadu

I, authorized representative of _____, hereby confirm that the Company has no local office in Chennai, Tamil Nadu. I hereby confirm that, if selected as successful bidder, we will be opening an office in Chennai, Tamil Nadu within 30 days of issuance of Letter of Acceptance (LOA).

I/ We _____ understand that if this information / declaration is found to be false or incorrect, State Crime Record Bureau (SCRB) reserves the right to reject the proposal or terminate the Contract with us immediately without any compensation.

Yours faithfully,

Signature of the Authorized Signatory:

Name and Designation of the Authorized Signatory:

Company Seal:

Place:

Date:

Business Address:

6. Format 6: Manpower Strength

(Self-Declaration of IT Professional Strength by the Bidder)

<To be printed on the Bidder's Letter head>

<Location, Date>

To,

Managing Director

ELCOT, II Floor MHU Complex

692 Anna Salai, Nandanam,

Chennai-600035.

Dear Sir,

Ref: Tender for Selection of System Integrator for Supply, Design, Development, Implementation and Maintenance of CCTNS 2.0

Sub: Self-Declaration of IT Professional Strength

I as Bidder, confirm that our company _____, has more than _____ technically qualified IT professionals having experience in Software development, System & Database Administration, Project Management on our pay rolls in India as on 31st March 2020.

I understand that if this information / declaration is found to be false or incorrect, ELCOT reserves the right to reject the proposal or SCRB reserves the right to terminate the Contract with us immediately without any compensation.

Yours faithfully,

Signature of the Authorized Signatory:
Name and Designation of the Authorized Signatory:
Company Seal:
Place:
Date:
Business Address:

7. Format 7: Declaration of No Conflict of Interest

<To be printed on the Bidder letter head>

<Location, Date>

To,
Managing Director
ELCOT, II Floor MHU Complex
692 Anna Salai, Nandanam,
Chennai-600035.

Dear Sir,

Ref: Tender for Selection of System Integrator for Supply, Design, Development, Implementation and Maintenance of CCTNS 2.0

Sub: Undertaking of No Conflict of Interest

I/We as Bidder do hereby undertake that there is, absence of, actual or potential conflict of interest on our part, due to prior, current, or proposed contracts engagements, or affiliations with State Crime Record Bureau (SCRB).

I undertake and agree to indemnify and hold NCRB/ MHA/ State Crime Record Bureau (SCRB) harmless against all claims, losses, damages, costs, expenses, proceeding fees of legal advisors (on a reimbursement basis) and fees of other professionals incurred (in the case of legal fees & fees of professionals, reasonably) by State Crime Record Bureau (SCRB) and/or its representatives, if any such conflict arises later.

Yours faithfully,

Signature of the Authorized Signatory:
Name and Designation of the Authorized Signatory:
Company Seal:
Place:
Date:
Business Address:

8.4 Annexure 4 – Technical Qualification Proposal

Instructions:

a. Bidder should submit the Technical Qualification Proposal, as per the below formats otherwise the proposal is liable for rejection.
b. Bidder shall provide requisite documentary proof for all proposal criteria otherwise the proposal is liable for rejection.
c. For each project where such details are not explicitly stated in the Work order, a Client Certificate declaring these details should be submitted in addition to the Word Order.

1. Format 1: Prior Project Experience

a. System Integration Experience

Ref. No.	Name of the Project and Client Name	Month and Year of Commence of the Project	Project Value (INR Crores)	Month and Year of Roll-Out/ Completion	Number of Internal Users	Number of Locations	Work Order(s)	Client Certificate

b. Application Development Experience

Ref. No.	Name of the Project	Month and Year of Commence	Project Value (INR	Value of Application Development/ Customization/	Scope of the Work	Month and Year of Roll-Out/	Work Order(s)	Client Certificate

	and Client Name	of the Project	Crores)	Maintenance work (INR Crores)		Completion		

c. Experience in Supply & Installation of Hardware

Ref. No.	Name of the Project and Client Name	Month and Year of Commence of the Project	Project Value (INR Crores)	Value of Hardware items supplied (INR Crores)	No of years of O& M completed	Work Order(s)	Client Certificate

d. Experience in Police Department

Ref. No.	Name of the Project and Client Name	Month and Year of Commence of the Project	Project Value (INR Crores)	Scope of Work	Month and Year of Roll-Out/ Completion	Work Order(s)	Client Certificate

e. Experience in Training & Capacity Building

Ref. No.	Name of the Project and Client Name	Month and Year of Commence of the Project	Project Value (INR Crores)	Number of users trained	Total duration of the training	Work Order(s)	Client Certificate

2. Format 2: Approach & Methodology

a. Solution Architecture conceptualized for the project

Bidder shall submit the following documents pertaining to the proposed solution design;

- Overall system architecture
- Application architecture
- Database Architecture
- Security Architecture
- Other Architecture

b. Proposed methodology for application development/ customization & implementation

Bidder shall provide detailed methodology for application development/ customization & implementation, Site Preparation, Hardware Supply and Installation keeping in view the minimum requirements mentioned in the RFP.

c. Approach for Setting up O & M of Helpdesk to meet the SLA requirement

Bidder shall provide the detailed understanding of the project SLA requirements, SLA management methodology, approach for carrying out the activities for expected output.

d. Strategy for Implementation Roll-Out

Full-Scale Rollout Strategy:

Bidder shall provide in detail approach and methodology that will be adopted by the Bidder to ensure smooth and timely rollout of the proposed solution. The Approach and methodology should clearly indicate the following:

- Structure of the team proposed with details of the size of team, experience of team, onsite/offsite breakup of effort for various teams / team- members. This should not be limited to the Key resources whose CV has been sought but rather provide a comprehensive coverage of all key teams involved in solution deployment
- Development team, testing team etc.

- Detailed work plan clearly identifying Key Tasks, timelines, internal and external dependencies
- Approach for transition of the system from the current to Proposed System

Operations & Maintenance post Full Scale Rollout:

Please provide in detail the approach and methodology that will be adopted by the Bidder to ensure operations and maintenance of the proposed solution. The Approach and methodology should clearly indicate the following:

- Structure of the team proposed with details of the size of team, experience of team, onsite/offsite breakup of effort for various teams / team- members.
- Approach to meeting and monitoring SLAs
- Approach to Incident Management

3. Format 3: Proposed Team and Governance Structure

Instructions:

a. Only 1 CV must be provided for each profile mentioned.
b. In case no CVs are proposed for any of the specified positions, nil marks will be awarded.
c. For lesser experience, marks will be given on prorate basis
d. CVs of all key resources proposed **MUST** be furnished in the format given below **(Max 4 pages per CV)**. Missing information in the specified format would amount to rejection of the CV for evaluation, at the discretion of the ELCOT.
e. Each CV shall be signed by the authorized Signatory of the Bidder.
f. ELCOT at its discretion, request the Bidder to provide additional details with respect to any or all of the personnel proposed, if required during the evaluation process.
g. ELCOT reserves the right to interview the personnel proposed, if found unsuitable, ELCOT/ SCRB reject the deployment of the personnel for this project.

a. Team Composite

Team Composition details						
Position Assigned	**Name of Staff**	**Qualification**	**Experience**	**Area of Expertise**	**Tasks Assigned**	**Time committed for**

						the engagement

b. Curriculum Vitae (CV) of Key Personnel

Personal Details	
Name	
Proposed Position	
Date of Birth	
Years with Organization (If applicable)	
Nationality	
Education	
Degree (Specialization)	
Relevant Certificate (If any)	
Languages & Degree of Proficiency	
Countries of Work Experience	
Employment Record	

Employer	From	To
Detailed Tasks Handled (Domestic & International)		
Name	Brief Description of Assignment	
Certifications		
I, the undersigned certify that:		
To the best of my knowledge and belief, this CV correctly describes me, my qualifications and my experience.		
I understand that my willful misstatement described herein may lead to my disqualification or dismissal, if engaged.		
Name & Signature (Personnel)	Name & Signature (Authorized Signatory)	
	Date of Signing	

c. Deployment of Personnel

The Bidders are required to substantiate their approach & methodology using the formats below:

Till Rollout:

#	Role / Designation	No. of Resource	Name of Staff	Total Proposed Effort (in Man-month) of Resources								Total staff man-months proposed
				M1	M2	M3	M4	M5	M6	M7	MN	Total
1												
2												
3												
N												
Total												

Post Rollout:

#	Role / Designation	No. of Resource	Name of Staff	Total Proposed Effort (in Man-month) of Resources								Total staff man-months proposed
				M1	M2	M3	M4	M5	M6	M7	MN	Total
1												
2												
3												
N												
Total												

With respect to the above formats, the Bidders are requested to note the following:

1. For Key Professional sought in the Proposal, the input should be indicated individually. For others, it may be indicated by category (e.g. Development team)
2. Effort should be indicated in man-months. Clear distinction to be made between onsite effort (at the project location) or offsite effort
3. Bidder may add any additional profile in the resource deployment plan above if required

d. Undertaking on Key Personnel proposed for the Project

<To be printed on the Bidder letter head>

<Location, Date>

To,

Managing Director

ELCOT, II Floor MHU Complex

692 Anna Salai, Nandanam,

Chennai-600035.

Dear Sir,

Ref: Tender for Selection of System Integrator for Supply, Design, Development, Implementation and Maintenance of CCTNS 2.0

Sub: Undertaking on Key Personnel proposed for the Project

1. I/We, as Bidder do hereby undertake that those persons whose profiles were part of the basis for evaluation of the proposals (**Project Manager, Technical Solution Architect, Data Center Expert, Service Desk Expert, Infrastructure Expert**), hereby referred to as "Key Personnel" of the proposed team, shall be deployed during the Project as per our Bid submitted in response to the RFP.
2. We undertake that all of the identified "Key Personnel" will be based out of Bidder's Chennai office atleast till the Full Scale Roll out of the project.
3. We undertake that any of the identified "Key Personnel" shall not be removed or replaced without the prior written consent of State Crime Record Bureau (SCRB).

4. Under exceptional circumstances, if the key personnel are to be replaced or removed, we shall put forward the profiles of personnel being proposed as replacements, which will be either equivalent or better than the ones being replaced. However, whether these profiles are better or equivalent to the ones being replaced will be decided by State Crime Record Bureau (SCRB).
5. State Crime Record Bureau (SCRB) will have the right to accept or reject these substitute profiles.
6. We also undertake to staff the Project with competent team members in case any of the proposed team members leave the Project either due to voluntary severance, disciplinary actions against them or any other reason.
7. We acknowledge that State Crime Record Bureau (SCRB) has the right to seek the replacement of any member of the Project team being deployed by us, based on the assessment of State Crime Record Bureau (SCRB) that the person in question is incompetent to carry out the tasks expected of him/her or found that person does not really possess the skills /experience/qualifications as Projected in his/her profile or on the ground of security concerns or breach of ethics.
8. In case we assign or reassign any of the team members, we shall be responsible, at our expense, for transferring all appropriate knowledge from personnel being replaced to their replacements within a reasonable time. We shall also ensure that such replacements do not adversely impact the quality and timeliness of the Project at any time.

Thanking you,

Yours faithfully

Authorized Signatory's (Bidder) Signature:

Authorized Signatory's Name and Designation:

Bidder's Company Seal:

Place:

Date:

Business Address:

4. Format 4: Project Plan

a. Envisaged Objectives and Outcomes of the Project

Please provide detailed envisaged objectives and outcomes of the project keeping in view the minimum requirements mentioned in the RFP.

b. Detailed Project Plan including week wise activities with Work Breakdown Structures

Work Breakdown Structure										
SNo.	Activity[1]	Months								Month N
		W1	W2	W3	W4	W5	W6	W7	W8	WN
1										
2										
3										
4										
5										
N										

1. Indicate all main activities of the assignment, including delivery of reports (e.g.: inception, interim, and final reports), and other benchmarks such as Purchaser approvals. For phased assignments indicate activities, delivery of reports, and benchmarks separately for each phase.
2. Duration of activities shall be indicated in the form of a bar chart.

c. Risk Management & Mitigation plan

Highlight the associated risks / problems and plans for mitigation and explain the technical approach it would adopt to address them

Risks / problems	Mitigation Plan	Technical Approach

5. Compliance to Minimum Hardware Specification

1) Desktop:

SNo.	Parameters	Minimum Specifications	Offered Specifications	Compliance (Yes/No)
1	Processor	Intel Core i5-10th generation (3.0 Ghz) or higher		
2	Memory	8GB DDR4 SDRAM@2666 MHz with minimum 2 DIMM slots, upgradeable up to 32 GB, Onboard memory is not acceptable		
3	Motherboard	OEM Motherboard		
4	Slots	Min 2 PCI/PCI Express Slots		
5	Network port	1000 BaseT, Gigabit Ethernet with remote booting facility, RJ45, Wi-Fi 802.11 AC or Above, Bluetooth 5.0 or Above.		
6	USB Ports	Min 6 USB Ports (out of that 2 must be in front) with at least two with 3.0		
7	Display Port	Display Port (DP), HDMI Port		
8	Audio	Line/Mic In, Line-out/Speaker Out (3.5 mm)		
9	Hard Disk Drive	Minimum 1 TB SATA Hard Disk @7200 RPM or higher		
10	DVD Drive	DVD Writer		
11	Keyboard	Minimum 104 keys Heavy Duty Mechanical Switch Keyboard (USB Interface). Rupee		

		Symbol to be engraved.		
12	Mouse	Optical with USB interface (same make as desktop)		
13	Monitor	Minimum 21.5” diagonal LED Monitor with 1366x768 or higher resolution. (Same make as desktop). Must be TCO05 certified		
14	Bays	2 Bays or more		
15	General Certification	Hazardous - RoHS, Energy efficient - Energy star, Safety - CE / UL, Environment – EPEAT, MIL - STD 810G test passed, ISO 9001:2008 OEM certification or better		
16	Operating System	Linux		
17	Office Application	Open Office Suite		
18	OS Compliance	Windows & Linux		
19	OS Certification	MS Windows and Boss Linux.		
20	Security	Discrete TPM 2.0(Hardware), Tool less Chassis with intrusion switch		

2) Online UPS with Battery (2KVA):

SNo.	Parameters	Minimum Specifications	Offered Specifications	Compliance (Yes/No)
1	Capacity	2 KVA TRUE ONLINE UPS		
2	Back-up Time	60 Minutes with 70% Resistive Load		

3	Inverter Type	IGBT (Make and current capacity to be specified by the tenderer)		
	Input			
4	Input Voltage Range	150 - 270V AC, SINGLE PHASE		
5	Input power factor at Full Load	>0.9		
6	Input Frequency with Tolerance	40 Hz to 70 Hz		
7	Battery (Secondary Source)	1. Sealed maintenance free (SMF) type – AH and no. of Batteries shall be suitably selected for the respective minimum backup time of 70% Resistive Load, 60 Minutes – 3160 VAH.		
8	DC Bus voltage	To be specified by the tenderer		
9	Make of the Battery	Specify the Manufacturer Make, Model and enclose the technical specification sheet. The make and AH of the battery submitted for evaluation only will be accepted.		
10	Battery Storage Box	External Storage Box / MS-Rack for housing the Batteries.		
	Output			
11	Nominal Voltage	230V AC, Single Phase (+/-1%)		
12	Frequency	50 Hz, +/-(0.2) Hz		

13	Waveform	Pure Sine wave		
14	Load power factor at full load	0.7 lag to unity		
	Others Features			
15	Overload Capacity	Overload Capacity: Withstand for 5 Minutes at 110% load (2200 Watts Resistive Load / 1540Watts Combinational Load).		
16	Total Harmonic Distortion	< 4% for Linear load and 5% for nonlinear load		
17	Efficiency	> 80%		
18	Ambient Temperature	To be specified by the tenderer (Preferable upto 50 Degree Celsius)		
19	Duty Cycle	Continuous		
20	Cooling	Forced air cooling		
21	Protections	1) Input, Output – Low and High 2) Battery low and high voltage 3) Input, output – Fuse 4) Battery - MCB/Fuse 5) Short circuit 6) Overload 7) Lightening		
22	Controls	Manual By-pass Switch and static bypass switch to be provided with Indications		
23	Power sockets	Power Sockets – 3 Nos. of 5A Socket.		

24	Trip Conditions	Indicators for AC Mains, Load on Battery, Fault, Load Level, Battery Low Warning, Inverter On, UPS on Bypass, Overload, etc.		
25	Alarms (Audio)	Battery low, Mains Failure, Over temperature, Inverter overload, Fault, Extreme battery low voltage.		
26	Meters	Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.		
27	Manuals	Operating and User manual to be Provided		
28	Name Plate in the UPS	Name plate in UPS-Riveted metal plates / Stickers		
29	Isolation Transformer	Isolation Transformer must be provided internally / externally at input.		
30	Software	Software for automatic shutdown of the system compatible with Linux		
31	Certification	SAMEER / ETDC / NTH / ERTL / NABL's or any other Government authorized Testing Lab Certification for any back up of each UPS Category Mandatory for this specification (issued within last 6 years) ISO Certifications Mandatory - ISO 9001:2015 and ISO 14001:2015		

32	Integrated Stand	UPS along with the batteries should be accommodated in the existing integrated stand available at the respective locations. If the supplied device cannot be accommodated, then the UPS along with batteries should be supplied along with the integrated stand. The integrated stand should also have electrical panel to control the supply to UPS through a tripper switch and should have provision to tap the UPS supply.		
33	Other Features	SNMP Card - Provisions should be available Diesel Generator – Compatible		

3) Online UPS with Battery (5KVA):

SNo.	Parameters	Minimum Specifications	Offered Specifications	Compliance (Yes/No)
1	Capacity	5 KVA TRUE ONLINE UPS		
2	Back-up Time	For code OL 5000-60 – 60 minutes		
3	Inverter Type	IGBT (Make and current capacity to be specified by the tenderer)		
	Input			
4	Input Voltage Range	150 - 270V AC, SINGLE PHASE		
5	Input power factor at Full Load	>0.9		

6	Input Frequency with Tolerance	40 Hz to 70 Hz		
7	Battery (Secondary Source)	Sealed maintenance free (SMF) type – AH and no. of Batteries shall be suitably selected for the respective minimum backup time of 70% Resistive Load, 60 Minutes – 7900 VAH		
8	DC Bus voltage	To be specified by the tenderer		
9	Make of the Battery	Specify the Manufacturer Make, Model and enclose the technical specification sheet. The make and AH of the battery submitted for evaluation only will be accepted.		
10	Battery Storage Box	External Storage Box / MS-Rack for housing the Batteries.		
	Output			
11	Nominal Voltage	230V AC, Single Phase (+/-1%)		
12	Frequency	50 Hz, +/-(0.2) Hz		
13	Waveform	Pure Sine wave		
14	Load power factor at full load	0.7 lag to unity		
	Others Features			

15	Overload Capacity	Overload Capacity: Withstand for 5 Minutes at 110% load (2200 Watts Resistive Load / 1540Watts Combinational Load).		
16	Total Harmonic Distortion	< 4% for Linear load and 5% for nonlinear load		
17	Efficiency	> 85%		
18	Ambient Temperature	To be specified by the tenderer (Preferable upto 50 Degree Celsius)		
19	Duty Cycle	Continuous		
20	Cooling	Forced air cooling		
21	Protections	1) Input, Output – Low and High 2) Battery low and high voltage 3) Input, output – Fuse 4) Battery - MCB/Fuse 5) Short circuit 6) Overload 7) Lightening		
22	Controls	Manual By-pass Switch and static bypass switch to be provided with Indications		
23	Power sockets	1 No.32 Amps. Capacity Terminal Block		
24	Trip Conditions	Indicators for AC Mains, Load on Battery, Fault, Load Level, Battery Low Warning, Inverter On, UPS on Bypass, Overload, etc.		
25	Alarms (Audio)	Battery low, Mains Failure, Over temperature, Inverter overload, Fault, Extreme battery low voltage.		

26	Meters	Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.		
27	Manuals	Operating and User manual to be Provided		
28	Name Plate in the UPS	Name plate in UPS-Riveted metal plates / Stickers		
29	Isolation Transformer	Isolation Transformer must be provided internally / externally at input.		
30	Software	Software for automatic shutdown of the system compatible with Linux		
31	Certification	SAMEER / ETDC / NTH / ERTL / NABL's or any other Government authorized Testing Lab Certification for any back up of each UPS Category Mandatory for this specification (issued within last 6 years) ISO Certifications Mandatory - ISO 9001:2015 and ISO 14001:2015		

32	Integrated Stand	UPS along with the batteries should be accommodated in the existing integrated stand available at the respective locations. If the supplied device cannot be accommodated, then the UPS along with batteries should be supplied along with the integrated stand. The integrated stand should also have electrical panel to control the supply to UPS through a tripper switch and should have provision to tap the UPS supply.		
33	Other Features	SNMP Card - Provisions should be available Diesel Generator – Compatible		

4) Inverter:

SNo.	Parameters	Minimum Specifications	Offered Specifications	Compliance (Yes/No)
1	Capacity	3 KVA		
2	Back-up Time	120 Minutes		
	Input			
3	Under Voltage	150 +/- 10V		
4	Over Voltage	285 +/- 10V		
	Output			
5	Voltage (INVERTER Mode)	230 V Nominal		
6	Frequency (Mains Mode)	Same as Input		
7	Frequency (INVERTER Mode)	50 Hz. +/- 2%		
8	Frequency (Mains Mode)	Same as Input (45-55 Hz)		
9	Overload	> 110%		
10	Transfer time	10 ms		

	Battery			
11	Type	12 V/135 AH Tubular		
12	Number	4 in Series		
13	Typical Recharge Time	10-12 Hrs		
14	Protection	Battery Deep Discharge, Reverse Polarity, DC Overvoltage		
15	LED Displays	Inverter ON Battery Low Mains On Battery Charged Overload No load Over Temperature Short Circuit Under Battery Mode MCB Trip or Short Circuit under Mains Mode		
16	Alarms	Low Battery Overload Short Circuit		
	Environment			
17	Operating Temperature	0-45 degree C (32-113-degree F)		
18	Storage Temperature	0-45 degree C (32-113-degree F)		
19	Humidity	0-95% RH non-condensing		
20	Certification	SAMEER / ETDC / NTH / ERTL / NABL's or any other Government authorized Testing Lab Certification for this specification (issued within last 6 years) ISO Certifications Mandatory - ISO 9001:2015 and ISO 14001:2015		

21	Integrated Stand	Inverter along with the batteries should be accommodated in the existing integrated stand available at the respective locations. If the supplied device cannot be accommodated, then the inverter should be supplied along with the integrated stand. The integrated stand should also have electrical panel to control the supply to inverter through a tripper switch and should have provision to tap the inverter supply.		

5) Printer MFP:

SNo.	Parameters	Minimum Specification	Offered Specifications	Compliance (Yes/No)
1	Printer type	Monochrome Laser		
2	Printer Function	Print, Scan, Copy		
3	RAM Size	256 MB or higher		
4	Printer speed	Minimum 25 PPM or higher		
5	Print Resolution	Up to 1200 x 1200 dpi		
6	Duty cycle	Minimum 25000 pages or higher		
7	Duplex	Automatic		

8	Input Tray Capacity	Minimum 250 pages		
9	Bypass Tray	1 Sheet or Higher		
10	Paper size	A4, Letter, Legal		
11	Paper Types	Plain paper, envelopes		
12	Toner Type	Composite		
13	Initial Toner(s) Yield	2500 pages & above		
14	Scanner Type	Flatbed, ADF		
15	Scan Resolution	Bidder to Specify		
16	Scan file format	JPEG, PDF		
17	Scan Mode	BW & Colour		
18	Copy speed	Min. 25 ppm or higher		
19	Copy Resize	25-400%		
20	Copier Resolution	Up to 600 x 600 dpi or Higher		
21	Interface/ Connectivity	USB and Ethernet 10/100		
22	OS Compatibility	Windows, Linux		

6) Printer LP:

SNo.	Parameters	Minimum Specifications	Offered Specifications	Compliance (Yes/No)
1	Printer type	Laser		
2	Printer speed	Minimum 25 PPM		
3	Resolution	Min 1200 x 1200 dpi		
4	Memory	128 MB		
5	Network	Ethernet 10/100 Mbps or above		
6	Duty cycle	Minimum 25000 pages or higher		
7	Duplex	Automatic		
8	Input Tray Capacity	Minimum 250 pages		
9	Paper size	A4, Letter, Legal		
10	Paper Types	Plain paper, envelopes		
11	Media Types	Paper (Plain, Recycled, Envelopes, Transparencies, Labels & Card stock)		
12	Interface/ Connectivity	USB and Ethernet		
13	OS Compatibility	Windows and Linux		
14	Toner cartridge - Yield	Yield of minimum 1500 pages		

7) Ext. HDD:

SNo.	Parameters	Minimum Specifications	Offered Specifications	Compliance (Yes/No)
1	Capacity	1TB		
2	Type	External		
3	Interface	USB 3.0 & USB 2.0		
4	Spindle Speed	5400 RPM		
5	Transfer Rate	100-200 MB/s		
6	OS Compatibility	Windows and Linux		

8) Server Specifications

SNo.	Parameters	Minimum Specifications	Offered Specifications	Compliance (Yes/No)
1	Processor	Latest series/ generation of 64-bit x86/ equivalent processor(s) with 16 or higher Cores Processor speed should be minimum 2.9 GHz and minimum 3.9 GHz turbo frequency, minimum 22MB Cache having SPEC Rate 2017_fp_base of 228 or Higher and SPEC Rate 2017_fp_base of 252 or Higher Minimum 2 processors per each physical server		
2	RAM	16 x 32 GB RDIMM scalability upto 1 TB. Proposed memory should have ECC support.		

3	Network interface	4 * 1 GB Ethernet Ports 2 * 10 GB Ethernet Ports 1* 16 Gbps Dual port FC HBA Card		
4	Power supply	Hot-pluggable 1 + 1 redundancy		
5	RAID support	12G SAS H/W Raid controller, which supports RAID: 0/1/5/10 with 2GB Flash Backed Cache		
6	Hard Disk Drive	2X600GB 12G SAS 15K SFF Or Higher, Hot Plug expandable upto 8 Nos or Higher		
7	Operating System	Licensed version of 64-bit latest version of Linux/ Unix		
8	Form Factor	2U Rack Mountable		
9	System Fans	Redundant & Hot Plug Fans		
10	Interfaces/PCI Slots	Minimum 4 PCI slots		
11	Pre-Failure Notification	Failure – Failure notification on HDD, Processor & Memory		
12	Industry Standard Compliance	PCIe3.0 Compliant, PXE Support, USB 3.0 Support		
13	Security	Power-on password / Keyboard password / Administrator's password, Hardware-based system security feature that can securely store information, such as passwords and encryption keys, which can be used to authenticate the platform.		
14	Benchmarks	SPEC int benchmark for the quoted processor models should be submitted either along with the bid or shall be submitted within 15 days from the date of submission of Bid.		
15	Virtualization	Shall support Industry standard virtualization hypervisor		

9) CAT 6 Cables:

SNo.	Parameters	Minimum Specifications	Offered Specifications	Compliance (Yes/No)
1	Cable Type and support	4 Pair Twisted Cable, Support for Fast and Gigabit Ethernet, IEEE 802.3/5/12, Voice, ISDN, ATM 155 & 622Mbps. Should be Tested up to 550Mhz		
2	Conductor	23 AWG Annealed bare solid copper		
3	Insulation	High Density Polyethylene		
4	Approx. Cable OD	6.3 mm.		
5	Core Color	Fire Retardant PVC Compound (FRPVC) Pair 1: White – Blue Pair 2: White – Orange Pair 3: White – Green Pair 4: White – Brown		
6	Pair Separator	4 twisted pairs separated by internal X shaped, 4 channel, polymer spine / full separator. Half shall not be accepted.		
7	Sheath	Fire Retardant PVC Compound (FRPVC)		
8	Sheath Colour	Grey / Blue		
9	Flame Rating	60 deg. C As per UL 1685 CM		

10	Operating Environment	Indoor		
11	Electrical Specification	@ 250 MHz		
12	Standards	TIA / EIA 568 C.2		
13	Impedance	100Ohms +/- 15%		
14	(NVP) Velocity of Propagation	69% or more @ 250 MHz Approx.		
15	Delay Skew	45 ns /100 mtrs. max. @ 20 deg. C, for 1 MHz~250 MHz Approx.		
16	Propagation Delay	<=536 ns / 100 mtrs. max. @ 20 deg. C, @ 250 MHz		
17	DC Resistance	<= 9.38 ohm / 100 mtrs. max. @ 20 deg. C		
18	Mutual Capacitance	5.60 nF / 100 mtrs. max. Approx.		
19	Safety	UL Listed		

10) Connection Module:

SNo.	Minimum Specifications	Offered Specifications	Compliance (Yes/No)
1	RJ45 connection module of Category 6, for the establishing of transmission channels of class E with up to 4 plugged connections, complies with Category 6 requirements of the standards ISO/IEC 11801:2002, EN 50173-1: May 2007, DIN EN 50173-1: Dec. 2007 as well as ANSI/TIA/EIA 568-B.2-1, de-embedded tested in acc. with IEC 60603-7-4, interoperable and backwards compatible with Cat.5e and Cat.5.		

2	Suitable for 10GBase-T applications in acc. with IEEE 802.3an up to 500 MHz and 55 m.		
3	Parallel pair termination without crossover in acc. with EIA/TIA 568-A/B, gold-plated bronze contacts for >1000 mating cycles, IDC contacts with single-wire strain relief and >20 insertion cycles, contact resistance <50 m Ohm, dielectric strength >1000 Veff.		
4	Maximum reliability through special contact design without internal transfer points.		
5	Should have integral dust cover and integrated bend-limiting strain -relief unit for cable entry.		
6	Should have IDC to hold conductor without using any tool for termination of cable.		
7	Outlets should be of single metal piece design without any PCB to support the IDC / Contacts.		
8	Should be reusable and tool less in design in terms of termination of solid wire installation cable AWG22-24 as well as stranded cables AWG 22/7 – 26/7.		
9	Should be made of halogen free material and should be certified by third party like 3P or Delta or GHMT.		

11) Patch Panel:

SNo.	Minimum Specifications	Offered Specifications	Compliance (Yes/No)
1	Patch panel with integrated cable tie shelf, 19" fastening kit, labeling field, accepting the snap-in type color coding clips in 8 colors.		
2	Material: sub-rack made of sheet steel (DC01A) 1.5 mm, color blue achromatized, screen made of plastic (ABS), halogen-free, color medium gray (NCS 2502-B)		

3	Complies with Category 6 requirements of the standards ISO/IEC 11801:2002, EN 50173-1: May 2007, DIN-EN 50173-1: Dec. 2007 as well as ANSI/TIA/EIA 568-B.2-1, de-embedded tested in acc. with IEC 60603-7-4, interoperable and backwards compatible with Cat.5e and Cat.5.		
4	Suitable for 10GBase-T applications in acc. with IEEE 802.3an up to 500 MHz and 55 m in case of unshielded.		
5	Each port should be individually terminated i.e. each Port should be individually replaceable & provide consistent port-to-port performance.		
6	Each port should have an integral dust cover and integrated bend-limiting strain relief unit for cable entry.		
7	Patch panels shall be modular in design and capable of supporting Cat 6 UTP/FTP and S/FTP modules on same port. The same panel should have the capability of terminating multimode and single mode fibers alongside the copper terminations.		

12) Patch Cord:

SNo.	Parameters	Minimum Specifications	Offered Specifications	Compliance (Yes/No)
1	Type	Factory Crimped Cat6 UTP Patch cord with 24 AWG 7/32 Round stranded copper wire.		
2	Length	1 Meter		
3	Insulation	Polyethylene		
4	Cable sheath	CM grade PVC Plug insertion		

5	Durability	1000 mating cycles		
6	Plug tensile strength	89 N, Plug insulation		
7	resistance	>500MW		
8	Contact resistance	10 mW		

13) Network & Server Racks:

SNo.	Minimum Specifications	Offered Specifications	Compliance (Yes/No)
1	Feature: 42U 800W X 800D Modular Structures made from aluminum extruded profile, minimum extrusion wall thickness at all sides and corner- 2mm, along with following items: Top and Base Cover with cable enter Black Color.		
2	Front/Rear Door: Front, Glass door, 800mm Wide, 42U, with Lock and hexagonal vent on the trims for thermal Management/ air cooling. 42U, 800mm W, Rear Steel Door, with 1/3 hexagonal vent at the base to allow proper air flow and thermal control, with Lock		
3	Mounting Angles: 19" Mounting Angles, 19" mounting angles powder coated along with "U" marking		
4	Side Panels: 2 Nos. of Removable Side Panels along with slam latch. 4 nos. of 100mm W, Reducing Cable channels on the sides to allow better cable management		
5	Castors: Castors - For providing mobility to the rack. Two with foot operated brakes and Two without		

	brakes, having a load carrying capacity of 100kg		
6	Fan: 230V AC 90CFM Fan (4 nos. for each Rack) with Fan Housing Unit.		
7	Cable Manager: 19", 1U, Horizontal Cable Manager, to allow proper cable routing		
8	Cable Loops: 24U to help route the cable vertically		
9	Power Supply: 10X 5 amps or 6 X 5 amps socket as per requirement		
10	Castors: Castors as needed		
11	Cable Storage: 2U cable storage shelf supported with 4 bobbins		
12	Power Consumption: Not more than 5 KVA		
13	Redundancy: Mechanical Devices such as Hard Disks, Fans and Power Units should be completely Hot Swappable and Redundant to ensure High Availability		
14	Power Guaranteeing complete availability even on failure of any 2 power units across the enclosure. Sufficient Power to run a fully loaded enclosure in N+N redundant mode.		
15	KVM/CD/USB/Floppy To be enabled Virtually over IP for Remote Access or Provided Locally.		
16	Multi-platform Support: Enclosure should support Xeon & RISC/EPIC blade on the Same chassis. Enclosure should also support Unix, Linux and Windows Operating environment		

14) Network Switch (Managed):

SNo.	Minimum Specifications	Offered Specifications	Compliance (Yes/No)

1	Interface Ports: 16 10/100/1000BASE-T Auto-negotiating, Auto-MDI/MDI-X ports with 802.3x Flow Control		
2	Performance Switch Capacity: 32Gbps		
3	Packet Forwarding Rate: 23.8Mpps or above		
4	MAC Address Table Size: 8K		
5	MAC Address Update: Up to 256 static MAC entries Enable/disable auto-learning of MAC addresses		
6	Packet Buffer: 512KB		
7	Power Input: 100 to 240 VAC 50/60Hz Internal power supply		
8	Port Standards and Functions: IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Gigabit Ethernet (fiber) ANSI/IEEE 802.3 IEEE 802.3x Flow Control Auto-Negotiation 802.3af Power over Ethernet		
9	LAYER 2 Features: IGMP v1/2 Snooping: supports 64 multicast groups 802.1D Spanning Tree Static Port Trunk (Link Aggregation): up to 6 group per device, up to 8 ports per group		
10	VLAN: 802.1Q VLAN (VLAN Tagging) Up to 256 static VLAN groups Management VLAN Asymmetric VLAN		

11	Quality of Service (QoS): 802.1p Priority Queues Up to 4 queues per port DSCP-based QoS		
12	Security: 802.1X Port-based Access Control Broadcast Storm Control Trusted Host Cable Diagnostics function		
13	Management: Web-based GUI SNMP v1 support DHCP Client Trap setting for destination IP, system events, fiber port events, twisted-pair port events. Port Access Control Web-based: Configuration backup/ restoration Web-based: Firmware backup/upload System Reboot using web-based interface		

15) Network Switch (Unmanaged):

SNo.	Minimum Specifications	Offered Specifications	Compliance (Yes/No)
1	Standards: IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet ANSI/IEEE 802.3 NWay auto negotiation		
2	Protocol: CSMA/CD		
3	Data Transfer Rates: Ethernet: 10Mbps (half-duplex) 20Mbps (full-duplex) Fast Ethernet: 100Mbps (half-duplex) 200Mbps (full-duplex)		

4	Network Cables: 10BASE-T: UTP Cat. 3, 4, 5 (100 m) EIA/TIA-586 100-ohm STP (100 m) 100BASE-TX: UTP Cat. 5 (100 m) EIA/TIA-568 100-ohm STP (100m max.)		
5	Number of Ports: 10/100Mbps port x 16		
6	Twisted-pair Rx Reverse Polarity: Auto-correction for each port		
7	MAC Address Learning: Automatic update		
8	RAM Buffer: 4MBits per device		
9	Power Supply: 100 - 240 VAC, 50/60 Hz 0.3A Internal power supply		

8.5 Annexure 5 – Commercial Proposal

1. Proposed Bill of Material

a. Hardware Requirements:

SNo.	Item description	Item procured by Bidder	
		Make	Model
A	**Field Assets**		
1	Desktop		
2	UPS Units		

SNo.	Item description	Item procured by Bidder	
		Make	Model
3	UPS Batteries		
4	Printer - MFP		
5	Printer - LP		
6	Inverter		
7	Ext. HDD		
B	**Site Infrastructure**		
1	Network CAT 6 UTP Cable		
2	CAT6 Information outlet		
3	Back box and Face plate		
4	Electrical cable 2.5 sq.mm wire (Mtr)		
5	Electrical cable 1.5 sq.mm wire (Mtr)		

SNo.	Item description	Item procured by Bidder	
		Make	Model
6	Electrical cable 4 sq.mm wire (Mtr)		
7	25 mm PVC for UTP CAT -6 data (Mtr) cabling (Clamp, Screw, L and T Bend)		
8	15 or 25mm PVC for electrical (Mtr) cabling (Clamp, Screw, L and T Bend)		
9	Power socket -5amp socket with (no's) switch		
10	Power socket -5/15amp SS Combined		
11	32 Amps MCB (Dual Pole) with Metal Box		
12	Copper wire/strip for earthing		
13	Earth Rod (5ft)		
14	Wall Mount 9 U Rack with Delivery (Power panel, Cooling Fan)		
15	16 Port Switch Unmanaged		
16	16 Port Jack Panel Unloaded		

SNo.	Item description	Item procured by Bidder	
		Make	Model
17	1 Mtr Patch Cord		
18	2 Mtr Patch Cord		
C	**Data Center / Disaster Recovery Center**		
1	Web/ Application Servers		
2	Database Servers		

Note:

The Bill of Material for hardware items is mentioned based on the existing Police Stations, Higher Offices, Special Units & Training centres in the state. The SI shall supply hardware items at the same quoted price to any new Police Stations that may come up in the state during the three phases of supply. The Operations & Maintenance expenses for hardware items supplied to the new Police Stations shall be calculated on a pro rata basis.

b. Software Application:

SNo.	Item Details
1	**Core Modules**
a	FIR Registration
b	Investigation
c	Prosecution

d	CSR
e	Regulatory Framework
2	**Tools on CCTNS platform**
a	Missing Person UIDB tool
b	History Sheets
c	Station Crime History
d	Bandobast Manager
e	Citizen & Officers Portal
f	DMU Mapping
g	Mobile Application Development
h	Unified Calendar
3	**Core Admin Module**
a	Form Builder
b	Report Builder
c	Nominal Roll Application
d	Query Builder
e	Dashboard Builder
f	System Diagnostic Tool
g	Admin Rights and Privileges

h	User Role & Privileges
i	Master Data Management
j	Data Capture & Validation
k	Platform Usage Analytics
l	Communication Module
4	**Integration with SCRB Applications**
a	e-Beat System
b	Crime Analytics Tool
c	Facial Recognition
d	Tollscope
e	Fingerprint Database
5	**Integration with Central Systems**
a	ICJS
b	NCCRP
6	**Integration with other systems of Police department**
a	SPMCR (Control Room)
b	e-Challan
c	RADMS
7	**Integration with external databases**

a	VAHAN & Samanvay
b	Personal Identity Databases
c	RTO (Regional Passport Office)
d	Hospitals & Health Centers
e	Licensing Authorities
f	Revenue, Tax, Census
8	**Testing**
a	Installation, Testing & Commissioning

c. Training:

SNo.	Items Description
1	Training sessions for Police Personnel & Departments

2. Pricing Formats

a. CAPEX: DC/ DRC/ Field Assets & Application Development

#	Item Description	UOM	Quantity	Unit Price	Total Price Without Tax	GST %	GST	Total Price (Incl. Taxes)
1	**CAPEX - DATA CENTER HARDWARE**							

1.1	Web / Application Servers	Nos.	**11**					
1.2	Database Server	Nos.	**4**					
1.3	Enterprise Management System	Nos.	**1**					
A	**TOTAL CAPEX: DATA CENTER**							
2	**CAPEX - DISASTER RECOVERY CENTER HARDWARE**							
2.1	Web / Application Servers	Nos.	**1**					
2.2	Database Server	Nos.	**2**					
B	**TOTAL CAPEX: DISASTER RECOVERY CENTER**							
3	**CAPEX - FIELD ASSETS HARDWARE**							
3.1	Desktop	Nos.	**6322**					
3.2	UPS Units (Excluding Battery)	Nos.	**979**					
3.3	UPS (Units + Batteries) 2 KVA Online UPS, 60 Mins Backup	Nos.	**372**					
3.4	Inverter	Nos.	**1923**					
3.5	Multi-Function Printer	Nos.	**421**					
3.6	Laser Printer	Nos.	**1923**					
3.7	External Hard Disk (1 TB)	Nos.	**1923**					

C	**TOTAL CAPEX: FIELD ASSETS**							
4	**CAPEX APPLICATION DEVELOPMENT**							
4.1	Design & Development of Web-based Application as per Scope of Work	Lumpsum	**1**					
4.2	Design & Development of API/ Web Service and Integration with Central Systems / State Departments & SCRB Applications as per Scope of Work	Lumpsum	**1**					
4.3	Design & Development of Mobile Application as per Scope of Work	Lumpsum	**1**					
D	**TOTAL APPLICATION DEVELOPMENT**							
TOTAL (A+B+C+D)								

b. CAPEX: Training & Capacity Building

SNo.	Description	Man-Day Cost	GST %	GST	Total amount (Incl. Taxes)
1	Train the Trainers				

	Total in INR				

c. OPEX: Newly Supplied Hardware, Application & Helpdesk Resources

SNo.	Description of Service	Quantity	Year 1	Year 2	Year 3	Year 4	Year 5	Total (Excl. Taxes)	GST %	GST	Total (Incl. Taxes)
1	Operations and Maintenance of Datacenter Hardware (Refer CAPEX: Data Center (1.1 & 1.2))	1	NA								
2	Operations and Maintenance of Enterprise Management System (Refer CAPEX: Data Center (1.3))	1									
3	Operations and Maintenance of Disaster Recovery Center Hardware (Refer CAPEX: Disaster Recovery Center (2.1 & 2.2)	1	NA								
4	Operations and Maintenance of Field Assets (Refer CAPEX: Field Assets (3.1 to 3.7))	1									
5	Operations and Maintenance of Application (Refer CAPEX: Application Development (4.1 to 4.3))	1									

6	Cost of Manpower deployed in shifts at Data Center (24x7) Total 360 Man-months	6									
7	Cost of Manpower deployed at SCRB for Service Desk Operations (16 x 7) Total 360 Man-months	6									
TOTAL in INR											

d. OPEX: Existing Hardware

1) UPS Units and Batteries:

#	Items Description	Count	Year of Procurement	Year 1	Year 2	Year 3	Year 4	Year 5	Total (Excl. Taxes)	GST %	GST	Total (Incl. Taxes)
				A	B	C	D	E	F=A+B+C+D+E	G	H = F*G	I = F+H
1	UPS Units	572	01.10.2020									
2	UPS Batteries	1551	01.07.2019									
	Total in INR											

2) Servers:

a) IBM Servers

SNo.	Items Description	Count	Year of Procurement	O & M Cost for Year 1 in INR	GST %	GST	Total (Incl. Taxes)
				A	B	C=A*B	D=A+C
1	IBM Servers	18	28.12.2011				
	Total in INR						

b) Dell Servers

SNo.	Items Description	Count	Year of Procurement	Year 1	Year 2	Year 3	Year 4	Year 5	Total (Excl. Taxes)	GST %	GST	Total (Incl. Taxes)
				A	B	C	D	E	F=A+B+C+D+E	G	H = F*G	I = F+H
1	Dell Power Edge R530	1	23.03.2018									
2	Dell Power Edge R930	1	30.01.2019									
3	Dell Power Edge R840	3	Jan.2021									
	Total in INR											

e. OPEX: Price Discovery

1. Site Infrastructure

1) Site Preparation:

SNo.	Items Description	Qty	UOM	Unit Rate	GST %	GST	Total Price with GST
				A	B	C=A*B	D=A+C
1	Network CAT 6 UTP Cable	1	Meters				
2	CAT6 Information outlet	1	Meters				
3	Back box and Face plate	1	Pieces				
4	Electrical cable 2.5 sq.mm wire (Mtr)	1	Meters				
5	Electrical cable 1.5 sq.mm wire (Mtr)	1	Meters				
6	Electrical cable 4 sq.mm wire (Mtr)	1	Meters				
7	25 mm PVC for UTP CAT -6 data (Mtr) cabling (Clamp, Screw, L and T Bend)	1	Meters				
8	15 or 25mm PVC for electrical (Mtr) cabling (Clamp, Screw, L and T Bend)	1	Meters				
9	Power socket -5amp socket with (no's) switch	1	Pieces				
10	Power socket -5/15amp SS Combined	1	Pieces				
11	32 Amps MCB (Dual Pole) with Metal Box	1	Pieces				
12	Copper wire/strip for earthing	1	Meters				
13	Earth Rod (5ft)	1	Pieces				
14	Earthing (including Cement pit & Cover)	1	Pieces				
15	Installation-Electrical	1	labour				
16	Installation-Network Components	1	labour				
17	Wall Mount 9 U Rack with Delivery (Power panel, Cooling Fan)	1	Pieces				

18	16 Port Switch Unmanaged	1	Pieces				
19	16 Port Jack Panel Unloaded	1	Pieces				
20	1 Mtr Patch Cord	1	Meters				
21	2 Mtr Patch Cord	1	Meters				
Total in INR							

2) Site Shifting

SNo.	Items Description	No of Locations	Unit Price per Location	GST (%)	GST in INR	Total amount
1	Site Shifting Charges (Police Stations/ Special Units/ Higher Offices/ Training Centers)	1				
	Total in INR					

Note:

1. Site Shifting involves complete wiring and earthing to be done to the shifted location as per the BoQ of the respective description of location.
2. Other items can be shifted to the new location.

2. Hardware Items

SNo.	Item	Qty	UOM	Unit Rate	GST %	GST	Total Price with GST
1	12 V/42 AH SMF Battery for 2 KVA Online UPS, 60 Mins Backup	1	Qty				
2	Online UPS (Unit + Battery) (5 KVA, 120 Mins Backup) as per	1	Qty				

	Specification						
	Total in INR						

3. Data Center/ Disaster Recovery Center

SNo.	Item	Qty	UOM	Unit Rate	GST %	GST	Total Price with GST
1	Anti-Virus Software for Servers	1	Qty				
2	Host Intrusion Prevention Software	1	Qty				
	Total in INR						

Note: Above components shall comply with TNSDC Standards.

4. API/ Web Service Development

SNo.	Item	Man-month required	Unit Cost	GST (%)	GST in INR	Total Cost
1	API Development					
2	Web service development					
	Total in INR					

5. Person Man-Month Rate

The Person Month rate are identified for discovery purposes which may be used for award in case of additional requirement if any.

GST @ the rate specified as per Applicable law will be borne by SCRB.

SNo.	Role	Qualification/ Certification	Person-Month Rate (in INR)	GST (%)	GST	Total Amount (Including GST)
1	Technical Solution Architect	Refer Section 13 for detail of Volume II of this RFP				
2	Database Expert	Refer Section 13 for detail of Volume II of this RFP				
3	Service Desk Expert	Refer Section 13 for detail of Volume II of this RFP				
4	Infrastructure Expert	Refer Section 13 for detail of Volume II of this RFP				
5	Application Developer	Experience in development of Web Application				
6	Server Admin	Experience in End to End Management of deployed Severs				
7	Mobile Applications Programmers	Experience in IT programming and has in depth knowledge of computer languages such as C++, Java, HTML, MySQL etc. Should also have experience in designing Mobile apps.				

SNo.	Role	Qualification/ Certification	Person-Month Rate (in INR)	GST (%)	GST	Total Amount (Including GST)
8	Network Expert/ Admin	CCNP/CCSP/CCIE				
9	IT Security domain expert	Certification - CISSP, CISM, CompTIA Security				
	Total in INR					

3. Total Bid Value

SNo.	Description	Reference	Total Price	GST	Total Price (Incl. of Taxes)
1	Total Cost of Implementation	CAPEX (DC/ DRC/ Field Assets & Application Development + Training & Capacity Building)			
2	Total Cost of Operations and Maintenance	OPEX (Newly Supplied Hardware, Application & Helpdesk Resources)			
3	Total Cost of Operations and Maintenance for Existing Hardware	OPEX (Existing Hardware)			
4	Total Cost of Operations and Maintenance for Price Discovery	OPEX (Price Discovery)			
Total in INR					

8.6 Annexure 6 – Template for Performance Bank Guarantee

(To be executed in Rs.100/- Stamp Paper purchased in Tamil Nadu)

To

Additional Director General of Police (ADGP),
State Crime Record Bureau (SCRB)
95, Greenways Rd, MRC Nagar, Raja Annamalai Puram,
Chennai, Tamil Nadu 600028

Bank Guarantee No:

Amount of Guarantee:

Guarantee covers from:

Last date for lodgment of claim:

This Deed of Guarantee executed by ..... (Bankers Name & Address) having our Head Office at .....(address) (hereinafter referred to as "the Bank") in favour of Additional Director General of Police (ADGP), State Crime Record Bureau, 95, Greenways Rd, MRC Nagar, Raja Annamalai Puram, Chennai, Tamil Nadu 600028 (hereinafter referred to as "the Beneficiary") for an amount not exceeding Rs._____/- (Rupees _____ Only) as per the request of M/s. _____ having its office address at _____ (hereinafter referred to as "Developer / Software Agency") against Letter of Acceptance reference _____ dated __/__/____ of M/s. State Crime Record Bureau. This guarantee is issued subject to the condition that the liability of the Bank under this guarantee is limited to a maximum Rs._____/- (Rupees _____ Only) and the guarantee shall remain in full force up to ___ months from the date of Bank Guarantee and cannot be invoked otherwise by a written demand or claim by the beneficiary under the Guarantee served on the Bank before ___ months from the date of Bank Guarantee.

AND WHEREAS it has been stipulated by you in the said ORDER that the Developer / Software Agency shall furnish you with a Bank Guarantee by a Scheduled Bank for the sum specified

therein as security for compliance with the Banker performance obligations for a period in accordance with the contract.

AND WHEREAS we have agreed to give the Developer / Software Agency a Guarantee.

THEREFORE, we (Bankers address)....., hereby affirm that we are Guarantors and responsible to you on behalf of the Developer / Software Agency upto a total of Rs._____/- (Rupees _____ Only) and we undertake to pay you, upon your first written demand declaring the Developer / Software Agency to be in default under the contract and without any demur, cavil or argument, any sum or sums within the limit of Rs._____/- (Rupees _____ Only) as aforesaid, without your needing to prove or show grounds or reasons for your demand or the sum specified therein. We will pay the guaranteed amount notwithstanding any objection or dispute whatsoever raised by the Developer / Software Agency.

This Guarantee is valid until ____months from the date of Bank Guarantee.

Notwithstanding, anything contained herein:

Our liability under this guarantee shall not exceed Rs. _____/- (Rupees _____ Only). This Bank Guarantee shall be valid up to __ months from the date of Bank Guarantee and we are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only and only if you serve upon us a written claim or demand on or before_____.

In witness whereof the Bank, through its authorized officer, has set its, hand and stamp on this ..... at _____.

Witness:1. (Signature)

Witness:2

(Name in Block Letters)

Designation:

Bank Seal:

8.7 Annexure 7 - Undertaking for Certificate of Registration as per GFR Rule

Ref: Date:

To
The Managing Director,
Electronics Corporation of Tamil Nadu Ltd,
MHU Complex, II Floor,
692, Anna Salai,
Nandanam,
Chennai-600 035.

Dear Sir,

Sub: Tender for Selection of System Integrator for Supply, Design, Development, Implementation and Maintenance of CCTNS 2.0 for SCRB.

Ref: Tender Reference ELCOT/PROC/OT/33384/CCTNS 2.0 (SCRB)/ 2020-21

I/We, < Bidder> have read the clause regarding restrictions on procurement from a Bidder of a Country which shares a land border with India.

I/We hereby certify that I/We, <Bidder Name> is not from any such country or, if from such a Country, has been registered with Competent Authority.

I/We hereby certify that I/We in the event of becoming a successful bidder shall not sub-contract works to any Contractor from a Country which shares a land border with India unless such Contractor is registered with the Competent Authority, as defined vide Section 2.5(ii) of this RFP.

I/We hereby certify that I/We fulfil all requirements in this regard and eligible to be considered

For <Bidder>

Authorised signature:

Name of the authorised person:

Designation:

Name of Bidder

Stamp of bidder

NOTE:

1. The letter should be submitted on the Letter head of the BIDDER and should be signed by the Authorized Signatory.
2. Any deviation would lead to summary rejection of bids/Proposals.
3. Wherever Applicable, valid Registration certificate obtained from the Competent Authority shall be attached.

CRIME & CRIMINAL TRACKING NETWORK AND SYSTEMS (CCTNS)

Tender Reference

ELCOT/PROC/OT/33384/CCTNS 2.0 (SCRB)/ 2020-21

Request for Proposal

For

Selection of System Integrator for Supply, Design, Development, Implementation and Maintenance of CCTNS 2.0

Volume II

Tender Document

Functional and Technical Requirements of the project

Table of Contents

1. Glossary and List of Abbreviations

RFP	Request for Proposal
ELCOT	Electronics Corporation of Tamil Nadu
CCTNS	Crime and Criminal Tracking Networks and Systems
CIPRUS	Common Integrated Police Records Updation System
SCRB	State Crime Records Bureau
MSA	Master Service Agreement
NDA	Non-Disclosure Agreement
RACI	Responsible Accountable Consulted Informed
EMS	Enterprise Management System
TN	Tamil Nadu
DGP	Director General of Police
ADGP	Additional Director General of Police
IGP	Inspector General of Police
SP	Superintendent of Police
DIG	Deputy Inspector General of Police
ADSP	Additional Superintendent of Police
EOW	Economic Offences Wing
CSG	Coastal Security Group
STPC	State Traffic and Planning Cell
CBCID	Crime Branch Criminal Investigation Department
AP	Armed Police
USRB	Uniform Service Recruitment Board
PCR	Police Control Room
PEW	Prohibition Enforcement Wing
MMP	Mission Mode Project
NCRB	National Crime Records Bureau
DR	Disaster Recovery
CAS	Core Application Software
CCIS	Crime and Criminal Information System

CAARUS	Crime Analysis & Automatic Records Updation System
BSNL	Bharat Sanchar Nigam Limited
UPS	Uninterruptible Power Supply
HDD	Hard Disk Drive
MFP	Multi-Functional Printer
LP	Laser Printer
KVA	Kilo Volt Ampere
HO	Head Office
CAT	Category *(as in Cable)*
SLA	Service Level Agreement
MPLS	Multi-Protocol Label Switching
VPN	Virtual Private Network
TNSDC	Tamil Nadu State Datacenter
PS	Police Station
API	Application Programming Interface
VIP	Very Important Person
DPO	District Police Office
DCRB	District Crime Records Bureau
MHA	Ministry of Home Affairs
FIR	First Information Report
UIDB	Unidentified Dead Body
SMS	Short Message Service
CSR	Community Service Register
MDM	Master Data Management
IMEI	International Mobile Equipment Identity
FACTS	Fingerprint Analysis Criminal Tracing System
AFIS	Automated Fingerprint Information System
ICJS	Inter-operable Criminal Justice System
NCCRP	National Cyber Crime Reporting Portal
DMU	Data Migration Utility
SPMCR	State Police Master Control Room
RADMS	Road Accident Data Management System

iRAD	*Integrated* Road Accident Database
PAN	Permanent Account Number
ALIS	Arms License Issuing Systems
FR	Functional Requirements
IO	Investigating Officer
PM	Postmortem
CrPC	Criminal Procedure Code
SOC	Scene of Crime
TI	Test Identification
PP	Public Prosecution
FSL	Forensic Science Laboratory
RCN	Regular Criminal Number
NCN	National Criminal Number
FP	Fingerprint
UIDAI	Unique Identification Authority of India
OTP	One Time Password
IPC	Indian Penal Code
SSL	Secure Sockets Layer
POCSO	Protection of Child from Sexual Offences Act
CII	Crime in India *(reports)*
BI	Business Intelligence
SPOC	Single Point of Contact
GO	Government Order
IM	Instant Messenger
SHO	Station House Officer
BC	Bad Character *check*
NGO	Non-Government Organization
IIF	Integrated Investigation Form
RTA	Road Traffic Accident
NBW	Non Bailable Warrant
FRS	Functional Requirements Specification
MO	Modus Operandi

DB	Database
ANPR	Automatic Number Plate Recognition
SDFPB	Single Digit Fingerprint Bureau
NAFIS	National Automated Fingerprint Information System
UAT	User Acceptance Test
TPA	Third Party Audit
SRS	System Requirements Specification
HLD	High Level Design
LLD	Low Level Design
SDD	System Design Document
ER	Entity Relationship
GUI	Graphical User Interface
UML	Unified Modeling Language
SOA	Service Oriented Architecture
PDS	Public Distribution System
BCP	Business Continuity Plan
DRP	Disaster Recovery Plan
RPO	Real Time Objective
RTO	Recovery Time Objective
WAN	Wide Area Network
UI	User Interface
SAN	Storage Area Network
OS	Operating System
SQL	Structured Query Language
HTTPS	Hypertext Transfer Protocol Secure
CMS	Content Management System
HIPS	Host Intrusion Prevention System
IPS	Intrusion Prevention System
VAPT	Vulnerability Assessment and Penetration Testing
STQC	Standardization Testing and Quality Certification
CERT-IN	Indian Computer Emergency Response Team
IS	Information System

OEM	Original Equipment Manufacturer
ATS	Annual Technical Support
SDLC	Software Development Lifecycle
SOAP	Service Oriented Architecture Protocol
GIF	Graphics Interchange Format
IMG	Image *file format*
TIFF	Tagged Image File Format
JPEG	Joint Photographic Expert Group
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
RSA	Rivest, Shamir, Adleman
PKCS	Public-Key Cryptography Standards
ITIL	Information Technology Infrastructure Library
EITM	Enterprise Information Technology Management
IEEE	Institute of Electrical and Electronics Engineers
CMMI	Capability Maturity Model Integration
DPR	Detailed Project Report
SSDG	State e-Governance Service Delivery Gateway
MSDG	Mobile Service Delivery Gateway
PAT	Portable Appliance Testing
EMS	Enterprise Management System
FAT	Factory Acceptance Test
SDK	Software Development Kit
XML	eXtensible Markup Language
HTML	Hypertext Markup Language
AJAX	Asynchronous JavaScript And XML
XSL	eXtensible Stylesheet Language
IDE	Integrated Design Environment
JSP	Jakarta Server Pages
EJB	Jakarta Enterprise Beans
PDF	Portable Document Format
DDL	Data Definition Language

PL/SQL	Procedural Language / Structured Query Language
TCV	Total Contract Value
SWAN	Statewide Area Network
MIS	Management Information System
MBA	Master of Business Administration
MCA	Master of Computer Application
PMP	Project Management Professional
VM	Virtual Machine
CS	Computer Science
IT	Information Technology
CPU	Central Processing Unit
MS IE	Microsoft Internet Explorer
TCP / IP	Transmission Control Protocol/Internet Protocol
SMTP	Simple Mail Transfer Protocol
TNPA	Tamil Nadu Police Academy
PTC	Police Training College
ITAM	Information Technology Asset Management
UIM	User Identity Module
UIMDB	User Identity Module Database
NIC	National Informatics Center
CCN	Change Control Note

2. Request for Proposal - Process

2.1 Structure of the RFP

Electronics Corporation of Tamil Nadu (hereafter referred as "ELCOT") invites the eligible parties (hereafter referred as "Bidder") for appointment as System Integrator (SI) to Design, Develop, Commission, Operate, Maintain and Manage the "CCTNS 2.0 (Infrastructure Refresh, Maintenance and New Web Application, Maintenance & Integration)" by providing a comprehensive solution as specified in the RFP.

The Bidders are advised to study this RFP document carefully before submitting their proposals in response to this notice. Submission of a proposal in response to this notice shall be deemed to

be been done after careful study and examination of this document with full understanding of its terms, conditions and implications. Failure to furnish all information required as mentioned in the RFP documents or submission of a proposal not substantially responsive to the RFP documents in every respect will be at the Bidder's risk and may result in rejection of the proposal

This Request for Proposal (RFP) document comprise of the following volumes:

1. **Volume I:** Instructions on the Bid process for the purpose of responding to this RFP. This broadly covers:
   a. General instructions for bidding process.
   b. Bid process management details.
   c. Bid evaluation process including the parameters for Pre-qualification evaluation, Technical evaluation and Commercial evaluation to facilitate SCRB in determining bidder's suitability as the System Integrator.
   d. Bid submission formats.
   e. Proposed BoM, Price Bid Formats & Minimum Technical specification.

2. **Volume II:** Functional and Technical Requirements of the project. The contents of the document broadly cover the following areas:
   a. About the project and its objectives.
   b. Scope of Work.
   c. Project Management & Governance
   d. Minimum Functional and Technical requirements.
   e. Implementation Schedule, Payment Schedule, SLA

3. **Volume III:**
   a. Master Service Agreement (MSA) Master Services Agreement (MSA) template outlining the contractual, legal terms & conditions applicable for the proposed Project.
   b. Change Control Note.
   c. Service Level Agreement (SLA).
   d. Non-Disclosure Agreement (NDA).

Applicability of Tamil Nadu Transparency in Tenders Act 1998:

This RFP process is governed by the Tamil Nadu Transparency in Tenders Act 1998 and The Tamil Nadu Transparency in Tenders Rules, 2000 as amended from time to time.

2.2 Structure of Volume II

Section	Coverage
Section 1	Glossary and List of Abbreviations
Section 2	Request for Proposal – Process
Section 3	Tamil Nadu Police
Section 4	Background of CCTNS
Section 5	Project Overview CCTNS 2.0
Section 6	CCTNS 2.0 Hardware Infrastructure Refresh
Section 7	CCTNS 2.0 Web Application Software
Section 8	CCTNS 2.0 Project Requirements & Deliverables
Section 9	Timelines and Schedule
Section 10	SCRB Project Governance Office
Section 11	Stakeholder Responsibility Matrix (RACI Matrix)
Section 12	Resource Requirement
Annexure 1	Web Application- CCTNS 2.0 Application Design Principles
Annexure 2	Non – Functional Requirements
Annexure 3	List of Police Stations, Special Units, Higher Offices, Training Centers

Section	Coverage
Annexure 4	CA EMS (Enterprise Management System) License Details
Annexure 5	Change Control Note Format
Annexure 6	Current User Count, User roles & Privileges
Annexure 7	Application Security Requirements

3. Tamil Nadu Police

3.1 About TN Police Department

The Tamil Nadu Police has a personnel strength of over a lakh and is headed by the Director General of Police (DGP). There are 8 other officers of the rank of DGP, 23 officers of the rank of Additional Director General of Police (ADGP), 41 officers of the rank of Inspector General of Police (IGP), 29 officers of the rank of Deputy Inspector General of Police (DIG), 153 officers of the rank of Superintendent of Police (SP), 144 officers of the rank of Additional Superintendent of Police (ADSP) and a large number of other police officers.

Given below is a pictorial representation of the department organizational chart.

Figure 1: General Hierarchy of Tamil Nadu Police

To cater to providing efficient policing and upkeep law & order, the state has been divided into 5 zones, 41 districts. Police stations in their respective locations carry out various activities, most importantly detect and prevent crime and provide citizen services. The Police Station is the basic operating unit while the District Police Office is the basic administrative unit.

Table 1: Administrative Units

Administrative Units	Number
Police Stations	1551
Special Unit Police Stations	372
Police Higher Offices	488
Training Centers	49

DGP (Law & Order) is the head of the State Police Department and there are ADGPs of different units reporting to the DGP as mentioned below:

a. **Economic Offences Wing (EOW):** This unit deals with white collared offences with respect to Non-Banking Financial Corporations (NBFCs)
b. **Coastal Security Guard (CSG):** This unit deals with protection of state's coastal borders
c. **State Transport Planning Cell (STPC):** This unit is in charge of analyses of traffic accidents and suggesting measures for improving road safety.
d. **Civil Supplies Criminal Investigation Department (CBCID):** This unit handles crimes done with respect to Essential Commodities act
e. **Armed Police (AP):** This unit deals with the deployment and maintenance of armed police force in the state
f. **Administration:** This unit deals with the administrative affairs of the entire state police department.

Enforcement, Training, Crime Bureau and Criminal Investigation Department (CBCID), Welfare, Uniform Services Recruitment Board (USRB) are some of the other functional wings that are headed by ADGP in the state Police Headquarters.

The Law & Order unit maintains order across the state and all 1551 police stations in the state report to the ADGP (Law & Order). There are IGPs reporting to these unit ADGPs. In the Law & Order hierarchy, the state is separated further into zones and then into Districts and Commissionerate.

A zone is managed by an officer of the rank of IGP and each range by a DIG. There are a number of districts in a range and each district is headed by the SP who is responsible for regular all police stations in the district. The SPs have Deputy Superintendent of Police (DSP) reporting to them. The DSPs are responsible for monitoring a limited set of stations under their control. The DSP is based in the sub-divisional office. Apart from cases which require DSP to act as the investigating officer, this office works more as an administrative unit collating case progress details and station administrative records. Each police station is headed by an Inspector/Sub-Inspector. In the case a station is headed by a sub-inspector, it is attached to another station

proximally closer to a station that is headed by an Inspector. where inspector heads that station. In such a case, the attached station becomes the circle office.

3.2 Organization Structure

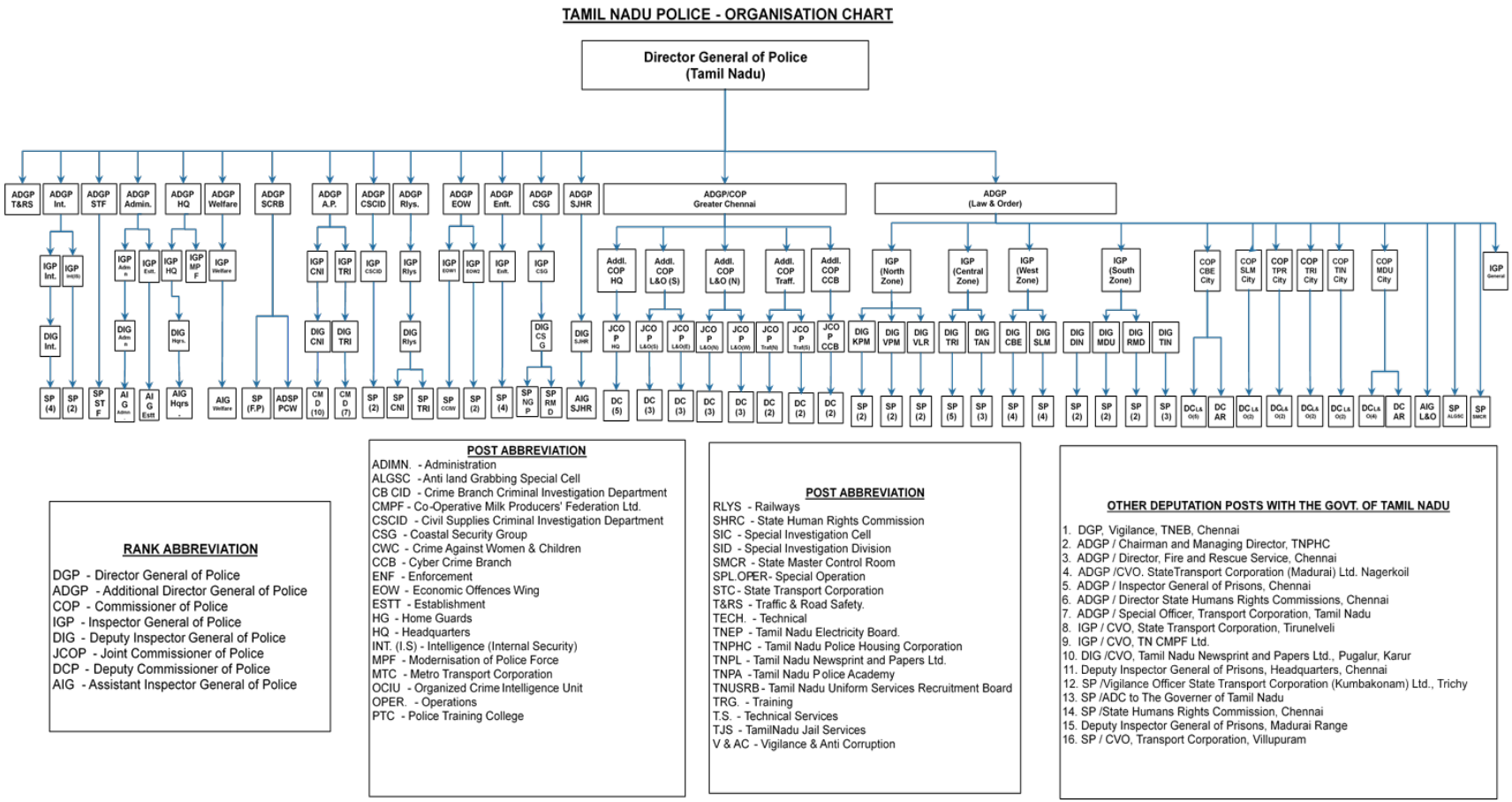


Figure 2: Tamil Nadu Police - Organization Chart

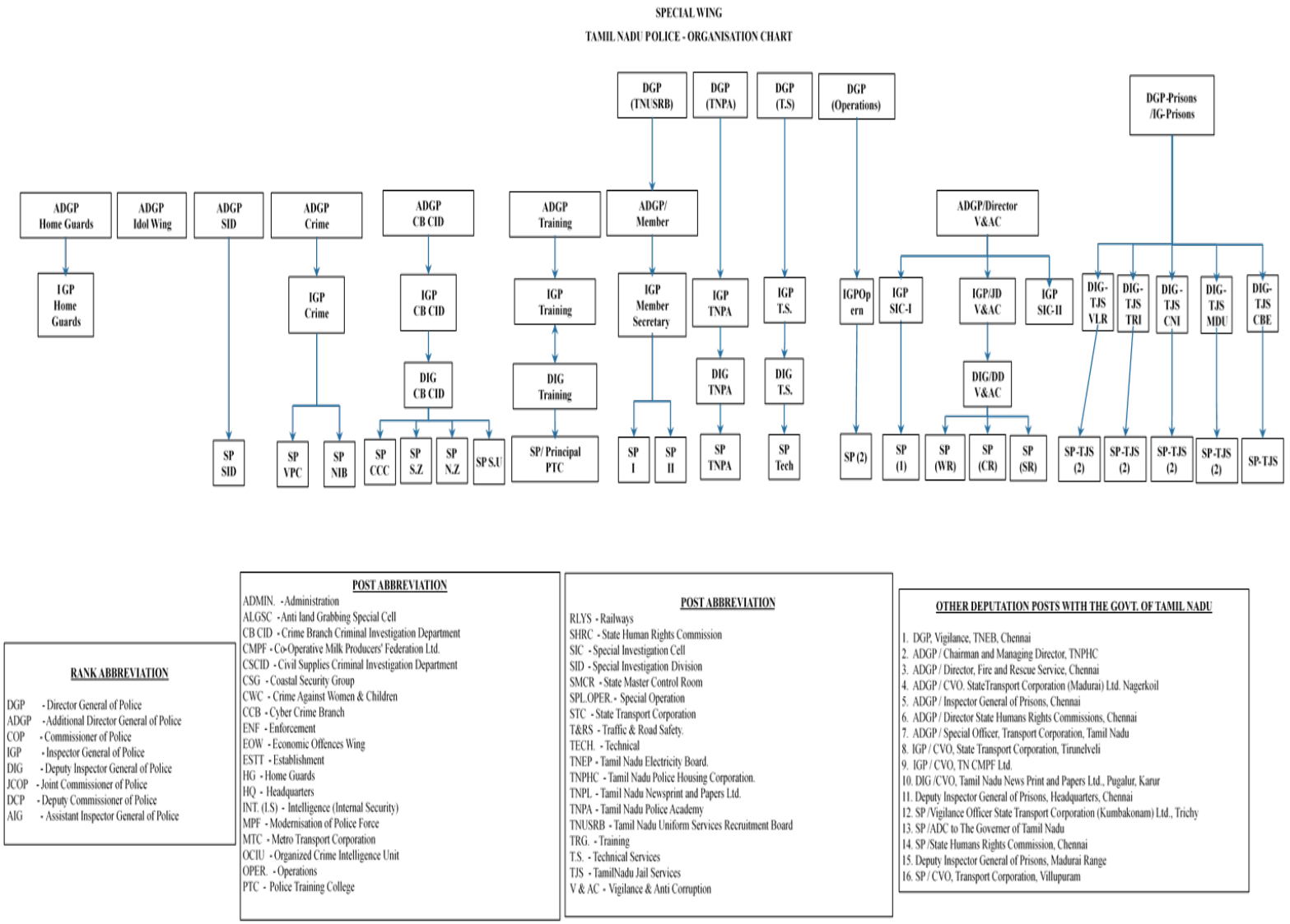


Figure 3: Tamil Nadu Police - Special Wing

The figures above depict that there are units under the control of SP and Commissioner at district and Commissionerate which deal with cases pertaining to specific areas such as Protection of Civil Rights (PCR), Prohibition & Enforcement wing (PEW), etc. They constitute the special units serving different purposes. The list of Special Units is mentioned below:

Table 2: List of Special Units

Intelligence Wing	District Special Branch	SB CID
SD CID	Q Branch CID	Security Branch, Core Cell & OCIU
Coastal Security Group (CSG)	Crime Branch CID	Crime (S.I.T)
Economic Offences Wing (EOW)	Commercial Crime Investigation Wing (CCIW)	Idol Wing
Tamil Nadu Police Academy (TNPA)	Police Training College (PTC)	Police Recruit School (PRS)
In-service Training Centre (ISTC)	Armed Police (AP)	Prohibition Enforcement Wing (PEW)
Home Guards	Special Task Force (STF)	State Traffic Planning Cell (STPC)
TN Commando Force (TNCF)	Government Railways	Technical Services (TS)
Social Justice & Human Rights (SJ & HR)	State Crime Records Bureau (SCRB)	Forensic Science Lab (FSL)
District/City - Crime Branch (DCB/CCB)	Civil Supply CID (CSCID)	Traffic Investigation Wing (TIW)
Traffic Enforcement Wing	Juvenile Aid Police Unit (JAPU)	Anti-Vice Squad (AVS)

(TEW)		
Anti-Dowry Cell (ADoC)	Crime against Women & Children	Cyber Crime Wing

Unit Offices of these Special units are usually located at the district HQ and Commissionerate are under the control of the district SP and commissioner respectively.

4. Background of CCTNS

CCTNS is a Mission Mode Project (MMP) under the National e-Governance Plan (NeGP) of Government of India. It was conceptualized and sponsored by the Ministry of Home Affairs (MHA). National Crime Records Bureau (NCRB) is the central nodal agency for managing the nationwide implementation of this project and the respective State Crime Records Bureau (SCRB), the State Nodal Agency for implementation in the State.

The CCTNS was envisioned as a system which shall allow access to real-time crime and criminal information. The focus was to make investigation record management more efficient, thus enabling the reporting, crime and criminal case analysis, supervisory management, field force management and deployment easier.

There are many objectives for which the CCTNS project was envisaged as mentioned below:

i. Provide enhanced tools for crime investigation, crime prevention, law and order maintenance and other regulatory functions:

a. Utilize IT for efficiency and effectiveness of core policing operations

b. Provide information for easier and faster analysis and trends

ii. Create a national platform for sharing crime and criminal information and intelligence across the country in between state and central and external agencies

iii. Improved services for general public and other institutions such as:

a. Access to police services in a citizen-friendly manner

b. Provide fast, accurate and digital modes of service delivery

4.1 Hardware Infrastructure

A "Bundling of Services" approach was recommended for implementation of CCTNS across various Police Stations and other units across the state during its first implementation in 2013-14. The scope of services included supply and commissioning of necessary hardware required for CCTNS operations. A separate CCTNS site within the police stations was identified and provisioned for the same. The scope also included readying the site for CCTNS through network, civil and electrical upgradation. A requisite number of servers was identified to be hosted at the ELCOT State datacenter in Chennai with its DR at Pune for CCTNS operations. The CAS (Central Application Software) was developed by NCRB and provisioned for use by Tamil Nadu Police. The CCTNS state SI that was onboarded was responsible for smooth functioning of the CCTNS project by maintaining and upkeeping the above stated infrastructure. An illustrative list of activities that was performed by the SI are:

1) Hardware assets supplied, installed & commissioned at the Police stations and other Department offices and Training centers.
2) Network and Electrical infrastructure were set up as a part of site preparation for CCTNS to house all assets, use the software and perform CCTNS project operations.
3) State hosted DR and DC infrastructure which included configured servers, storage and switching infrastructure where all the applications were hosted
4) Training, capacity building of the department as required
5) Setup and maintenance of a dedicated helpdesk and asset monitoring system.

The current CCTNS 2.0 project has been envisioned and being tendered because the hardware and infrastructure that was part of the CCTNS 1.0 has reached beyond the end of life period. Owing to technology advancements, pressing recurring issues arising out of obsolete hardware

and difficulty to procure and service asset spares and parts through OEMs are some of the reasons the CCTNS 2.0 has been envisioned. This will ensure the department infrastructure is well equipped, state-of-the-art and in accordance with the CCTNS project objectives.

4.2 Core Application Software

There were many programs initiated both from the central as well as the state levels to leverage IT in efficient functioning of the Police. Some of them being NCRB initiated CCIS (Crime and Criminals information system) and CIPA (Common integrated Police application). Some that were state initiated were e-COPS (Andhra Pradesh), Police IT (Karnataka), Thana tracking (West Bengal), erstwhile CAARUS now CIPRUS (Tamil Nadu) and IITS (Gujarat).

The CCTNS application software that was developed at NCRB was provided to the states and UTs for deployment. Each state had customized to their unique requirements. The CAS (Core application software) would fall under 2 broad categories:

CAS (State): This would cover functionalities that would be aligned to central core platform at NCRB, with customizations, configuration, enhancement and extensions. It was the responsibility of the state to determine the requirements for configuration and needful customizations pertaining to the particular state.

CAS (Centre): This would reside at NCRB and would cater to the functionality that is required at the GOI level (MHA and NCRB). This was also developed at NCRB.

NCRB developed the CAS (core application software) and offered it to the states for customization to suit their requirements. Tamil Nadu opted to go for its own state CAS, named CIPRUS (Common Integrated Police Records Updation System). To fulfill the objectives of the CCTNS project, data capture and building up of a database of crimes and criminals is a basic necessity. Police stations, being the point of generation of data, the CIPRUS 1.0 application was developed in Tamil Nadu and put in place in all police stations for data entry. The data is currently being shared with NCRB for enabling nation level database building and also to activate national searches.

The functionality of the existing application has been described in Section 7.1.4

5. Project Overview CCTNS 2.0

5.1 Scope Overview

Given below is a brief of the scope overview of the CCTNS 2.0 project:

Infrastructure Refresh, Operate and Maintenance

i. The replacement and maintenance of all hardware assets in all the police stations, higher offices and training centers in a phased manner, excluding furniture and certain other accessories that were previously supplied in CCTNS 1.0

ii. The conditional repair or replacement and maintenance of all infrastructure (electrical, cabling and local network) items as part of site preparation subject to site inspection by the Bidder.

iii. The maintenance of existing servers, and storage at the SDC and DRC for the first year (O&M), supply of new servers in Phase 2 or Year 2 and maintenance of newly supplied servers till the end of contract period.

Application Development, Integration & Maintenance

i. The development of a complete end-to-end new web-based application- CCTNS 2.0. The development scope of work shall entail three categories of modules – Core Modules, Tools and portals on CCTNS platform, Core Admin Module with respective sub-modules.

ii. The development of API/web services required for integration of web application with existing applications of SCRB, central systems, other systems of Police department and external databases

iii. Operation & Maintenance of the above developed applications and integrations throughout the contract period

5.2 Project Stakeholders

There are multiple stakeholders with various roles and responsibilities with regard to adoption, implementation, impact, enforcement and governance of the project. The following table provides details of the various stakeholders of CCTNS 2.0:

SNo.	Stakeholder Name	Role
1	Police Department (Stations, Special Units, Higher Offices, Training Centers, Enforcement Wings)	Adoption and direct beneficiaries of the CCTNS 2.0 project (hardware replacement,) at their respective site locations.
2	SCRB	State nodal agency – Project implementation & governance authority
3	NCRB	Central nodal agency – Secondary stakeholder, state applications connect to and from central databases
4	New System Integrator	New Bidder to be onboarded for implementation and O&M of CCTNS 2.0 project
5	Current System Integrator	Current SI, responsible for O&M up to 31st March 2021
7	ELCOT	SDC & DRC- maintenance and operations
8	BSNL	For providing dedicated network connectivity across stakeholder systems and site locations
9	National Informatics Centre (NIC)	CIPRUS application development & maintenance

6. CCTNS 2.0 Hardware Infrastructure Refresh

6.1 Existing (As-is) Hardware Infrastructure Overview

6.1.1 Existing Hardware Infrastructure

Station Hardware:

The first time the CCTNS project was rolled out in 2013-14 for the modernization and digitization of the Police force, it had the following as part of station hardware

Hardware – The police stations, higher offices, training centers in the department were supplied and commissioned with necessary hardware for smooth functioning and operations of CCTNS.

As a part of hardware requirement, the following items were installed and commissioned in all police units:

1) Desktops
2) Printer Multi-functional printer
3) Printer Laser printer
4) UPS (2 different load variants for police stations and training centers)
5) Inverters
6) Digital Cameras
7) e-Pens
8) External Hard Drives (HDD)

The supporting infrastructure for the assets were:

1) Storage and servers deployed in state owned Datacenter (SDC) in Chennai & DRC in Pune
2) Furniture, electrical cabling for desktops, UPS and Inverters at the sites

Hardware items were supplied subject to operational requirement of the unit type. The detailed breakup of the hardware assets that were supplied and were installed are as follows:

	Police Stations	Police HO	Training Centers	Special Units

Desktop	Y	Y	Y	Y
Printer MFP	Y	N	N	Y
Printer LP	Y	N	N	N
UPS	Y	Y	Y	Y
Inverter	Y	N	N	N
e-Pen	Y	N	N	N
Digital Camera	Y	N	N	N
External HDD	Y	N	N	N

i. Two variants of UPS were commissioned; 2 KVA and 5 KVA. The 2 KVA load capacity was installed in all police stations to serve a maximum capacity of 4 desktops. For the training centers, 5 KVA was installed since training have a high concurrent user base (training batches) and usage of electronic assets like desktops and printers.

ii. A standard load capacity of 3 KVA inverters were commissioned

iii. Desktops were supplied to all police stations, HO, training centers and special units.

iv. Printers were selectively supplied depending on the usage requirement.

v. e-Pens, Digital cameras and External HDDs were supplied only to the Police stations.

The total number of the above-mentioned items that were supplied earlier is given below:

Hardware	
Items	**Current Count**
Desktop	6800
UPS (Excluding Batteries)	1541
UPS (Unit + Batteries)	372
Printer- MFP	1913
Printer- LP	1541
Ext. HDDs	1541

Inverter	1541
e-Pen	1541
Digital Camera	1541

Under the CCTNS hardware refresh, the SI shall fulfill the baseline criteria for procurement, supply and installation at the stations. The detailed scope of work for hardware refresh CCTNS 2.0 has been described in detail in Section 6.2

Site Preparation:

The site preparation part of CCTNS involved the electrical, network infrastructure and furniture at the station premises to ensure smooth operations of CCTNS.

The site preparation during CCTNS inception and rollout in 2013-14 involved site identification and requisiteness to house the hardware assets. Preparation of the site included the following installations:

1) Electrical cabling
2) Earthing and earth pit
3) Wall mountable network rack
4) Patch panel
5) Information outlet CAT 6
6) CAT 6 with cabling
7) Patch cords

As a precursor to the CCTNS 2.0 project, a site inspection was conducted to understand current condition of the site infrastructure. The various aspects checked are as follows:

1) Condition of electrical cabling – If all the electrical connections are in good working condition without any wear and tear, scratches or malfunctioning
2) Condition of earthing and earth pit – Whether short circuitry or electrical faults are encountered in any plugs or sockets or any metal parts (racks / UPS stands)

3) Condition of inverter and UPS – If the earthing for the metal stand is good, if backup time for the UPS and Inverter is above the minimum threshold as required
4) Network connectivity - Whether the BSNL connectivity is working fine inside the CCTNS room and to the nearest network hub and if there are any issues of network outage reported
5) Spaciousness of the CCTNS site – If the sq. ft. area is sufficient for the number of desktops, infrastructure and accessories

Further, the sites were segregated into **Good** working condition and **Not Good** working condition, e.g., Multiple issues (major and/or minor) were combined as **Not Good** condition. If the parts were reported as working with no operational issues, no short circuitry or handling issues for the users, no cracks or breaks in cables, then the site was marked under **Good** condition.

It was found out that an estimated **10 to 15%** of the items in the police stations are Not in Good Working Condition and some items may have to be replaced, however, the items are in use and the extent of damage could not be ascertained. The item that has incurred the most wear and tear is the Earth Pit and the Cabling. Other items are largely operational and in use.

6.1.2 Existing Data Center Infrastructure

The Datacenter for the CCTNS project is maintained at the SDC in Chennai, Tamil Nadu.

All the servers required for CCTNS use were procured, commissioned and setup in SDC at ELCOT premises. The server details that are currently functioning for CCTNS at the SDC are given below in the table:

#	Make	Server Details				Physical Server Specification			
		Type of Server	Operating System	Servers	Location	RAM	LUN Spaces	Disk Space	Processor Details
1	IBM	Physical	Windows	1	SDC, Chennai	64 GB		2*300 GB, 2*1 TB	Intel Xeon 4C Processor model E5620 80W 2.40 GHZ/1066 Mhz/12 MB Cache*2 nos
2	IBM	Physical	Windows	1	SDC, Chennai	64 GB	2 TB	2*300 GB, 2*1 TB	Intel Xeon 4C Processor model E5620 80W 2.40 GHZ/1066 Mhz/12 MB Cache*2 nos
3	IBM	Physical	Linux	1	SDC, Chennai	64 GB		2*300 GB	Intel Xeon 4C Processor model E5620 80W 2.40 GHZ/1066 Mhz/12 MB Cache*2 nos
4	DELL	Physical	Windows	1	SDC, Chennai	256 GB		8*1.2 TB	-
5	IBM	Physical	Windows	1	SDC, Chennai	256 GB		4*1.2 TB	Intel Xeon 4C Processor model E5620 80W 2.40 GHZ/1066 Mhz/12 MB Cache*2 nos
6	IBM	Physical	Linux	1	SDC, Chennai	64 GB	2 TB	4*146 GB, 4*600 GB	Intel Xeon 10C E7-4870 130W 2.40GHZ/30 MB L3 Cache *4 nos
7	IBM	Physical	Linux	1	SDC, Chennai	132 GB		2*300 GB	Intel Xeon 4C Processor model E5620 80W 2.40 GHZ/1066 Mhz/12 MB Cache*2 nos
8	IBM	Physical	Linux	1	SDC, Chennai	132 GB		2*300 GB	Intel Xeon 4C Processor model E5620 80W 2.40 GHZ/1066 Mhz/12 MB Cache*2 nos

9	IBM	Physical	Linux	1	SDC, Chennai	128 GB	4 TB	4*146 GB	Intel Xeon 10C E7-4870 130W 2.40GHZ/30 MB L3 Cache *4 nos
10	IBM	Physical	Linux	1	SDC, Chennai	128 GB	4 TB	4*146 GB	Intel Xeon 10C E7-4870 130W 2.40GHZ/30 MB L3 Cache *4 nos
11	DELL	Physical	Linux	1	SDC, Chennai	512 GB	4 TB	3*1 TB	-
12	IBM	Physical	Linux	1	SDC, Chennai	64 GB		2*300 GB	Intel Xeon 4C Processor model E5620 80W 2.40 GHZ/1066 Mhz/12 MB Cache*2 nos
13	IBM	Physical	Linux	1	SDC, Chennai	64 GB	2 TB	2*300 GB	Intel Xeon 4C Processor model E5620 80W 2.40 GHZ/1066 Mhz/12 MB Cache*2 nos
14	IBM	Physical	Linux	1	SDC, Chennai	64 GB	1 TB	2*300 GB	Intel Xeon 4C Processor model E5620 80W 2.40 GHZ/1066 Mhz/12 MB Cache*2 nos
15	IBM	Physical	Linux	1	SDC, Chennai	64 GB		2*300 GB	Intel Xeon 4C Processor model E5620 80W 2.40 GHZ/1066 Mhz/12 MB Cache*2 nos
16	IBM	Physical	Linux	1	SDC, Chennai	64 GB	8 TB	2*300 GB	Intel Xeon 4C Processor model E5620 80W 2.40 GHZ/1066 Mhz/12 MB Cache*2 nos
17	IBM	Physical	Windows	1	SDC, Chennai	64 GB		2*300 GB	Intel Xeon 4C Processor model E5620 80W 2.40 GHZ/1066 Mhz/12 MB Cache*2 nos

There were 17 physical servers procured by the current SI, 15 IBM make, and 2 DELL make. The 15 IBM physical servers were procured during project initiation in December 2011. The 2 servers of DELL have been procured recently in March 2018 and January 2019 respectively. The O&M scope for the new SI shall apply accordingly as mentioned in Section 6.2.3.

There are 3 more DELL make servers that have been procured by SCRB in January 2021. The specifications for the 3 new servers are given below:

SNo.	Make	Server Details				Physical Server Specification			
		Type of Server	Operating System	Total No. of Servers	Location	RAM	LUN Spaces	Disk Space	Processer Core
1	DELL	Physical	Linux	1	SDC, Chennai	512 GB		3*600 GB	20 Core
2	DELL	Physical	Linux	1	SDC, Chennai	512 GB		3*600 GB	20 Core
3	DELL	Physical	Linux	1	SDC, Chennai	512 GB		3*600 GB	20 Core

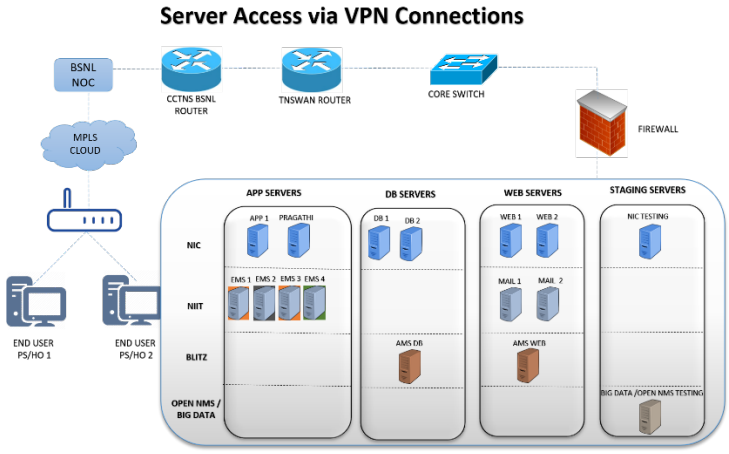
The Disaster Recovery for the CCTNS is maintained by NIC at DRC, Pune. For the DRC, 3 IBM physical servers were procured and deployed. The O&M scope of the same has been mentioned in Section 6.2.3. The details of the existing DRC servers are given below:

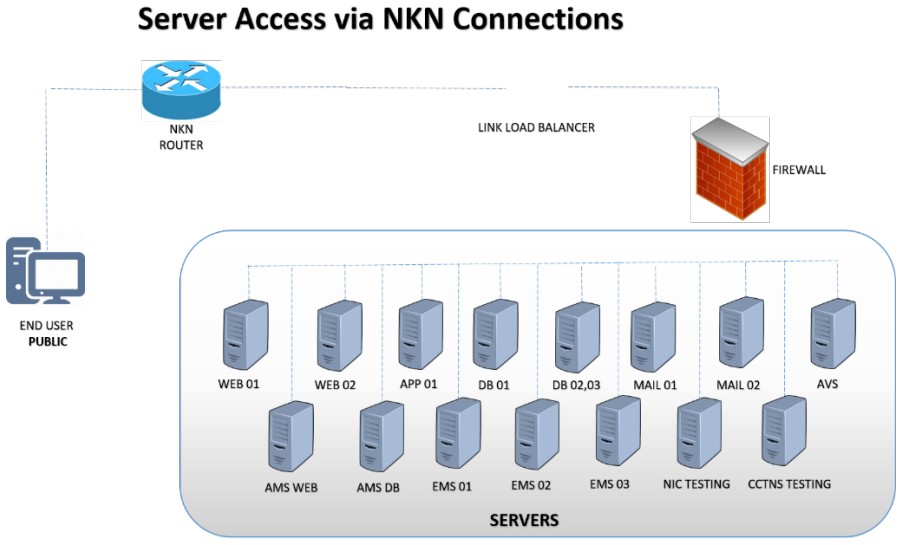
#	Make	Server Details				Physical Server Specification		
		Type of Server	Operating System	Servers	Location	RAM	Disk Space	Processor Details
1	IBM	Physical	Linux	1	DRC, Pune	128 GB	4*146 GB	Intel Xeon 10C E7-4870 130W 2.40GHZ/30 MB L3 Cache *4 nos
2	IBM	Physical	Linux	1	DRC, Pune	64 GB	4*300 GB	Intel Xeon 4C Processor model E5620 80W 2.40 GHZ/1066 Mhz/12 MB Cache*2 nos
3	IBM	Physical	Linux	1	DRC, Pune	64 GB	4*300 GB	Intel Xeon 4C Processor model E5620 80W 2.40 GHZ/1066 Mhz/12 MB Cache*2 nos

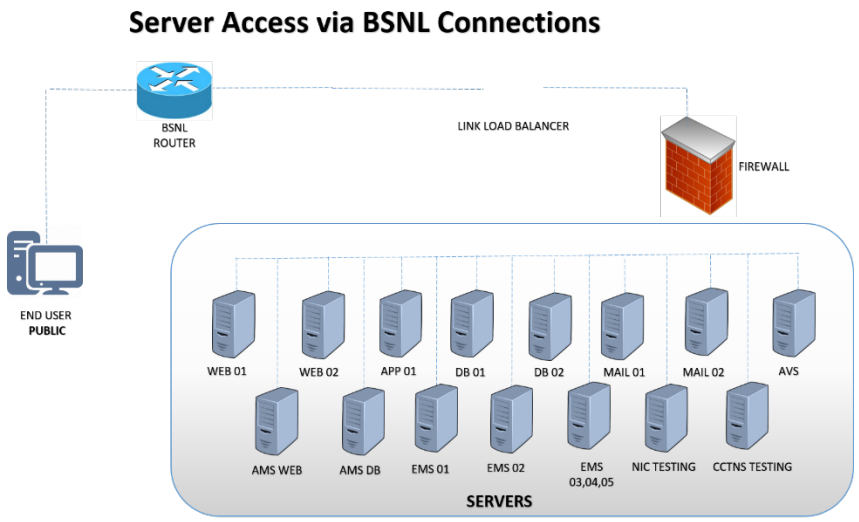
6.1.3 Existing Connectivity Infrastructure

The network connectivity for the CCTNS project was provided by BSNL through MPLS VPN connectivity from police stations till head offices and VPN broadband for rest of the offices beyond district levels.

Given below is a connectivity network architecture that is part of the existing connectivity infrastructure:







The above network architecture is currently in operation, and there is no additional connectivity setup to be done by the SI.

The above is only for reference and network connectivity setup or operation is Not under the Scope of work of the SI. For network related issues, the SI shall raise calls to the Helpdesk team and the same shall be addressed by BSNL.

6.2 Scope of Work Hardware Infrastructure

The selected SI of the CCTNS 2.0 will be responsible to procure, supply, install, commission and maintain the hardware, accessories and peripherals, servers and site infrastructure items to the required site locations of department in a phased manner as per the rollout plan described in the RFP. The list of all locations and the required quantities are mentioned in Annexure 3.

As mentioned in Section 5.1, the key responsibilities for the SI under CCTNS 2.0 hardware & infrastructure scope will be:

1) Supply, install and commission hardware items
2) Supply install and commission site infrastructure subject to site inspection by the SI.
3) Supply, install and commission servers and storage in year 2 (Phase 2)
4) Maintain -new hardware items, existing and repaired site infrastructure, existing UPS units and batteries, existing servers and storage, new servers and storage

6.2.1 Station Hardware

Station infrastructure is the fundamental tenet of CCTNS 2.0 project. The below section gives an item wise scope of work for supply, install & commissioning of the items at the stations and other units:

Desktops:

The desktops in use at the police stations currently will be replaced by new desktops. The new desktops will have a more advanced techno-functional specification in line with the latest technology trends and as specified in the technical specifications in Section 7 of Volume 1 of this RFP. The timeline of the supply of the desktop computers will depend on the rollout plan and will happen in a phased manner as detailed in Section 6.2.11.1 in this Volume of the RFP.

The supply plan has been provided in detail in the delivery schedule and rollout plan in a following section.

The detailed technical specifications of the desktops have been detailed below in Section 7 of Volume 1 of this RFP.

Printers – MFP (Multi-functional Printer) & Laser:

1) The SI shall replace all existing Laser printers in line with the phased rollout plan.
2) The SI shall replace the MFP (Multi-functional) printers as per the rollout plan and specifications given.
3) Currently 4 printer cartridges are supplied on a yearly basis per printer. The frequency of cartridges shall remain the same for the SI. Yield details has been given in the list of printer specifications.

The delivery schedule of the printers has been provided in detail below in Section 6.2.11.3.

The technical specifications of the printers have been provided in detail below in Section 7 of Volume 1 of this RFP.

UPS:

Majority of the UPS batteries were supplied in July 2019, and some UPS units were also supplied in October 2020. The SI shall:

Supply and maintain UPS units, UPS batteries and UPS (battery + units) as per the specifications mentioned in Section 7 of Volume 1 of this RFP, and as per the delivery schedule as mentioned in Section 6.2.11.2 in this volume of the RFP.

The required configuration is:

i. A 2 KVA load capacity UPS for all police stations, higher offices and special units.
ii. A 5 KVA load capacity UPS at all training centers due to high concurrent peak load capacity requirement.

The technical specifications of the UPS have been provided in detail in Section 7 of Volume 1 of the RFP

Inverter:

Under CCTNS 2.0 scope, all existing inverter units will have to be replaced with new inverter units by the SI.

The delivery schedule of the inverters has been provided in detail below in Section 6.2.11.5

The technical specifications of the inverters have been provided in detail below in Section 7 of Volume 1 of this RFP.

External Hard Disk Drives (HDDs):

As a part of CCTNS 2.0 scope, all the stations will get External HDDs since the external physical storage capacity initially supplied is obsolete and insufficient now, also with the ongoing expansive CCTNS 2.0 operations in the future, there is a need for higher external physical storage.

The delivery schedule of the External HDDs has been provided in detail below in Section 6.2.11.6.

The technical specifications and storage capacity of the External HDDs have been provided in detail below in Section 7 of Volume 1 of this RFP.

6.2.2 Site Preparation

As mentioned in Section 6.1.1 above, an estimated **15%** of the premise infrastructure items which include cabling, network racks & switches, earthing, etc. are damaged or in poor condition. Hence, as part of CCTNS 2.0 site preparation scope of work, such items have to be checked for faults, replaced or rectified.

As a methodology to execute this, the CCTNS 2.0 SI shall perform a detailed site survey and inspect the premise readiness of the stations for CCTNS operations. Further, the SI shall submit a detailed site inspection report to the department. The SI will replace or rectify (for minor fault) any site infrastructure component after necessary scrutiny of the same by SCRB.

The list of site infrastructure items is given below:

1) Electrical Cabling
2) Earthing & Earth Pit
3) Wall Mountable Network Rack
4) Network Switch (Managed/Unmanaged)
5) Patch Panel
6) Information Outlet CAT 6
7) CAT 6 with Cabling
8) Patch Cords

The site inspection report shall include a **complete checklist of parameters** for each item category, that is necessary to testify and signoff an item as 'fit for use'.

The decommissioning and disposal of existing furniture shall be internally decided by the department and the SI shall have no role to play in the same.

6.2.3 Data Center Infrastructure

The datacenter infrastructure is currently managed by ELCOT and maintenance and monitoring for SLA time, peak utilization and storage is done by the helpdesk team.

As a part of the current scope of work, the CCTNS 2.0 SI:

1) Will maintain the existing 18 IBM and 2 DELL servers procured and deployed during CCTNS 1.0, at the State Datacenter for next 1 year. The details of the servers to be maintained have been listed in Section 6.1.2
2) Will replace the existing 18 IBM servers in Year 2 (Phase 2) of this CCTNS 2.0 project with new servers with configuration as listed in Section 7 in Volume 1 of this RFP.
3) Will maintain the new servers that shall be procured in Year – 2 until end of O&M period of CCTNS 2.0 contract.
4) Will continue to maintain the existing 2 DELL servers procured during CCTNS 1.0. These servers have been procured recently and hence shall be maintained for the next 5 years, i.e., across the O&M period of CCTNS 2.0 contract.
5) Will continue to maintain the existing 3 IBM servers at DRC till the end of contract period.
6) Will maintain 3 additional new DELL make servers that were procured in Jan‘2020, till the end of contract. The specification and details of these servers have been listed in Section 6.1.2.
7) Rackspace, Power, Cooling and Network arrangement will be provided by TNSDC.
8) Will continue to monitor for peak utilization and storage and recommend the department for streamlining load, while maintaining server uptime in accordance with the SLA terms and conditions as described in Section 2.4 of SLA in Vol 3 of this RFP

The department reserves the right to deploy or redeploy servers at any given point in time with joint consultation with CCTNS 2.0 Bidder, without hindering CCTNS 2.0 project operations.

An estimated count and specification of servers required in Year 2 (Phase 2) have been detailed in Section 7 of Volume 1 of this RFP.

6.2.4 Supply, Installation & Commissioning

The SI shall carry out the following list of activities:

1) Supply of the hardware items and components and other accessories to the location as per the requirements.
2) Physical installation of Desktops, Printers UPS, Inverters, and other related hardware and accessories.

3) Operating System Installation and Configuration.
4) Existing CIPRUS (or any future versions) Application Installation and Configuration.
5) Configuring the security components in all servers.
6) Network and browser configuration.
7) Ensuring all hardware items are supplied, installed, configured, tested and commissioned, signed off and declaring the site to be operational.

The SI shall ensure that their staff presence is available at district level to attend and satisfy SLA conditions.

6.2.5 Data Backup & Restoration

All necessary backups shall be taken from the existing systems (desktops, digital cameras, external HDDs and transferred to system hard drive of newly procured and installed computers by respective station officers/ detachment teams before decommissioning them. The SI shall be legally binding by Non-disclosure and Confidentiality clauses and shall ensure there is no unauthorized transfer or destruction of data.

Data backups and restoration will be done in phased manner subject to delivery schedule as detailed in Section 6.2.11. Signoffs to be taken from State Mission Team, District Mission Teams, and / or SCRB.

6.2.6 Secure Formatting

After the required data is backed up from the existing systems, the SI shall securely format the hard disks of the existing systems.

6.2.7 Redeployment/ Disposal of existing systems

The SI shall hand over the existing systems to the station staff with complete acknowledgment for the same. The SI shall not have any further role in redeployment or disposal of the systems. The same will be done by the department in accordance with internal policies and terms.

6.2.8 Operation & Maintenance

The SI shall maintain all the systems and hardware supplied till the end of contract period. The SI shall setup a dedicated Helpdesk which shall be available over the phone as well as Web

based ticket management system. The SI shall procure and setup three customer care numbers for the users to reach out to helpdesk team. Any issues with the supplied hardware will be reported to the Helpdesk and the SI will provide resolution as per the applicable SLAs.

i. The O&M period of the existing items that were supplied by current SI (UPS batteries and units as mentioned in Section 8.5.2 (d) of Volume 1 of the RFP, existing site infrastructure) will start from the date of Issue of Work Order.
ii. The O&M period of new hardware items will start from date of completion of Supply and commissioning as mentioned in Section 6.2.8 of this document.

6.2.9 Helpdesk & Incident Management

The department is currently using an Enterprise Management System (EMS) from CA Technologies. The CA EMS tool has been in use since CCTNS 1.0 inception. The tool is used for Helpdesk and Incident management. The CA EMS tool is also used for other purposes like Asset Monitoring, Server utilization Monitoring, etc.

The licenses for the tool that were procured was Perpetual, the details of which has been mentioned in Annexure 4 in this volume of the RFP. While the licenses were Perpetual, the product support for the current version has expired and no longer provided by CA Technologies. It is therefore suggested that the SI shall either:

i. Procure support for the existing CA EMS tool and continue to use it for Helpdesk, SLA monitoring, Asset management, Incident management etc. (OR),
ii. Procure and setup a new EMS tool and use it for Helpdesk, SLA monitoring, Asset management, Incident management etc.

If the support for existing CA EMS tool is not available anytime during the contract period, the SI should procure alternate tool required for incident management, asset monitoring, SLA monitoring etc. Some of the existing customizations to the CA EMS tool tailored to the department monitoring requirements are listed below:

Call Reporting at Stations:

- Incident reporting
- Incident complaint management

- Call assignment
- Call consolidated reports
- Call reports compliant wise
- Customized MIS (including daily SLA report integration)
- Stakeholder wise reports

Infrastructure Monitoring:

- Server uptime
- Server downtime call log
- Server peak utilization
- Memory utilization
- Processor utilization

SLA:

- Call assignment to resolution
- Resolution status trackers
- Recurring issues
- Prioritization of call logs based on stations and asset categories
- Incident performance management

The logic and reporting for SLA measurement and monitoring prepared by SI from CA EMS tool/ New tool shall be verified by PMU and approved by SCRB.

The same list of functionalities shall be retained for monitoring by the SI. The Helpdesk shall be setup to receive, acknowledge and redirect calls to the concerned stakeholders like:

- Admin users – For issues or requisitions related to web application-CCTNS 2.0
- BSNL – For issues pertaining to network connectivity
- TNSDC – For issues related to Datacenter operations
- SI hardware team – For station premise hardware issues that need field support

The Helpdesk support team shall be deployed at SCRB and work closely with PMU and divisional staff of the project to resolve issues. SI may deploy additional resources based on the need of the project and also meet the defined SLAs defined in the RFP.

The detailed service levels and response time, which the SI is required to maintain for provisioning of the services are described in the Section 2.4 of SLA in Volume 3 of the RFP.

6.2.10 List of Hardware, DC/ DRC, Site Preparation Items

6.2.10.1 Hardware Items

Item delivery classification:

Items	Police Station	Special Units	Higher Office	Training Centers
Desktop (With all accessories)	Yes	Yes	Yes	Yes
UPS Units	Yes	Yes		
Printer – MFP		Yes		Yes
Printer – LP	Yes	Yes		
Inverter	Yes			
Ext. HDD	Yes	Yes		

Item delivery count (in Phase):

SNo.	Items	Phase 1	Phase 2	Phase 3
1	Desktop (With all accessories)	4334	392	1596
2	UPS Units	979	-	372
3	Printer – MFP	-	-	421
4	Printer – LP	-	-	1923
5	Inverter	-	-	1551
6	Ext. HDD	-	-	1923
7	Server	-	18	-

Phase Definition:

The CCTNS 2.0 hardware and infrastructure delivery will be completed by the SI in 3 distinct Phases. The delivery has been envisaged in 3 Phases to supply and commission the hardware in accordance to the overall wear-and-tear, prioritization of hardware supply, and rapid technology obsolescence. The phase definitions have been given as below:

Phase 1

Phase 1 will consist of procurement, delivery and commissioning of desktop computers and UPS units in batches, i.e., with every police station having a capacity and sanction for 4 desktop computers, 2 will be supplied in Phase 1 and the remaining in Phase 3. Similar rollout plan for UPS. Detailed rollout plan has been described in Section 6.2.11

Phase 2

Phase 2 will consist of supply, delivery and commissioning of new servers at the state Datacenter for use by the CCTNS 2.0 project. Detailed specification of the servers has been mentioned in Section 7 of Volume 1 of RFP

Phase 3

Phase 3 procurement, delivery and commissioning will entail desktop computers, UPS units, printers, inverters and external HDDs across all stations and other offices as mentioned in the rollout plan in Section 6.2.11

In accordance with the above, and SLA, payment and project milestones, 3 different work orders will be issued by SCRB to the SI in a phased manner.

***Note*:**

The Bill of Material for hardware items is mentioned based on the existing Police Stations, Higher Offices, Special Units & Training centres in the state. The SI shall supply hardware items at the same quoted price to any new Police Stations that may come up in the state during the three phases of supply. The Operations & Maintenance expenses for hardware items supplied to the new Police Stations shall be calculated on a pro rata basis.

6.2.10.2 Data Center/ Disaster Recovery Center

Servers are installed at State Datacenter, maintained and operated by ELCOT. Currently the existing servers and storage suffice the requirements for functioning of CCTNS.

For the 2nd phase of the project, i.e., Year 2, an estimated 15 servers shall be commissioned and deployed by the SI at the State Data center. For detailed specifications of servers to be procured in Year 2, please refer Section 7 of Volume 1 of this RFP.

For details regarding the server count, please refer below table:

Item	Place of deployment	Item type	Count
Server	ELCOT SDC Chennai	RACK-2U- 4 PROCESSOR (APPLICATION/ WEB SERVER)	11
		RACK-2U- 4 PROCESSOR (DATA BASE SERVER)	4
Server	DR Pune	RACK-2U- 4 PROCESSOR (DATA BASE SERVER)	2
		RACK-2U- 4 PROCESSOR (APPLICATION/ WEB SERVER)	1

6.2.10.3 Site Preparation Items

SNo.	Items	Details
1	Electrical Cabling	As described in Section 7 of Volume 1 of this RFP, all site infrastructure items as mentioned alongside shall be rectified or replaced subject to site inspection report and station complaints during site preparation setup before hardware commissioning.
2	Earthing & Earth Pit	
3	Wall Mountable Network Rack	
4	Patch Panel 12 Ports CAT 6	
5	Network Switch 16 Ports 10/100	

6	Information Outlet CAT 6	
7	Cat 6 Cable with Cabling (In Meters)	
8	Patch Cords 1 Mtr. CAT 6	
9	Patch Cords 2 Mtr. CAT 6	

6.2.11 Hardware Distribution Details

6.2.11.1 Desktop Distribution Details

Types of Station	Total Station	Total Units / PS	Total Count	Phase 1		Phase 2		Phase 3	
				Units	Total	Units	Total	Units	Total
Heavy PS	391	4	1564	2	782	-	-	2	782
Medium PS	326	3	978	2	652	-	-	1	326
Light PS	834	2	1668	2	1668	-	-	-	-
Special Unit	372	2	744	2	744	-	-	-	-
Higher Offices	488	2	976	1	488	-	-	1	488
Training Center	49	8	392	-	-	8	392	-	-

6.2.11.2 UPS Distribution Details

1. UPS Units:

Types of Station	Total Station	Total Units / PS	Total Count	Phase 1		Phase 2		Phase 3	
				Units	Total	Units	Total	Units	Total
Heavy PS	391	1	391	1	-	-	-	-	-
Medium PS	326	1	326	1	181	-	-	-	-
Light PS	834	1	834	1	798	-	-	-	-

2. UPS Units inclusive of Batteries

Types of Station	Total Station	Total Units / PS	Total Count	Phase 1		Phase 2		Phase 3	
				Units	Total	Units	Total	Units	Total
Special Unit	372	1	372	-	-	-	-	1	372

6.2.11.3 Printer – MFP Distribution Details

Types of Station	Total Station	Total Units / PS	Total Count	Phase 1		Phase 2		Phase 3	
				Units	Total	Units	Count	Units	Count
Special Unit	372	1	372	-	-	-	-	1	372
Training Center	49	1	49	-	-	-	-	1	49

6.2.11.4 Printer – LP Distribution Details

Types of Station	Total Station	Total Units / PS	Total Count	Phase 1		Phase 2		Phase 3	
				Units	Count	Units	Count	Units	Count
Heavy PS	391	1	391	-	-	-	-	1	391
Medium PS	326	1	326	-	-	-	-	1	326
Light PS	834	1	834	-	-	-	-	1	834
Special Unit	372	1	372	-	-	-	-	1	372

6.2.11.5 Inverter Distribution Details

Types of Station	Total Station	Total Units / PS	Total Count	Phase 1		Phase 2		Phase 3	
				Units	Total	Units	Total	Units	Total
Heavy PS	391	1	391	-	-	-	-	1	391
Medium PS	326	1	326	-	-	-	-	1	326
Light PS	834	1	834	-	-	-	-	1	834

6.2.11.6 Ext. Hard Disk Drive (HDD) Distribution Details

Types of Station	Total Station	Total Units / PS	Total Count	Phase 1		Phase 2		Phase 3	
				Units	Total	Units	Total	Units	Total
Heavy PS	391	1	391	-	-	-	-	1	391
Medium PS	326	1	326	-	-	-	-	1	326
Light PS	834	1	834	-	-	-	-	1	834
Special Unit	372	1	372	-	-	-	-	1	372

6.2.11.7 Server Installation Details

Types of Station	Total Station	Total Units	Total Count	Phase 1		Phase 2		Phase 3	
				Units	Count	Units	Count	Units	Count
Server	1	15	15	-	-	1	15	-	-

6.2.12 Delivery Challan and Installation Note

System Integrator will supply and install the hardware items to the ultimate consignee and shall obtain the signature in the delivery challan and installation note after confirmation of technical specification of the hardware items by the authorized person. The above procedure shall be carried out to check whether the items are in conformance with the technical specifications attached to the work order and as per the General conditions of contract.

7. CCTNS 2.0 Web Application Software

Tamil Nadu Police department has envisaged a new web-based application that would replace the current CIPRUS application that is based on a client server architecture. The SI scope of work will be to design and develop the complete end-to-end application with all the required modules and integration functionalities. The details have been described in the sections below:

Section in Document	Module Category	SI Scope of Work
7.1	System Overview	*For reference*
7.2	Core Modules	Design and development
7.3	Core Admin Module	Design and development
7.4	Tools on CCTNS Platform	Design and development
7.5	Integration with SCRB Applications	Web service/API integration
7.6	Integration with Central Systems	Development, Web service/API integration
7.7	Integration with other Systems of TN Police	Web service/ API integration
7.8	Integration with other Department Databases	Web service/ API integration
7.9	Integration with Communication Channels & Payment Gateway	Web service/ API integration

A detailed outline and description of the modules and sub-modules have been given in the above-mentioned sections in subsequent chapters in this volume of the RFP document.

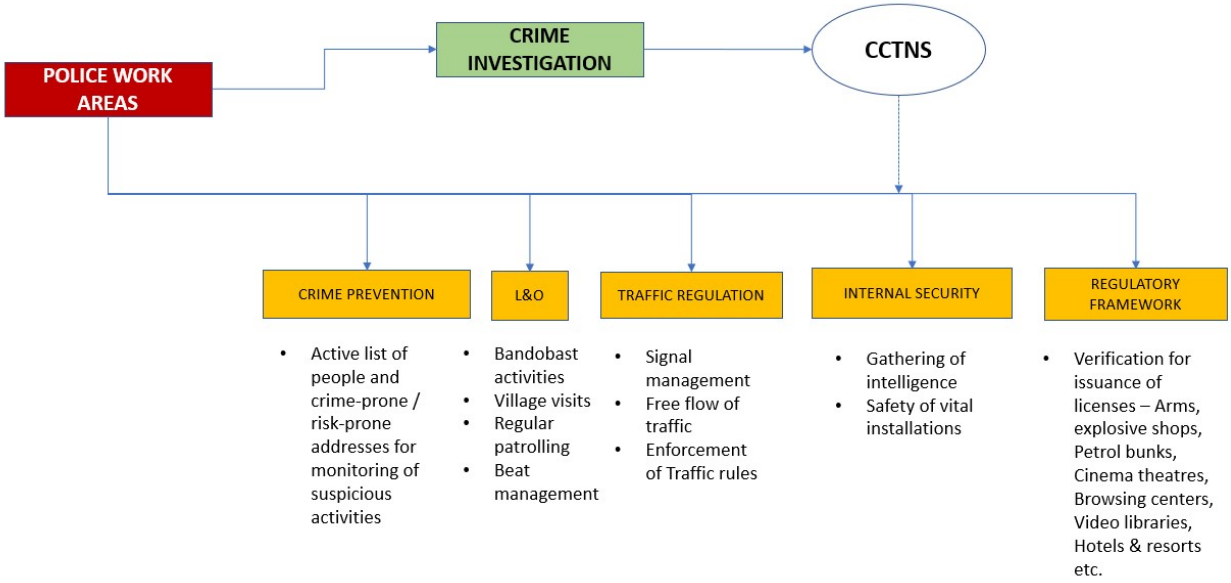
7.1 System Overview

It is for reference and understanding of the Bidder that a system overview has been given as outlined below:

S.No.	Sections	Description of the Section
7.1.1	Major functions of Police department	This section gives a high-level picture of the broad areas of work of TN Police
7.1.2	Investigation and Station	This section gives an understanding of investigation

	registers	records and its relationships with other station registers
7.1.3	About CCTNS and its objectives	This gives a brief on CCTNS project and objectives to be met
7.1.4	Current CIPRUS system of CCTNS	This section gives a brief on the current CIPRUS application
7.1.5	Challenges with the existing system	This gives a list of major challenges with the current CIPRUS and the need for a better techno-functional system
7.1.6	Scope of work overview	This section gives a list of the modules to be designed, developed and integrated

7.1.1 Major functions of Police Department



The above diagram depicts the major work areas of the police department. The work of the department can be divided into investigation and non-investigation duties. A further classification of the same is given below:

1. Crime Investigation is the most important work of the department. An investigation starts once FIR is registered based on complaint received at a police station or through citizen

services portal. It includes all the proceedings for collection of evidence by the police officer when a crime is reported.

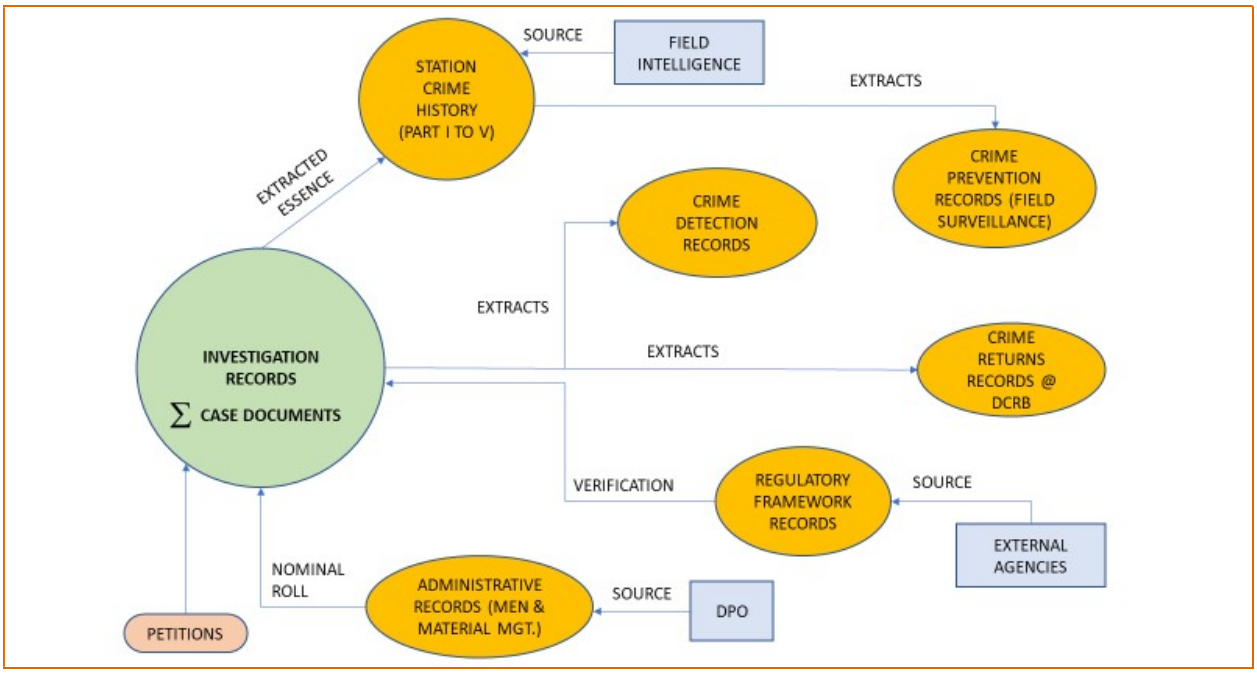
2. Crime Prevention relates to regular surveillance and monitoring of crime prone areas, ex-offenders and suspects to prevent occurrence of crimes. This monitoring helps to prevent and control criminal activity.

3. Law & Order (L&O) activities are done to ensure civic discipline is maintained in a jurisdiction by conducting proactive routine check activities. Such activities include – Bandobust activities for VIP movement and festivals /other public events which involve large crowds. It also includes village visits, regular patrolling at designated or crime prone locations, etc. These activities ensure public safety through needful surveillance.
4. Traffic Regulation is done to ensure decongested free movement of vehicles on roads. During traffic regulation, enforcement of traffic rules and registration of motor vehicle petty cases in event of violations, is also carried out. Awareness programs are conducted for the citizens regularly as part of efforts to prevent and reduce accidents.

5. Internal Security refers to surveillance based on intelligence gathered from the field and other external agencies. These activities help the department to minimize risks and threats to VIPs/ vital installations/ places of historic importance/ safety of general public by terrorists/ anti-social elements.

6. Regulatory Framework refers to verification activities that are conducted by the department regarding the criminal antecedence and other parameters for recommending for issuance of license for Arms, Explosive shops, Petrol bunks, Cinema theatres, Browsing centers, and Video libraries, Hotels /Resorts to commercial establishments. The Police department checks and monitors active licensure to function or sell services. These activities ensure all citizens and businesses have required permit to conduct any commercial business.

7.1.2 Investigation & Station Registers



The above diagram shows the various sources or points of generation of the data which results in creation of registers in the police station. The diagram clearly depicts the importance of investigation records which is major source for registers in the police station while the field intelligence, external agencies and the DPO also contribute but a minor part of data to the registers.

In the manual set up, during the investigation, documents were created, and then data was entered in various related station crime registers. However, with automation, once the documents are created, the relevant registers should get auto populated. The data from these registers form the basis for carrying out activities in the field like field surveillance/beat patrolling, antecedent verification, crime returns to senior officers of Police Department and to external agencies as and when requested.

Classification of Station Records

The station crime records are extracted from investigation records. These registers help in monitoring the crime occurrence and to undertake preventive measures like field policing in crime prone areas and bad character check to keep in surveillance the ex-convicts in the jurisdiction.

1. Crime detection records are used for detection purpose. Examples: Name War Index, Loose Leaf Index, etc.

2. Crime prevention records & Station crime history records: The station crime history registers are given below -

    Part 1- True occurrence registers (aggregation of all property crimes)

    Part 2- Crime charts (hotspots and maps)

    Parts 3- General conviction register (all conviction details)

    Part 4- Village history sheets

    Part 5- Bad character check register

    The crime prevention records are a subset of station crime history which concerns lists such as people and locations which are active in the database. These locations may be prone to crime as on date, and the people in the crime records are those who are suspicious or currently involved in criminal activities. These records help to keep vigil and plan crime preventive activities.

4. Crime returns records are statistical reports on various categories of crimes that are collected and consolidated by DCRB (District Crime Records Bureau) /SCRB (State Crime Records Bureau) for analytical and detection purposes. These returns are shared with other government agencies, researchers and academicians also as and when requested.

5. Regulatory framework records are databases of Gun licenses, Explosives shops, Petrol bunk license, Hotels and resorts, etc. in the police station jurisdiction. These records are built as and when requests are received from the respective authorizing agencies for issuing licenses. In order to conduct verification when such requests are received, the data in station crime registers and detection registers are helpful.

6. Administrative records are non-investigation records which deal with men and material information pertaining to stations and other department units. The source for this data is the district/city Police headquarters (District Police Office/Commissionerate in

Cities)/headquarters of Special Units/Police headquarters. This data is helpful in assigning duties/ roles to the police station staff and for creating user privileges.

7.1.3 About CCTNS and Objectives

CCTNS is a Mission Mode Project (MMP) under the National e-Governance Plan (NeGP) of Government of India. It was conceptualized and sponsored by the Ministry of Home Affairs (MHA). National Crime Records Bureau (NCRB) is the central nodal agency for managing the nationwide implementation of this project and the respective State Crime Records Bureau (SCRB), the State Nodal Agency for implementation in the State.

The CCTNS was envisioned as a system which shall allow access to real-time crime and criminal information. The focus was to make investigation record management more efficient, thus enabling the reporting, crime and criminal case analysis, supervisory management, field force management and deployment easier.

There are several objectives for which the CCTNS project was envisaged as mentioned below:

i. Provide enhanced tools for crime investigation, crime prevention, law and order maintenance and other regulatory functions:

a. Utilize IT for efficiency and effectiveness of core policing operations

b. Provide information for easier and faster analysis and trends

ii. Create a national platform for sharing crime and criminal information and intelligence across the country in between state and central and external agencies

iii. Improved services for general public and other institutions such as:

a. Access to police services in a citizen-friendly manner

b. Provide fast, accurate and digital modes of service delivery

7.1.4 Current CIPRUS System of CCTNS

To fulfill the objectives of the CCTNS project, data capture and building up of a database of crimes and criminals is a basic necessity. Police stations, being the point of generation of data, an application was developed and put in place in all police stations for data entry.

NCRB developed the CAS (core application software) and offered it to the states for customization to suit their requirements. Tamil Nadu opted to go for its own state CAS, named CIPRUS (Common Integrated Police Records Updation System). The data is being shared with NCRB for enabling nation level database building and also to activate national searches.

Some of the features of the currently functioning CIPRUS application are given below:

1. The current CIPRUS is an application primarily used to capture crime and criminal related data during investigation resulting in building up of database.
2. It is built on a client server architecture and is a workflow-based application.
3. It is developed using the Java Wicket framework and PostgreSQL database.
4. The information captured is used to generate documents and reports at the police stations. Certain case related documents like FIR, Arrest card and charge sheet are being generated through CIPRUS and submitted in the courts. It is also being used for detection of cases and for crime prevention measures during field policing.
5. A bunch of online services have been enabled for citizens and police officers using CCTNS data. The services are being accessed through the web portals and mobile apps.
6. The application is rigid and allows user to enter information under various case events in a sequential manner.

Due to the rigid nature of the application, client server architecture and a complex database structure it is faced with many challenges which has been described in the next section.

7.1.5 Challenges with the Existing System

The state CAS that was developed by the department is currently being used by all FIR registering units (police stations/special units) in the state. The application has served to some extent in fulfilling the objectives of CCTNS. However, it still fails to address some key requirements of the department due to its client server architecture, database design issues

and the system design approach. Some of the key techno-functional challenges are as follows:

Important data fields related to person, property, place and crime are optional for entry by the user, e.g., Identity No of accused, Occupation of accused/victim, Photograph of accused/missing person, physical features and Identification marks of Missing person / UIDB, Vehicle registration details, etc. Hence, important information is unfilled or partially filled which limits the effectiveness of the platform.

The structure of the database is complex by design and many data fields are entered redundantly in multiple case events without any correlation to workflow logic.

The application architecture is rigid in nature, i.e., it allows users to enter data using a sequence of case events. If an information is not available, the user has no option to return to it when it is available. Also, since most data fields are optional to enter, users mostly skip filling it and keep it null and making it difficult for the investigating officer to track it later.

The workflow does not have well laid out rules for data correction and validation. For example, all correction requests are sent to SCRB and corrections are done manually after forwarding request to the software developer. There are no automated approval workflow & minimal admin rights, no provision in the system to ask the user reason for correction and review or approve the reason later.

For minor corrections/updation like addition of new PS, new Act & section, making a field mandatory etc, the entire application version is upgraded to a new version. This involves testing of all functionalities again, which makes the process time consuming.

The architecture is based on a client-server model and an outdated framework (Java Wicket) which makes data sync and sharing difficult. It also makes web service and API integration difficult. Even SMS services are not real time but run in scheduled manner.

There is no system diagnostic tool, analytical or reporting tools that will help the supervisory officers in analysis and supervision. Diagnostic tool as proposed in the envisaged system will help trigger system alerts and pop up messages on user actions, automatically correct logical errors and leverage the communication module to notify the user. Analytical and reporting tools help in building custom or dynamic reports, generate and display intuitive dashboards.

The current system does not have these features. A detailed list of such system functionalities has been described in Sections 7.3

7.1.6 Scope of Work Overview

The below table shows the list of modules which need to be developed and integrated with the web application by the SI:

S.NO	CATEGORY	MODULE	SCOPE OF WORK
1	**CORE MODULES**	a) FIR Registration b) Investigation c) Prosecution d) CSR e) Regulatory Framework	The SI shall design and develop the listed modules which forms the core data capturing modules of the web application
2	**CORE ADMIN MODULES**	a) Form Builder b) Report Builder c) Nominal Roll d) Query Builder e) Dashboard Builder f) System Diagnostic Tool g) Administrator Rights & Privileges h) Master Data Management (MDM) i) Data Capture, Correction & Validation	The SI shall design and develop the listed modules which form the core data admin modules of the web application

		j) User role & Privileges k) Platform Usage Analytics l) Communication Module – Emails, Alerts, Chats	
3	**TOOLS & PORTALS ON CCTNS PLATFORM**	a) Missing Person UIDB Tool b) History Sheets module c) Station Crime History d) Bandobust Manager e) Citizen & Officer portal 1.Citizen Services Portal 2. Officers Portal f) Mobile Application development for 1) Citizen services portal 2) Officers portal 3) Bandobust Manager 4) SoC details in Investigation module 5) Search Features: Accused Name Search, IMEI Search, Vehicle details search g)Unified Calendar	New design and development of all the tools. Though the Missing Person UIDB tool, citizen services and officers' portal are existing tools, the SI shall study the existing system and design new tools with features as mentioned in Section 7.4 of this volume of the RFP

4	**INTEGRATION WITH SCRB APPLICATIONS**	a) Crime Analytics Tool b) Facial Recognition c) Tollscope d) Fingerprint Database (FACTS/AFIS) e) E-beat System	The listed applications are already developed, and the SI's scope covers the development of APIs/webservices for integration of listed applications with CCTNS platform to exchange data
5	**INTEGRATION WITH CENTRAL SYSTEMS**	a) ICJS b) NCCRP c) DMU Mapping	The SI's scope covers the development of APIs/webservices for integration of ICJS and NCCRP application with CCTNS platform to exchange data. However, the SI shall design and develop the DMU mapping tool for sharing data with central agency/ NCRB
6	**INTEGRATION WITH OTHER SYSTEMS OF POLICE DEPARTMENT**	a) SPMCR b) E-Challan c) RADMS/iRAD	The SI's scope covers the development of APIs/webservices for integration of listed applications with CCTNS platform to exchange data
7	**INTEGRATION WITH EXTERNAL DATABASES**	a) Vahan & Samanvay b) Personal Identity Databases like Aadhaar, Voter ID, Ration Card, Passport, PAN etc. c) Regional Transport Office d) Hospitals & Health Centers	The SI's scope covers the development of APIs/webservices for integration of listed databases with CCTNS platform to exchange data

		e) Licensing Authorities (ALIS, other systems) f) Revenue, Tax, Census etc.	
8	**INTEGRATION WITH COMMUNICATION CHANNELS & PAYMENT GATEWAY**	a) E-mail b) Short Messages c) Payment Gateway (PayGov/ any gateway assigned by TN Police)	The SI's scope covers integration of listed communication channels with CCTNS platform

The SI has to develop the CCTNS 2.0 web application as per the indicated scope of work mentioned in Section 7.1.6 and need to ensure that developed web application System is 100% compliant with the requirements and specifications provided in the RFP such as ***functional, non-functional, security & technical requirements and overcome all the challenges in existing system as mentioned in section 7.1.5***

The envisaged web Application- CCTNS 2.0 should be developed based on the design principles as mentioned in Annexure 1 of this RFP. The SI also needs to develop a mobile application as mentioned in Section 7.4.7 with selective features that are required to be filled/updated by officers on the field. The functional requirements for the web application are broadly outlined in this RFP however the SI shall capture the detailed requirements during the requirement gathering phase through focussed group discussions, interviews with concerned stakeholders prior to SRS preparation.

7.2 Core Modules

The Core modules will form the primary area where information will be captured in the system. There will be other tools and portals that will consume and use this data as explained under Section 7.4. The SI shall design & develop these primary modules which includes FIR Registration, Investigation, Prosecution, CSR (Non-cognizable offences) and Regulatory Framework. A brief description about the modules as well as tools on CCTNS platform to gain a

broad understanding of the various features required has been illustrated in the below sections. However, detailed inputs on required data fields in every module/sub module and the workflow will be provided during the Requirement Gathering phase prior to SRS preparation.

7.2.1 FIR Registration

Outline:

A case timeline will usually start with a complainant visiting a police station or citizen services portal to file a complaint. For all cognizable offences, the station officer notes the complaint details and registers the complaint in the system. A new FIR is opened, and all the details required in the FIR form (Integrated Investigation Form - I) is filled in. The system generated FIR is signed by the investigating officer and a copy of the same is handed over to the complainant. The complainant also signs the FIR copy. Once the FIR is registered, the investigation process commences.

SI Scope of Work:

During the FIR registration process, the officer will go through one or more of the following events:

1. Add new FIR
2. Pending FIR
3. Update FIR
4. View FIR

The details of the FIR will vary depending on the type of the cognizable offence, the related case type and section of law. The SI shall develop the functionalities as illustrated below:

FR No.	Sub Module	Functional Requirement
FR 1	Add new FIR	The FIR registration form should be generated in the same format as the Integrated Investigation Form -I.
FR 2	Add new FIR	The user should be able to capture all / any of the required data based on the category of crime which will be determined by complaint given by the complainant. Certain fields shall be mandatory in the FIR form which will be defined by the client.

FR 3	Add new FIR	The user should be able to save a FIR, get approval of the senior officers and then generate the final copy. Once the final copy is generated, changes should not be allowed by the system.
FR 4	Add new FIR	In the case the complaint does not belong to the jurisdiction where the complainant is registering the complaint, the user should be able to generate the FIR number and then transfer the FIR to the jurisdiction concerned.
FR 5	Pending FIR	In case the application or module is unavailable for FIR registration, the system should auto-save the form with the partially filled entries as draft and store it in a separate folder for retrieval after the online application is made available again. If the user tries to register a new FIR or update any other pending FIR, system should prompt the user to complete the previous pending FIR. If the user wants to skip the pending FIR, system should ask the user to enter a reason. Again, during next login, the system should prompt the user of all the pending draft FIRs yet to be frozen/finalized.
FR 6	Pending FIR	The Pending FIRs should be stored with an identifier for each search, e.g., Date, Jurisdiction, Offence type, etc.
FR 7	Pending FIR	The system should allow the user to search for a particular Pending FIR, invoke the form and continue to complete the new FIR registration.
FR 8	Update FIR	The system should not allow any update to FIR after the data has been finalized & frozen and sent to court.
FR 9	Update FIR	The system should integrate with the Admin data correction Module in case any update/modification needs to be done after an FIR has been finalized/frozen .
FR 10	Update FIR	In such a scenario, a workflow logic has to be built that will enable sending correction requisition by the field staff to SCRB through help desk. The help desk shall forward the software related requests to SCRB admin level 3 officer who shall be able to enable corrections/modifications only after obtaining approval of the Admin level 2 officer and Super admin at SCRB. Logs of all such changes should be maintained for future references.
FR 11	Update FIR	Such update requests should also be integrated with the Communication Module so that clarifications can be requested or provided.
FR 12	View FIR	The system should allow different formats for the user to view the FIRs such as

		1. Summary FIR view 2. Detailed FIR view 3. FIR view by offence type 4. FIR view by section of law 5. FIR view by date 6. FIR view by investigation officer etc.

7.2.2 Investigation

Outline:

The next step in the process after a FIR is registered is Crime investigation. The investigation process runs through multiple case events (which form the sub-modules) such as Accused/Victim/property details, Inquest details, arrest card etc. Some of the events are undertaken by investigation officer, while some are dependent on external parties and experts. Information captured could be used to generate a document or used for detection/analytical purposes. There are multiple events under the investigation process.

SI Scope of Work:

1. The SI will study the system to design data capture forms for various events in the cases.
2. The system design should be flexible allowing the user to add any information at any point in time pertaining to case events as listed below, with necessary checks and balances.
3. The forms should have built in logic for upstream and downstream data entry, data fields marked as mandatory or optional depending on the criticality and usage of the information.
4. The system should have provision for geo tagging of locations by the officer from his mobile phone.
5. The system should have provision to *upload audio-video clips* of witness statement, confession statement, **CCTV footages** etc. in the relevant sub modules/case events.
6. The system should have provision to **add more case events (sub modules)** as this will vary depending on nature of the case and future changes /additions legal framework and

investigation processes. Case events will be peculiar to different category of crimes as well. The case events listed below is illustrative and not exhaustive.

7. All design principles for data capture, validation, etc. as described in Annexure 1 will apply throughout the design and development stage

FR. No.	Sub-Module	Functional Requirements
FR 1	Accused Victim Property Details	The system should allow the user to add an accused or victim or property during the course of investigation
FR 2	Injured Person Statement Recorded / Dying Declaration	The system should allow the user to record the statement on a field device and upload information to the web application or through mobile application directly.
FR 3	Inquest Details	The system should allow the user to enter inquest information to know the apparent cause of death
FR 4	Alteration Report	The system should allow the user to change the sections of law based on the outcome of the investigation
FR 5	Investigation Closed / Stopped	The system should allow the user to record the reason why an investigation is closed or stopped
FR 6	Arrest Card	The system should allow the user to generate arrest card which is sent to court
FR 7	Investigation Reopened	The system should allow the user to record why an investigation is reopened for investigation
FR 8	Bail / Details of the Sureties	The system should allow the user to record bail and sureties' details
FR 9	Missing Person Traced / Matched with UIDB Status	The system should allow the user to record the status of missing person
FR 10	Missing Person Traced / Matched with UIDB Status	The system should integrate with the Missing Person / UIDB matching tool explained in Section 7.4.1 and allow the user to push or pull information from the tool as

		required.
FR 11	Case Transferred to other IO / Police Station through Court / Agency	The system should allow the user to record information why, when and to whom a case is transferred.
FR 12	Prayer for Remand	The system should allow the user to generate the Remand Report which is submitted before court
FR 13	Confession Statement	The system should allow the user to record confession statement given by the accused
FR 14	Property Sent to Magistrate [Form 95]	The system should allow the user to send seized property along with the seizure mahazar, in the specified format
FR 15	Dead body Handed over to Relative / cremated after PM	The system should allow the user to record details to whom the dead body is handed over after postmortem
FR 16	Requisition Letter	The system should allow the user to send requisition letter to other agencies like Hospitals, RTO, Forensic Department, Courts etc (in standard format and relevant data fields auto populated) to get expert opinion.
FR 17	Dead body sent for PM	The system should allow the user to record when & why the dead body is sent for postmortem
FR 18	Search Proceedings – 165 CRPC	The system should allow the user to record the details about the permission obtained for the search & details collected during search
FR 19	Death of Injured / Missing Person	The system should allow the user to record the date and time & place of death of missing / injured
FR 20	Seizure Mahazar Form	The system should allow the user to record the Date, Time, place & seized property details about the seizure of the property
FR 21	Details of Investigation at SOC (Scene of Crime)	The system should allow the user to record the exact details about the place of occurrence and also record the motive,

		methods etc. which was used to commit crime. Provision to geo-tag the location so that latitude and longitude of scene of crime is recorded.
FR 22	Test Identification Parade	The system should allow the user to record the details about the TI parade conducted
FR 23	Exhumation Details	The system should allow the user to record the details about the place, date, time of exhumation and also about the permission given by, doctors conducted PM
FR 24	Final Report / Charge sheet Generated	The system should allow the user to generate Final Report of a case
FR 25	Final Report / Chargesheet Returned from the PP	The system should allow the user to record the details about final report returned by PP
FR 26	Update Complainant / Witness / Accused / Victim Details	The system should allow the user to update the details about the complainant and accused during course of investigation
FR 27	Final Report / Charge sheet Sent to the PP	The system should allow the user to record Date of final report sent to PP for approval
FR 28	Witness Statement Recorded	The system should allow the user to record the witness statement
FR 29	Final Report / Charge sheet Taken on File / Returned by the Court	The system should allow the user to record the reference number given by the court after court taking cognizance
FR 30	General	The system should have provision to upload documents/reports/request letters such as bail order, expert opinion for handwriting etc. in respective submodules

For Bidder reference, given below is an indicative process flow of a case under standard scenario and some events that relate to specific cases:

Process flow of a case	Additional events that may apply for heads like Murder, Accident, etc.
1. Registration of FIR 2. Visited the Scene of Crime 3. Collected evidence at SOC 4. Prepared Rough Sketch & Observation Mahazar 5. Prepared Seizure Mahazar 6. Examination of witnesses 7. Arresting of accused 8. Confession Statement recorded 9. Prepared Seizure Mahazar 10. Accused sent to judicial custody 11. Objection petition filed against the Bail petition filed by accused 12. Captured bail details (if granted by court) 13. Prepared Alteration Report and sent to court (if necessary) 14. Examination witnesses including expert witnesses 15. Prepared Final Report 16. Obtaining opinion from Public Prosecutor 17. Filing Final Report before court 18. Obtaining Court reference number for a case	1. Conducted Inquest (if the case having deceased details) 2. Sending dead body for post-mortem 3. Collecting samples & weapons and sent to FSL 4. Handed over the dead body to relatives 5. Obtaining PM report & FSL report 6. Sending vehicle to Motor Vehicle inspection (for Accident cases) 7. Collecting Fingerprint report 8. Examination expert witnesses

The above-mentioned events can be captured in any sequence by the investigating officer. The system should allow data entry in any order with minimum dependencies.

7.2.3 Prosecution

Outline:

The third step after completion of case investigation is Prosecution. In this module, details of trial of a case in Court will be captured after a case has been taken on file by court.

SI Scope of Work:

1. All the points mentioned in Section 7.2.2 under Scope of work will apply here.
2. Additionally, the prosecution module will involve sharing of information to and from the courts. The SI shall perform system design and development keeping in view the data fields that will require information interchange with the courts system which may involve both manual entry & online transfer through web services integration.

Given below is a list of Prosecution events and the purpose for each event:

FR. No	Sub-Module	Functional Requirements
FR 1	Split FIR / Charge Sheet	The system should allow the user to record the details about the split charge sheet details
FR 2	Commencements of Proceeding in Court	The system should allow the user to record the hearing details of a case
FR 3	Committal / Transfer of Case	The system should allow the user to record the details about the committal or Transfer of a case
FR 4	Summon / Warrant Issued by the Court	The system should allow the user to record the details about the summon / warrant issued by the court
FR 5	Summon Served / Warrant Executed	The system should allow the user to record the details of work done by the police on the issuance of summon / warrant issued by the court
FR 6	Property Attached	The system should allow the user to record the Attached property details
FR 7	Proclamation of Offender	The system should allow the user to record the Proclamation of an accused issued by the court
FR 8	Court Disposal	The system should allow the user to record the disposal of a case given by court

FR 9	Details of Conviction Memo	The system should allow the user to record the Conviction Memo details
FR 10	Appeal Filed in the Court	The system should allow the user to record the filing of Appeal in court
FR 11	Details of RCN / NCN	The system should allow the user to record the Details of RCN assigned by the FP Bureau
FR 12	Attachment Order	The system should allow the user to record the Property Attachment order issued by the court
FR 13	Announcement of Reward for Information on Accused	The system should allow the user to record the announcement of reward details by the court

Given below is a general sequence of case events during case prosecution for Bidder reference.

1. Court Proceedings commencement
2. Capturing hearing details
3. Receiving summons from the court
4. Service of summon to witness and accused
5. Issuance of warrants by Courts
6. Execution of the summons and warrants
7. Production of witnesses and accused before court
8. Capturing disposal for the case given by court
9. Appeal

7.2.4 CSR (Non-Cognizable Offence)

Outline:

Citizens come to police stations for a range of complaints. The categorization of a complaint depends on its narrative and other details. All complaints are categorized as under Cognizable or non-Cognizable offence. For non-cognizable offences, wherein a police officer cannot arrest

without warrant, a CSR is registered. A CSR (community service register) is maintained in every police station for petty crimes which does not fall under category of "Cognizable offences"

SI Scope of Work:

The SI shall design and develop the CSR module to register CSRs in the police stations. The system should adhere to the following functional requirements:

FR No.	Sub Module	Functional Requirement
FR 1	CSR Registration	The system should allow the officer to enter details of the petition, petitioner, counter petitioner and other details including content of petition.
FR 2	CSR Registration	The system should generate a unique CSR No. automatically in sequential manner. Once CSR is created, system should not allow the user to edit the CSR Number or delete the CSR without permission and approval of supervisory officers.
FR 3	CSR Registration	The system should allow user to generate CSR receipt and print and sign the same. There should be provision to digitally sign the CSR receipt as well. The signature will be issued only after successful OTP authentication of the CSR issuing officer using his unique Aadhaar number to access eKYC of the UIDAI server and triggering OTP to the officer/s verified mobile number. In case of manual authentication, system should allow scan and upload of the signed CSR copies.
FR 4	CSR Registration	The system should store the receipt in the document database marked and physically scanned.
FR 5	Disposal of CSR	The system should have capability to enter and update the disposal of a CSR.
FR 6	Disposal of CSR	The system should have the capability to send CSR status to the complainant using SMS notification or email
FR 7	Disposal of CSR	The system should have the capability to dispose CSR after department approval and enter closure information, disposal status and action taken to the complainant
FR 8	General	The CSR module should have an end to end workflow from the start of registration of CSR to final disposal in the system.
FR 9	General	The system should allow the user to link the CSR to an FIR which has been

		registered already for the same matter or an online complaint for the same matter.
FR 10	General	The system should also have the capability to allow the user to monitor a person involved in a CSR by keeping him/her under 'Watch List' if his current action needs to be kept under surveillance for possibility of future cognizable crimes.

7.2.5 Regulatory Framework

Outline:

The module comprises of details of arms licenses and various institutions/ hotels / shops/ theatres / etc. which run on license from govt. The police department needs to keep track of such institutions/ hotels / shops/ theatres / etc. to ensure license is valid and no illegal activities are being done. The police department is one of the stakeholders in the issue of licenses for the said institutes. CCTNS data is used for verification of antecedents of the applicant who runs these institutes. Further, after capturing the details, these locations should be part of the village history register for monitoring the same during crime prevention activities. The system should throw alerts for expiry of license. Some of institutes which fall under the regulatory framework are given below:

a) Arms
b) Explosive shops
c) Petrol bunks
d) Cinema theatres
e) Internet browsing centers
f) Video libraries
g) Hotels and resorts, etc.

The primary stakeholders concerned during the above regulatory checks are:

1. Owner or license holder of the establishment
2. Jurisdiction in-charge officer of the department
3. Licensing authority

The licensing authorities are many, license types and establishments are numerous. Hence, it is difficult and time consuming to check validity of licenses.

As a solution, the SI will design and develop a module which will enable the department to keep a check of license validity, nabbing of offenders operating establishments with expired license or fake license, etc.

The modules that will be designed and developed by the SI are given below:

1. License check from application – This module will be a part of the web application where officers can enter details of an establishment and its license certificate details and check the validity or the authenticity of the license.
2. License check from mobile app – The SI shall develop a field mobile application which will enable officers to have access to real time license check information. This may be integrated with the Field officers' mobile app explained in Section 7.4.7
3. Licensee interface – The SI shall develop a basic web interface where an establishment owner can login, authenticate himself and upload documents and other details. These details will be synced with the module database.
4. External API – The SI shall develop APIs for licensing authorities to send and receive data from the module.

The functionalities of the module are mentioned as below:

FR No.	Module	Functional Requirement
FR 1	License Check Application	The system should allow the user to enter license information of an establishment/weapon into the application with validity period and also enable provision for development of web services to consume data
FR 2	License Check Application	The system should generate alerts on expiry of licenses.
FR 3	License Check Application	The system should allow the user to fetch details of renewal of license from the licensing authority through the API (developed in FR 1.)
FR 4	License Check Application	The system should allow the user to generate a note intimation which can be sent to the owner if the license has expired

FR 5	License Check Mobile App	The system should allow the user to enter license details in a mobile interface also
FR 6	License Check Mobile App	The mobile app interface should be responsive and intuitive in nature
FR 7	License Check Mobile App	All data capture design principles mentioned in Annexure 1 should apply to the interface
FR 8	External API	As mentioned above, the system should allow the sharing of details between police and the licensing authorities through API/web services

Integrity of data captured in the above core modules is one of the core design principles of the web application and hence the system shall have provision to enable finalization(Freezing) of important report/case event such as FIR, Arrest Card, Charge Sheet and Court disposal through OTP based verification from respective Investigation Officers. The admin should have provision to enable/disable the OTP based authentication for freezing the reports/case event.

7.3 Core Admin Module

The SI shall design and develop an admin module so that the department may have multiple levels of supervision on user actions. The admin module will also help the department make data corrections, use intuitive features like forms, reports and dashboards. The admin module will also manage the communication between users and workflow in case investigation. The admin user shall be a powerful role and will consist of multiple levels of authority. The admin role shall be undertaken at district and state level. At the State level, the changes shall be done by Level 3 who is the admin user followed by Level 2 who will be the Superadmin. Level 1 will be supervisory senior officers who shall approve the actions of Admin & Superadmin and grant and oversee admin rights and actions. The district admin who will be the Superintendent of Police of respective districts will primarily be able to approve/reject data updation requests from Police Stations and forward requests (such as report customization) to State admin for necessary action. The detailed categories of requests to be forwarded to district and state admin along with the workflow of the requests shall be provided to SI during SRS -Requirement Gathering phase.

7.3.1 Form Builder

Outline:

To further strengthen the hybrid nature of the data capture in the application, a Form Builder has been envisaged. The admin user should be able to add, modify or delete data fields from a form using the Form Builder. The admin user may also be able to add a new form. It is a powerful feature of any web-based application which enables admin users to add and modify data forms from the front-end editor. By this, the department need not rely on SI software support team for such changes.

The objective of the Form Builder will be to make data capture more flexible in case requirements or processes need to be changed.

SI Scope of Work:

FR No.	Module	Functional Requirement
FR 1	Form Builder	The system should allow the admin to add, modify or delete data fields in a form subject to necessary approvals from Superadmin
FR 2	Form Builder	The system should allow the admin to add a new form as and when required on proper requisition and approvals by superadmin.
FR 3	Form Builder	The system should allow the user to send requisition to the SI to delete a form with approval from Superadmin
FR 4	Form Builder	The system should not allow admin user to add a form in production environment directly
FR 5	Form Builder	The form builder should allow the admin user to view data field dictionary containing all the existing fields to add in a form
FR 6	Form Builder	The form builder should contain a design dictionary containing all canvas design and toolbox items needed to modify or add new data fields and forms
FR 7	Form Builder	The form builder should have ‘Save as Draft’ and ‘Resume on Return’ functionality
FR 8	Form Builder	The system should allow the admin user to view: 1. the case event where to embed a form, or,

		2. which form to modify
FR 9	Form Builder	The display of the form builder should be responsive by design so that it can be accessed both from desktop as well as mobile application
FR 10	Form Builder	The form builder should have a Preview functionality before testing and go-live.
FR 11	Form Builder	Intuitive user-friendly features (like drag and drop) should be part of the system design.

7.3.2 Report Builder

Outline:

The current software does not have a report builder function built into the platform. The standard reporting requirements of the department is fulfilled through another portal known as the officers' portal. The officers' portal is a supervisory tool meant for generating standard reports which are shared with NCRB and other authorities periodically and other reports meant for internal consumption, record keeping and analysis. Details about the same has been described in Section 7.4.5.

One drawback of the portal is that the parameters for all reports are pre-fixed and once generated, the same cannot be edited. This makes making any changes to the existing report structure or generating on-demand dynamic reports difficult.

SI Scope of Work:

The SI shall develop the Report Builder module primarily for preparing new reports and customizing the existing reports used mainly for supervision, analyzing crime trends and crime detection.

Dynamic Reports:

FR No.	Module	Functional Requirement
FR 1	Report Builder	The builder should include a filter panel consisting of all data fields that may be used for generating reports.
FR 2	Report Builder	The builder should be designed for ease of use. It should allow the user to drag and drop data fields into the reporting canvas and generate reports as

		desired.
FR 3	Report Builder	The system should display error pop-up messages in case a user arrangement of data fields into rows and columns is inappropriate.
FR 4	Report Builder	The system should display error pop-up messages in case a report does not display any data. The report builder should allow the admin user to fix certain validations while building a report.
FR 5	Report Builder	The admin should be able to design reports based on selective parameters (including calculated fields) such as conviction ratio among Police Stations, Charge sheet filed within particular time and publish in dashboard whenever required
FR 6	Form Builder	The admin should be able to make changes to a report format, include or exclude data fields from the filter panel with approval from super admin
FR 7	General	The report builder should help extract flexible reports from the sub-module when higher officers seek instant information
FR 8	General	Other functionalities like export through multiple formats, download, share as link or through the Communication Module should also be a part of the Report Builder.
FR 9	General	The output of the reports should be responsive in nature and should be generated in standard formats such as pdf, xls, doc, tabular etc.
FR 10	General	The Report Builder should be easily accessible by the Admin user in case the department wants to make amendments related but not limited to: 1) Structure of a report 2) Change in calculated logic of data fields 3) Inclusion or exclusion of data fields

The SI should study and ensure that all necessary fields should be available in Report builder for admin user to customize the reports.

Apart from the dynamic reports, the Report Builder should also allow users to extract Standard Reports and Crime in India reports which are periodic statistical reports needed to be extracted and shared with authorities.

A brief overview of standard reports being generated currently are described below for bidder reference:

Static Reports:

The key static reports that the Report Builder should allow the user to extract periodically are:

a) Comparative Statement of Murder and Property Crimes up to the month, current year & previous year up to the month.
b) Monthly Crime Reports - City/ District wise on IPC & SSL Cases during month & year and IPC & SLL Crimes variation up to month current year & up to month previous year
c) POCSO Act cases reported up to and for the month current year
d) Crime against Women – up to the month reported cases particulars, police disposal & court disposal details till date.
e) Data on Missing/ Traced/ Untraced persons particulars for the month for current year.
f) Missing Person analytical report for the month for current year

Crime in India (CII) Reports:

The Crime in India (CII) report is a list of 62 reports with multiple sub reports under each main report that has a standard structure but is very exhaustive in nature. These reports are subject to changes as per the requirements by NCRB. The admin user should be able to create these reports and generate them online.

7.3.3 Nominal Roll

Outline:

The Nominal roll module is to enter details of police personnel across the state. The SI will develop the Nominal Roll application as part of the core admin module. The nominal roll information will flow from the admin module to the investigation module.

The nominal roll module is used to assign roles for police personnel and will be used by department for planning and executing field activities such as Bandobust and e-Beat through respective applications. The information that will flow from the admin to the investigation module shall be the manpower data required for deployment, e.g., Home jurisdiction, Transfer or not, Currently deployed or not, Other basic details about the officer, etc.

SI Scope of Work:

The system should ensure that the transfer of police personnel is captured both in new department/station and the exiting station/department and provide alert notification to respective department/station for completion of pending action within stipulated timelines. For ex. A transferred officer's details is entered in the newly posted Police station and not removed from the old police station from where he was transferred, the system should prompt the old Police station to update his transfer status.

The admin privileges/user access rights for modifying personnel details shall be done by respective station SHOs, approved by district supervisory officer and the same shall be viewed by state admin.

7.3.4 Query Builder

Outline:

The admin module will have a built-in query console for the user to be able to write queries using query commands and fetch desired output from the database. The query console may be used by the administrator only on request from the field officers which have been approved by Super Admin and Final Approving Officer at SCRB. .

SI Scope of Work:

FR No.	Module	Functional Requirement
FR 1	Query Builder	The query builder should have an easy-to-use interface.
FR 2	Query Builder	The system should allow the user to parse queries using both command line and front-end user interface.
FR 3	Query Builder	The system should allow the user to search and filter database objects

FR 4	Query Builder	The system should allow the user to select database objects and columns
FR 5	Query Builder	The system should allow the user to create relationships between objects
FR 6	Query Builder	The system should allow the user to view formatted query results
FR 7	Query Builder	The system should allow the user to save queries without extensive use of query languages
FR 8	Query Builder	The query builder should have all important filters available for selection to be parsed into the query as condition
FR 9	Query Builder	The system should allow the user to design complex queries independently using various conditions and join criteria and fetch information from the database.
FR 10	Query Builder	The system should be able to generate results of queries in pdf, csv, tabular, chart form in pdf, xls etc.

7.3.5 Dashboard Builder

SI Scope of Work

The web application should have rich dashboard generating capabilities that will help the department visualize reports and trends in a fast and effective manner. The SI will design and develop the dashboard builder as part of the admin module. The dashboard builder may be used by both admin and station users.

Dashboards are canvas of charts and graphs which can be viewed on a front-end page, also known as visualizations. A typical dashboard consists of many visual components which depict patterns and trends in an engaging manner to the user. The dashboard builder should have the following functionalities:

FR No.	Module	Functional Requirement
FR 1	Dashboard Builder	The system should allow the user to view different crime trends and patterns through intuitive dashboards.
FR 2	Dashboard Builder	The system should allow admin user to create master dashboards and make them accessible to other users using a service interface, where other users can view them and customize using various filters.

FR 3	Dashboard Builder	The dashboard builder should let the user add pages and sections to a dashboard and also use objects to design the layout of the dashboard. The dashboard builder should have provision to display ranking of police stations based on performance parameters such as conviction ratio, charge sheet filed within given time period etc.
FR 4	Dashboard Builder	The system should have drag and drop functionality of objects in the page layout area of the dashboard builder.
FR 5	Dashboard Builder	The system should have a built-in BI (business intelligence) engine to connect to web application master databases and generate visualizations.
FR 6	Dashboard Builder	The system should have integration functionality with external databases and other software like IBM Cognos, Crime Analytics tool, etc.

The Admin users can share the reports/queries/dashboards/forms created using the abovementioned builder tools with all or any particular officer/ unit as per the decision of the Final Approving Officer.

7.3.6 System Diagnostic Tool

The SI should develop a system diagnostic tool as a part of the core admin module. The objective of this tool will be to ensure:

a) Information sharing is secure
b) Integrity of the data is maintained
c) Anomalies in data are captured and alerted
d) Unauthorized access is captured and alerted
e) Performance issues are captured and alerted
f) Peak concurrent usage is captured and alerted

The diagnostic tool should have built in SOPs (standard operating procedures) that will proactively display system messages to the user or send emails and alerts. The system diagnostic tool shall try to correct or trigger alerts for any logical errors.

Logical errors are related to erroneous data during capture, final entry, upload, download, or due to data dependencies in workflow, data manipulation due to vulnerability, etc. Logical errors are

errors committed which are against the design principles of the application. The system should be able to handle such user errors.

FR No.	Sub Module	Functional Requirement
FR 1	Logical Error Correction	The system should automatically detect erroneous data entry based on built-in design. E.g., 1. If a photograph uploaded does not meet minimum pixel and image size requirements, system should trigger alert 2. If a user has selected Passport not available for a person, the system should automatically disable the Passport number field 3. If a user enters date of birth using a built-in calendar, system should automatically display and enter the age of the person
FR 2	Logical Error Correction	The system should send user alerts to flag other errors, E.g., Digital signatures not completed for a document, Trigger alert if freeze timeline crosses maximum limit, Trigger alert if mandated documents or reports not shared with external authorities, etc.
FR 3	Logical Workflow	The system should not allow the user to proceed to the next case event without entering all mandatory fields or entering reason for not doing the same.

7.3.7 Admin Rights & Privileges

Outline:

One core objective of the web Application is the ability of the platform to address data vulnerability and make the information more usable and effective to investigation related activities of the department. To fulfil the same, the data needs to be correct and complete and free from errors.

It has been observed there is a need for an administrator at the department who will be the first level SPOC for resolution of all data related requests, errors and validations. As a process, all requests shall land at the Helpdesk where they shall be segregated.

For all requests related to web application, the requests shall be routed either to district admin or state level admin where the Level 3 admin user receives request, followed by Level 2

Superadmin who approves/rejects the request and final Level 1 Supervisory senior officer who oversees the admin rights and privileges. The users either calls the helpdesk team or raises ticket using the online incident management tool for data updation request post freezing, generate customized report, update nominal roll details etc. Based on the nature of request, the request shall be routed to either district admin or state admin. While the data updation requests shall be handled by district admins, the report generation requests, extraction of queried results etc. shall be handled by state admin. The district admin shall have provision to forward requests to state admin, wherever essential. The district admin shall have provision to activate/deactivate data entry for FIR/ any case event. The district admin shall view and monitor nominal roll of Police personnel in respective jurisdiction. Given below is a list of admin user rights and privileges.

SI Scope of Work:

FR No.	Module Features	Functional Requirement
FR 1	Data Requisition	The district admin user should be able to review and correct any manual errors in data entry based on requisition from concerned Police Station
FR 2	Data Requisition	The district admin user should be able to review and approve a reason code that may have been entered by a user for skipping a mandatory field
FR 3	Moderation	The state admin user should be able to act as a moderator for the Communication Module for any coordination or issues with emails, emails and chats
FR 4	Admin Rights	The state admin user should be able to forward approval requests of his actions to super admin and / or a senior officer
FR 5	Admin Rights	The state admin should be able to assign user access privileges to reports generated. i.e. customize recipients of every report and schedule the frequency for auto generation of report, if required.
FR 6	Admin Rights	The state admin should be able to update any bifurcation of districts/ movement of Police Station from one district to another (with effective date) with necessary approval from super admin citing the GO/formal email as reference. In this case, the data should reflect after the effective date.
FR 7	Admin Rights	The state level admin should be able to assign/update roles to all the users and modify whenever required post approval from Superadmin. The roles of

		different categories of users in the web application and details of access to various features in the web application to each category of users shall be provided to the SI.
FR 8	Access Rights	The state level admin should be able to forward any access right requests including Mobile application access request to super admin
FR 9	Access Rights	The state level admin should be able to create user logins as and when necessary with super admin approval
FR 10	New or Modify Data	The state admin user should be able to add/modify /delete data field(s) on approval of the super admin and its validation
FR 11	Usage Analytics	The state level admin should be able to extract usage analytics reports from the admin module pertaining to user sessions, logins, etc. for supervisory review. Based on the log trails history, the system should be able to capture the corresponding user making any change, capture content before change and after change along with time log.
FR 12	Supervisory Quality	The state level admin should be able to extract usage reports pertaining to supervisory action on remarks / comments / alerts / flags.
FR 13	Supervisory Quality	The system should be able to record date and timewise log of all activities including the old data/content before change for any modifications done.
FR 14	Completeness of Database	The state admin should be able to trigger alerts to users for skipping data fields important for detection
FR 15	Data Import	The state admin should be able to import data in csv format when other department is unable to share data through API/web services
FR 16	Master Data updation	The state admin user should be able to update the master list of data such as addition of new Police Station, addition of new district, Jurisdiction change of an existing Police Station, etc. with necessary approval from super admin

Note: The term 'admin' in this document simply refers to state level admin and reference to admin at district level is mentioned specifically as district admin.

7.3.8 Master Data Management

Outline:

The core admin module should have a built-in MDM utility which will be responsible for managing the master data of the web platform. The system will contain multiple other applications and systems which are hosted on other devices.

SI Scope of Work:

The SI shall develop a master data management utility and integrate it with the web application. The MDM should have a secured integrated architecture which should be able to resolve data replication, data integrity, data security and data inconsistency issues.

The utility should classify and maintain the following data layers:

FR No.	Module Feature	Functional Requirement
FR 1	Master Data	Master data which is the core data layer of the CCTNS 2.0 based on which other data relationships emerge, e.g., FIR data, Jurisdiction data, Case type, Section of law, etc.
FR 2	Hierarchical Data	Hierarchical data which are the relationships that exist between different data including master data
FR 3	Unstructured Data	Unstructured data which may be email alerts, chat and audit logs, query and search logs, usage monitoring logs, etc.
FR 4	Transactional Data	Transactional data such as document numbers, challans, requisition number, etc.
FR 5	Metadata	Metadata, which is the data about data, e.g., XML documents and repositories, report and form definitions, dashboard element definitions, log files, connections and configuration files.
FR 6	Reference Data	Reference data which are shared across master transactional data objects, e.g., countries, currencies, time zones, payment terms, etc.

The SI should ensure that the performance speed of application is high on the web portal. The database structure should be planned in such a way that retrieval of data should be quick. The backend search logic and methodology should be coded in effective manner so that the response to search for items like high resolution image search is not delayed.

7.3.9 Data Capture, Correction & Validation

Outline:

Data correction and validation is a very important admin module since it relates to how the data can be allowed to be added, modified or deleted from the database. All correction and validation will be done in accordance to the rules of admin rights and privileges and role wise privileges which has been described in Section 7.3.7. These rules would ensure the data is safe and secure from misuse or manipulation.

The data alteration protocols will be part of the admin design and will be additional level of data protection apart from the platform security features and data center security. Datacenter security is operational at the SDC, and the SI shall peruse the same for application security.

SI Scope of Work:

An inherent drawback of the client server architecture on which the current CIPRUS is based on makes the local database easily accessible to users. This makes data vulnerable without any log or audit trail. The new functionalities for data capture, correction and validation shall fulfil the below mentioned functionalities:

FR No.	Module Feature	Functional Requirement
FR 1	Data Capture	The system should ensure all documents have a timestamp.
FR 2	Data Capture	The system should ensure timestamp information of all data fields from source of capture to final capture to be maintained. E.g., Time of photograph capture, Time of upload, System time for documents generated, etc.
FR 3	Data Capture	The system should ensure that all mandatory fields are filled and if skipped due to data unavailability, such fields must be filled within stipulated timelines. The user has to provide reasons for skipping a field. The system shall have an escalation mechanism for non-entry beyond stipulated timelines.
FR 4	Data Capture	The system should provide multiple modes of data capture to the user based on the situation as explained in Annexure 1.
FR 5	Data Capture	The system should allow the user to capture information in any sequence as

		and when the information becomes available to the Investigating Officer
FR 6	Data Correction	The system should maintain audit trails of all user sessions and actions. The audit trails should also include actions taken by admin user for review by super admin and so on.
FR 7	Data Correction	The system should allow only the requested field to be changed based on requisition form. The system should have provision for admin to make changes or allow user to make required changes only on the requested field.
FR 8	Data Validation	The system should have provision to track and notify users on their accountability to complete legally binding events, e.g., FIR submission to court, Arrest intimation, Accused produced before magistrate, etc.
FR 9	Data Validation	The system should design the admin workflow through 3 levels depending on the criticality of data correction or validation – Admin, Superadmin & Supervisory senior officer who oversees rights privileges to admin and Superadmin
FR 10	General	The system design should include a data correction and validation workflow engine starting from user requisition through helpdesk then admin or Superadmin as the case may be

7.3.10 User role & Privileges

The various roles of Police Personnel in a station along with the modules/events for which access shall have to be provided is illustrated below for reference. However, during the application development phase, the final list on role-wise access to data, features in the application for respective officers shall be provided.

Sl.NO	Role of the Police Personnel	Modules accessible in Web Application
1	SI of Police	Provision to give access to registration of FIR and Investigation modules like Examination of Witnesses, Arrest of Accused including laying Final Report of the case, CSR, Registration of Ordinary Petty Case & Motor Vehicle Petty Case and its disposal.

2	Station Writer	1. Generate station permanent records (Part I to V) and other registers and its abstracts. 2. Made entries in registers like Duty Roster, Leave Register, Arms Issued Register, Quarters Register
3	Station House Officer	1. Taking care of all administration activities like enrollment of police personal allotted to their police station, 2. Assigning rolls to them 3. Registration of FIR and Investigation modules like Examination of Witnesses, Arrest of Accused including laying Final Report of the case, CSR, Registration of Ordinary Petty Case & Motor Vehicle Petty Case and its disposal. 4. Entries to be made in Gun License, Explosive Shop Registers and Inspection/Visit details made on the place where it is kept. 5. Creation and maintenance of History Sheets 6. Made entries in registers like Duty Roster, Leave Register, Arms Issued Register, Quarters Register

Logins for the CCTNS 2.0 application shall be created for all Police stations and their respective SHOs, Supervisory and senior officers in Higher offices, Special units and Training centers. The majority of user logins shall belong to the Police stations as they are the basic operational unit of the department. The total user count for the application shall be an estimated 4000 to 5000 approximate users. This estimate is based on the current count of user logins and estimation of use. This may increase depending on future integrations with other applications, and general operational expansion of the department.

The concurrent usage of the application shall be an estimated 3000 users. This is based on concurrent usage of 2 data entry operators in each police station.

Current user count, roles & privileges details are mentioned in Annexure 6 for SI reference

7.3.11 Platform Usage Analytics

Outline:

The current CIPRUS platform suffers from a range of challenges with regard to usage analytics. Currently only basic information of usage of the platform is maintained. Since the architecture is based on a client server model, advanced usage metrics is difficult to capture and maintain. Thus, the envisaged web application will keep an advanced array of usage information thus making it easy for the department to evaluate the effectiveness of the application to the police force.

Some of the basic metrics that are tracked now are:

1. Supervisory officers' login details into the platform limited to login time, session duration, logout time.
2. Number of application downloads, application installed and uninstalled.
3. Number of times staff logged into the platform
4. Total login accounts
5. Active and inactive accounts

The above-mentioned basic metrics do not take into account in-depth analysis of usage and hence difficult to ascertain the helpfulness of the platform to the department. The usage analytics for the new web platform shall be more thorough and delve into features/tools level usage analytics by different categories of users.

SI Scope of Work:

The SI will design and develop the usage analytics module as part of the Core User Management / Admin module.

The system should keep a record of all supervisory actions taken on tasks:

a) Data requisitions attended
b) Review and approval actions taken
c) Request for additional comments or clarification
d) Create new user requisition

e) Actions taken on form and report builder

Review, remarks or action taken on Crime Analytics modules

One of the design principles of the usage analytics module shall also be to monitor the outcome of use of the platform. The SI shall include outcome-based metrics such as quality of supervision will be critical to the adoption of the platform by everybody in the department.

Platform Usage effectiveness –

Th focus should be more on developing effective and meaningful usage metrics of the system. Few identified use cases for system usage is mentioned below:

The system should capture pendency within stipulated timelines and communicate the same to senior officers. The system should capture the usage of features such as Facial Recognition software, stolen vehicles versus abandoned vehicles/property used in crime match, & Missing person versus UIDB match detected against attempts made by users and thereby estimate the success rate of usage. This shall be captured for individual user, Police station, district up to state so that the analysis of feature usage shall be measured. In case of match found, the officer initiating the search should only be assigned the credit for success match.

The system should capture the most used feature based on user log of activities and every log including communication module shall be used for analysis of usage. For e.g. Police Station wise usage of chat box feature in the communication module. This data shall be used to create dashboards.

7.3.12 Communication Module

Outline:

The web Application will have an integrated communication module across all the modules. The communication module will consist of features and functionalities that will allow department officers to share information, communicate with each other through chats, trigger auto emails and alerts for important actionable items, etc.

SI Scope of Work:

This module will consist of various channels through which the department will send, receive and share information. The SI shall design detailed use cases which shall consist of communication channels, communicating officers or parties and context of communication. This admin module will apply to all other application modules, and the channels shall be invoked depending on the use case.

FR No.	Module Feature	Functional Requirement
FR 1	Email Service	The system should have 2 modes of email triggers: Manual mode and Auto-trigger mode
FR 2	Email Service	The system should invoke the auto-trigger mode when a user action needs to be alerted to other users, e.g., generating a document or altering some information that require supervisory notice
FR 3	Email Service	The system should invoke the manual mode when a user needs to send information to an intended set of recipient(s)
FR 4	Email Service	The system should also be able to trigger emails when a workflow or a SOP involves a step where an email has to be sent before proceeding to the next step
FR 5	Email Service	The system should also allow sharing of information to all external email domains
FR 6	Email Service	The system should have an email local client view for user specific logins where users can check messages regarding user actions on the application
FR 7	Broadcast Service	The system should be able to integrate with other IM (Instant Messenger) service providers like Whatsapp to broadcast important citizen information
FR 8	Broadcast Service	The system should be able to send automated messages to individuals to render digital citizen services like sharing of documents, verification services, digital receipts, etc.
FR 9	Station Messages	The system should be able to send messages to police stations for matters related to a station, e.g., Important notification, Birthday messages, etc.
FR 10	System Alerts	The system should be able to trigger real time system alerts for scenarios such as: any user modification which his next supervisory officer must be alerted, alerts from field apps like officers' apps, Bandobust module, etc.
FR 11	System Alerts	The system should notify through pop ups and provide alerts to officers

		regarding messages received from other officers
FR 12	Notes and Remarks	The system should allow user to enter notes and remarks to insert comments on a user action, requisitions pending for his inputs, notes or clarifications regarding an approval, notes to other officers, etc.
FR 13	Chat Service	The system should allow users to invoke a real time chat interface where users can chat regarding some issue, a situation that needs immediate conversation, etc.
FR 14	Admin Rights	The admin should be able to enable and disable rights to send broadcasts and also chats with whomever approved.
FR 15	Calendar	The system should have a unified calendar feature where the concerned officers are alerted through pop-ups/SMS/email alert about the upcoming activity such as timeline for completion of investigation, prison release convict alerts, custody request alert, Bandobust, trial in a court etc. based on the dates of various activities/ events captured in the relevant modules

7.4 Tools & Portals on CCTNS Platform

7.4.1 Missing Person UIDB Tool

Outline:

This module relates to comparing and matching UIDB (Unidentified Dead bodies) with Missing Persons reported. The department already has a tool for this purpose. Missing persons reported are matched with UIDB reported by manual comparison of the photos and filters based on physical attributes.

The outcome of the comparison tool is dependent on the capability of the user and is manual. Using the tool, the department may also extract pendency reports, matched reports, view details and analyze reasons for the missing person turning out as dead, key attributes that helped in the matching, etc. However, there are certain functionalities that the current tool does not feature which are described below. Hence, the SI scope of work will include design and development of a new Missing Person UIDB tool that address the current gaps.

The process of matching is explained in the below section.

Missing Person UIDB matching Complete process:

The process of comparison of missing persons and unidentified dead bodies should involve the following two components:

1. Creation of a common database of details of missing persons and unidentified dead bodies including photographs
2. Comparison by the concerned investigation officers for detection of their respective cases of missing persons and unidentified dead bodies

Common database:

The common database creation should involve the following tasks:

Missing Person:

a) Photograph procurement for missing person: The police station procures the photograph from the family of the missing person.
b) Collecting details of the missing person: The police station collects details of the missing person like physical details (age, height, complexion, identification mark etc.) and other details like clothes worn at the time of missing, languages spoken, any other behavioral feature etc.
c) Photograph uploading for missing person: The police station uploads the photographs through the web application while registering the case of missing persons.
d) Uploading the details: The police station uploads the details of the missing person through the web application platform. In few cases the photograph availability might be delayed. The other details are generally available immediately at the time of reporting of the case.

Unidentified Dead Body:

a) Photograph of Unidentified Dead Bodies: The police officer visiting the SOC should take photographs from different angles ensuring clear close up photo of the dead body.

b) Collecting physical & other details from dead body & SOC: The basic details like probable age, height, identification marks, clothes worn, and other items on the body will be noted at the SOC and uploaded on the application through web portal or mobile app.

c) Uploading the photograph/other details: The police station uploads the other details of the missing person through the web application.

Comparison:

The common database creation should have the following information:

1. Date: The date of missing of person is generally known with reasonable precision. However, there might be a delay in reporting. The probable time of death in case of unidentified dead bodies is only estimated by postmortem. Hence some margin for error should be provided in filtering the cases for comparison.
2. Geographical: The normal tendency is to compare cases in nearby or adjoining districts. However, in cases of murders the bodies are dumped in neighboring states. Hence it is important to include the missing persons and unidentified dead bodies from at least the neighboring states.
3. Gender: Chances of error on gender are practically nil. Hence the basic filter for gender has to be applied as default
4. Photograph: Most important comparison is the comparison of the photograph of the missing person and dead body. However, this is not possible in many cases because the face is mutilated, or the body is totally decomposed, or the photograph has not been taken properly.
5. Physical parameters: Comparison of other physical parameters is helpful. However adequate margin for error should be given in the filtering mechanism because the measurements are not always accurate. (Height errors can be even up to 6” as many times approximate height is entered)
6. Clothing & other details: Comparison of clothing & other details is also helpful. However adequate margin for error should be given in the filtering mechanism because the

measurements are not always accurate. The color of clothing has subjective descriptions which has to be taken into design consideration.

7. Injuries on the body: These are useful to assess whether any foul play is involved. Some cases of unidentified dead bodies are clear cases of murder. However, in some cases the injuries might be due to hit & run accidents.
8. Cause of death: The current common database does not provide for the column for apparent cause of death. This is an assessment of the investigating officer of the case whether any foul play is involved.
9. Circumstances of missing: These are not incorporated in the current website or the citizen portal. Many cases of missing persons are related to elopement. However, there are cases where the circumstances of missing clearly point out to foul play. Identification of these cases as such will help in focused comparison.

SI Scope of Work:

The scope of work for the SI will be to:

1. Conduct an As-is study of the current tool
2. Gather requirements from the department
3. Find out identified gaps or improvement areas in the current tool
4. Understand additional functionalities to be built
5. Design & develop a new and more effective tool

The indicative list of functionalities that the module should fulfil:

FR No.	Module/Tool	Functional Requirement
FR 1	Missing Person UIDB tool	All comparison logs and audit trails of user actions making the comparison must be recorded.
FR 2	Missing Person UIDB tool	The system should allow the officer in charge of conducting the comparison to record a detailed step by step procedure of comparison completed, e.g., search keywords used, basic and advanced filters used

		both for circumstantial as well as physical related, matches rejected, matches approved, etc.
FR 3	Missing Person UIDB tool	The system should be designed in such a way that the officer must enter remark at every stage of comparison.
FR 4	Missing Person UIDB tool	The process of comparison must be step by step sequential in nature so that actions can be logged in a sequence, e.g., date of photo picked up for comparison, date range of photos picked up for search, percentage of filters entered (e.g., 2 out of 10 filters marked Yes for search – 20%, 5 out of 10 filters marked Yes for search – 50%, etc.)
FR 5	Missing Person UIDB tool	The system should let the officer enter remark why for a certain match complete or partial keyword was entered
FR 6	Missing Person UIDB tool	The system should let the officer enter remark why a match was rejected or accepted
FR 7	Missing Person UIDB tool	The system should let the officer enter reason why a comparison activity was not completed
FR 8	Missing Person UIDB tool	The system should be designed for multi-user entry and multi-user approval workflow so that action taken by officer comparing can be approved or confirmed or asked for further clarification by an officer senior to him/her.
FR 9	Missing Person UIDB tool	Audit trails with regard to action taken by user details (identity details of officer), login logout details, session time and logs, approval logs, case pendency reports, metrics of comparisons done to date, etc.

7.4.2 History Sheets

Outline:

History sheets information is captured by the department to keep track of accused information

from case files. The department currently has an existing history sheets module in the existing CIPRUS; however, it has been envisaged to develop a new tool where based on crime history data of accused from core modules, the system categorizes the accused into Habitual Offender, Known Depredator, Dossier Criminal, Rowdy and Suspect and notifies SHO, DSP and SP concerned. For instance, an accused convicted in 3 IPC cases in chapter XII, XVI & XVII falls under Habitual Offender Category. The detailed criteria for above categorization and the required workflow logic for SHO, DSP & SP. shall be provided to the SI.

Description:

Some of the illustrative functionalities of the history sheets portal are outlined below:

FR No.	Module Feature	Functional Requirement
FR 1	Transfer of History Sheet	The system should allow the user to forward a history sheet to another station through divisional officer.
FR 2	Transfer of History Sheet	The system should allow forwarding history sheet to the district SP in which the individual concerned has taken residence.
FR 3	Detention of History Sheets	The system should allow detention of a history sheet after two years of resignations.
FR 4	Detention of History Sheets	Orders of an offices of and above the rank of DSP must be taken for the extension in the first instance up to the end of the next December and further annual extensions from Jan to Dec.
FR 5	Suspect History Sheets	The system should allow maintaining history sheet of suspects from the date of registration up to the end of December.
FR 6	Suspect History Sheets	Discontinuous or retention for a further period from Jan to Dec where necessary shall be obtained.
FR 7	Close History Sheets	The system should allow closure of History Sheets of person who has died and shall be destroyed under orders of an officers of and above the rank of DSP.

FR 8	Close History Sheets	The system should allow closure of History Sheets of persons who have become too old to commit crime under orders of an officers of and above the rank of DSP.
FR 9	Close History Sheets	The system should allow closure of History Sheets of persons who are unable to commit crime due to physical infirmities under orders of an officer of and above the rank of DSP.
FR 10	Close History Sheets	The system should allow closure of History Sheets of persons who are completely reformed as is established by continuous good record over a period of 15 years under orders of an officer of and above the rank of DSP.
FR 11	General	Some of the History Sheets information that are to be designed through a form capture module are given below: 1. Sheet No. 1: Personal Details 2. Sheet No. 2: Physical Details 3. Sheet No. 3: Relatives & Associates 4. Sheet No. 4: Receivers of stolen properties & disposal 5. Sheet No. 5: Cases Involved 6. Sheet No. 6: Cases in which suspected 7. Sheet No. 7: Convicted Cases Details 8. Sheet No. 8: Current Doing 9. Sheet No. 9: Photograph & Fingerprint

7.4.3 Station Crime History

Outline:

Station crime history stores information about past case records in a jurisdiction. It consists of 5 parts as described below:

1) Part 1- True occurrence register (aggregation of crimes)
2) Part 2- Crime charts (hotspots and maps)
3) Part 3- General conviction register (all convicts)
4) Part 4- Village history sheets

5) Part 5- Bad character check register

These are useful information by which the police stations are able to conduct various functions like bad character (BC) checks, match and verify field intelligence inputs with village history sheets, view convict registers and analyze crime charts. These activities help police stations keep a track of suspicious activities or identify hotspots in a given jurisdiction which help prevent crimes or early detection.

SI Scope of Work:

The SI shall design & develop the mentioned 5 sub-modules under station crime history that should fulfil the below indicative requirements:

FR No.	Sub Module	Functional Requirement
FR 1	True Occurrence Register	This sub module captures all property offences and the data such as FIR, accused details, court disposal etc. shall be auto populated from core modules
FR 2	Crime Charts & Hotspots	The system should have a 'crime mapping feature' where all geo tagged locations such as scene of crime, accident prone zones etc. are plotted
FR 3	Crime Charts & Hotspots	The tool must enable stations and offices to plot local crimes, cases, activities
FR 4	Crime Charts & Hotspots	The tool must contain basic data filters and visualizations
FR 5	Crime Charts & Hotspots	The station crime mapping tool will aggregate and integrate with the Crime Analytics tool which is being externally developed by the department
FR 6	General Conviction Register	This sub module should auto populate convict details from the prosecution module
FR 7	Village History Sheets	This sub module will contain the details of places in a jurisdiction
FR 8	Village History Sheets	This sub module will be a revamp of the current village card section and capture more details that will help in crime detection and analytics

FR 9	Village History Sheets	Some of the illustrative attributes that needs to be captured are: 1. Area classification – Block or Mother Village, Locality or Hamlet, etc. 2. Population – Population of the village 3. Type of village – Normal, Communal, Crime Prone, Naxal, Caste, Factional, etc. 4. Type of places in village – Religious, Commercial, Residential, Public Spot, etc. 5. Presence of sub-place in village – If religious – Mosque, Temple, Church, etc. 6. Socio-economic classification of village – Rural, Semi-Rural, Urban, etc.
FR 10	Bad Character Check	This sub-module will be developed to monitor suspicious activities in the local jurisdiction
FR 11	Bad Character Check	This sub-module will be used to view, or update or add into accused history sheets
FR 12	General	The module should be able to access accused history sheets and bring efficiency to beat management and patrolling of suspicious persons, places or activities
FR 13	General - Integration	The module will be integrated with: 1. the crime prevention records 2. the history sheet module 3. the e-Beat module 4. the Bandobust manager module

7.4.4 Bandobust Manager

Outline:

The Bandobust module is another important module in the web Application platform. Bandobust is a police activity specifically planned for a purpose or an event, or a routine activity at a particular place.

Bandobust activities ensure people and places are safe and under strict supervision. Since most of the Bandobust activities have to be pre-planned which involves deployment of required police personnel, it is important to have a Bandobust management system that will help the department plan, execute and oversee the activities from end to end.

SI Scope of Work:

The SI has to develop a 'Bandobust Manager' application that will be built-in to the web Application platform. Since Bandobust is a field activity and would require extensive real-time on-the-go men management, the application would also be built-in to the officers' field devices.

The Bandobust Manager application should include the following functionalities:

FR No.	Module Features	Functional Requirement
FR 1	Bandobust Manager	The application has to be developed for both web application and mobile app versions since the app will be used by the field officers.
FR 2	General - Integration	The mobile version of the application has to be part of Field officers' mobile application as mentioned in section 7.4.7
FR 3	Bandobust Manager	The application should have a layered approval workflow where officers should be able to assign, delegate, view or edit manpower deployment for a Bandobust activity.
FR 4	Bandobust Maps	The application should have a built-in Maps module with real-time location pinning functionality.
FR 5	Bandobust Maps	The Maps feature should enable officers to: 1. pin Bandobust area checkpoints 2. assign personnel from the deployment team on the checkpoints 3. assign and delegate tasks 4. view and edit personnel and checkpoints 5. approve or reject changes in deployment and checkpoints through the approval workflow
FR 6	General - Integration	The application should integrate with the nominal roll application so that officers can access manpower data from the districts to create deployment teams for a Bandobust activity

FR 7	Bandobust Manager	The application should have a 'people pool' feature where officers can view and verify reporting status of the manpower on the field for the activity
FR 8	Bandobust Manager	The application should have necessary role wise access control definitions that should allow: 1. Senior officers to delegate tasks and subtasks to officers in charge of the activity 2. The teams deployed should be able to view and enter self-information like: a) Reported for the activity or in transit b) Reported at the checkpoint assigned c) No. of vehicles checks performed d) Search for suspicious persons or vehicles e) No. of stolen vehicles detected f) No. of suspects verified & found to have criminal antecedents – entry of the basic details
FR 9	General - Integration	The application should integrate with the investigation module to search and immediately report cases of matching suspicion with past crime records.
FR 10	Bandobust Reporting	The application should have a remarks interface functionality where deployment team may enter feedback or comment about any important share worthy information or officers may interact with each other
FR 11	Bandobust Reporting	The application should have report extraction feature where various reports may be generated from the mobile app or application after the Bandobust activity is completed to review the activity
FR 12	General - Integration	The application should be integrated with the communication module with built in features like alerts, emails, notification triggers, IM (instant messenger) chats for seamless communication between officers before, during and after the activity.

7.4.5 Citizen & Officer Portals

The SI shall develop a unified portal for citizens and officers with open access to citizens and with login-based access for approved officers. The existing facilities from both citizen services portal and officers' portal along with additional features through requirement gathering are to be included in the new portal. A brief description of existing portal features and indicative additional requirements are mentioned below:

7.4.5.1 Citizen Services Portal

The current list of services that can be availed using the citizen services portal are given below:

Citizen Services (Free)

1) Register Online Complaint
2) Online Complaint Status
3) View FIR
4) Arrested Person Details
5) FIR Status
6) CSR Status
7) Vehicle Verification
8) Private Security Agencies
9) Found by NGO

Citizen Services (Paid):

1) Police Verification
2) Lost Document Report
3) E-Pay Fingerprint Bureau
4) Road Accident Documents
5) E-Payment for Traffic Challans

In addition to the above existing citizen free and paid services, the system should have the capability to:

1) Enable easy-to-use citizen centric forms that records complaints

2) Give citizens the option to choose categories and give description for online complaints
3) Give citizens the option to report complaints anonymously
4) Authenticate all online complaints through a valid mobile number and OTP
5) Give department officers full and filtered complaint views
6) Forward application / request to external agencies or feedback to higher offices through an approval workflow
7) Trigger assignment and approval workflows for all online complaints through petition officer / administrator
8) Dispose non-cognizable offences and integrate with the CSR workflow
9) Integrate with FIR module in case a complaint is deemed Cognizable
10) Generate unique identifiers like Service Request, Complaint No., etc.
11) Add any citizen facing services that may come up in the future

7.4.5.2 Officers' Portal

Reports:

The Report Builder as part of the Admin module will be to generate custom, dynamic and supervisory reports by the Administrator depending on parameter input and calculated logic.

However, there will be a reporting module that will be a part of the Officers Portal which shall be available for use and extraction by department staff at the police stations and higher offices. These reports are static statistical reports which shall be mostly pre-designed and pre-configured. These would be standard reports for consumption and analysis by the staff.

The SI scope of work for the static reports shall include:

Studying the current Officers' Portal reporting module and gather additional requirements from SCRB .The output of a joint consultation between the SI and SCRB will include:

1) The errors in current reporting module (parameters, structure, etc.) and corrections needed
2) To-be report (Gap analysis) of the improvements needed
3) Any additional standard reports that are currently not a part of the module

The new reports design will be based on the above To-be report and will be a robust reporting module which shall address all the current challenges. The exhaustive list of the mandated reports for department submission to external authorities will be provided by SCRB to the SI.

Reports:

The reports from the current Officers Portal include:

1) Online complaints summary and status report
2) Case progress detail report
3) Review reports by Cognizable crimes, Grave cases, L&O cases, sessions cases.
4) Citizen feedback report
5) Statement reports - IIF count, IIF statistics, UIDB statement, Stolen vehicle, Stolen property, Property crimes
6) Exception report by RTA wrong entry, RTA case updation status, Improper replication.

The SI shall make an exhaustive list of all standard periodical reports and develop the new Officers Portal accordingly.

The design framework shall be in alignment with web Application design principles as listed in previous section.

Search:

The Officers Portal will contain a Search module. This will be a functionality that will allow officers to search the database for specific attributes relating to person or item involved in a case.

Some of the key search criteria include:

1. Name search
2. Accused Name search
3. Accused M.O search
4. Accused to be arrested search
5. Vehicle search
6. Generic keyword search
7. Advanced NBW search

8. Accused photo gallery search
9. IMEI number search

The search module will be intelligently built to accommodate the following (but not limited to) capabilities:

1) Past searches should be saved and shown to user to re-initiate search or view past search conducted.
2) Past searches should be saved and displayed to supervisory users as part of reporting module or generic views for him to decide efficacy of search on a case.
3) Audit logs of previous detection searches should be kept and integrated into dashboard and reporting module for more focused searches or matching.
4) Search functionalities should apply to all relevant core modules – E.g., UIDB Missing Person search tool, Crime Cases search, History Sheet search, Station Crime History search, Fingerprint search, etc.
5) Automatic searches should be integrated in all applicable workflows.
6) All latest search techniques like phonetic search, multiple filters, etc. should be incorporated.

7.4.6 DMU Mapping

Data Migration Utility (DMU) is a utility software that is used for real time sync of certain important information from the state CAS with the central CAS at NCRB. There is a mapping between data tables between state and central databases, and the same gets synced and updated as and when fresh information is populated in the system.

The current version of the DMU software is partially developed due to certain difference in database design, data table and data field mapping, sharing architecture – since both the platforms (state and central DMU) was independently configured not keeping in view future information sharing requirements.

The SI scope of work will include conducting a thorough system study of the currently functioning DMU, study and analyze the sharing and mapping requirements as per the requirement of MHA/NCRB (critical information to be shared shall be provided by the department), identify gaps in data mapping, design and develop a new state level DMU software

that will take into consideration database design of the central DMU so that information sharing in real time is accurate, data mapping is complete, and the system is devoid of redundancies.

7.4.7 Mobile Application Development

The SI should develop a mobile application which should be compatible with Android OS latest version. The SI should develop mobile application for the modules and features which are mentioned below:

The citizen services portal should also be accessible through mobile application which shall be made available through Android Play Store. The functionalities of the citizen services portal shall be as per requirements mentioned in Section 7.4.5.1

The officers' portal should be accessible through mobile application (limited only to selective officers) authenticated through OTP/Login credentials and connected through secured VPN. Secured VPN shall be provided by SCRB. The functionalities of the officers' portal shall be as per requirements mentioned in Section 7.4.5.2

The Bandobust Manager is to be made accessible through mobile application as per requirements in Section 7.4.4

The Scene of Crime details in Investigation module should be accessible through mobile application for the Investigating Officers for uploading documents, audio-video clippings of statements, CCTV footages etc.

The license check feature as part of Regulatory Framework as mentioned in Section 7.2.5 should be made accessible for the field officers through mobile application.

The search features such as Accused Name search, IMEI number search, Vehicle Number Search shall be made available for all the Police Officers in the state. This search is done based on integration with Accused name from crime details, Vehicle Number from RTO database and IMEI number from crime details.

The Station House officers shall be able to view overall summary of cases reported at respective police stations and the pendency status of cases which are yet to be disposed by the Court.

Similarly, the higher officers shall be able to view overall summary of cases reported at police stations/district/range/zone under their jurisdiction and the pendency status of cases which are yet to be disposed by the Court

7.4.8 Unified Calendar

Scope:

The System Integrator should develop a unified calendar tool to capture dates and timelines from various case events/sub modules in the core modules and other SCRB applications and have provision to auto-populate alerts to the concerned officers. This tool shall be integrated with the communication channels as mentioned in Section 7.3.12. The system should have provision for scheduled automatic alerts and manually triggered alerts as well. While some alerts shall be informative to the recipient, other alerts should be seeking response to close the workflow. For instance, pendency in cases beyond 30 days could be sent as informative alert whereas, alerts for cases coming up for trial in court needing the concerned officer's presence could be closed only after the officer responds. The illustrative list of alerts to be provided are mentioned below:

1) Alerts for Bandobust scheduling
2) Alerts for investigation completion for relevant set of cases beyond particular time period.
3) Alerts for bail application and other court petitions relating to the case.
4) Alerts for court hearing date, summons and warrants timeline
5) Alerts for prison release of convicts

The admin should have complete control over the scheduling of the alerts. The three level of admin privileges should be provided for calendar tool where the Level 3 admin should be able to customize the scheduling of alerts by adding new alerts/ modify existing alerts scheduled time etc. with necessary approval from Level 2 Super admin. Level 3 admin shall be able to view the scheduled alerts.

7.5 Integration with SCRB Applications

The ancillary modules integration with the core Web application means developing web services required to seamlessly connect all existing and future applications and databases that are currently being used or envisaged by SCRB.

Some of these portals are administered by various central agencies and others are directly under the purview of SCRB. The SCRB is also the central user department of these portals, hence it is imperative to integrate information interchange to and from the core modules with these systems for real time data access, reference and analysis.

Given below is the ancillary modules integration scope of work.

7.5.1 e-Beat System

Beat is a specific policing activity to serve purposes of crime prevention and detection. Every Police Station limit is divided into beats and the police personnel of the concerned police station are deputed for policing these beat areas.

The SI scope of work will be to integrate the e-Beat system with the web Application platform through API/web service. The integration data fields required for information exchange between the 2 systems may be gathered during the requirements stage. At a high level, the touchpoints illustratively will be:

a) Police verification services
b) Crime and criminal data – Details of cases (Type of crime, SOC – scene of crime, etc.)
c) Summons
d) Details of NBWs
e) Bad character check registers
f) Person search
g) Vehicle search
h) Mobile number search

7.5.2 Crime Analytics Tool

A crime analytics tool is under development by the department. This tool will have 4 modules built-in:

1. Crime Trends
2. Accused Search
3. Timeline Visualization
4. Hotspot Analytics

This tool is an analytics tool for the department which feeds on data from the CIPRUS and churns out crime trends, patterns and insights regarding crime occurrences.

After the completion of development, an API connectivity shall be given to the web application. Necessary functionalities within the core application that may peruse information from the crime analytics tool are: information search of accused and property databases, indexing and retrieval, view crime trends and charts, view timeline visualizations, etc.

7.5.3 Facial Recognition

A facial recognition software (FRS) is currently under development as a separate project of SCRB. The scope of the SI for this project will be to integrate the FRS system when it is completely developed, tested and deployed for use.

The FRS tool is envisaged to capture and consume photographs from CIPRUS modules – accused photos, UIDB photos, person missing, etc. The tool then converts the photo into a data format with related details like FIR number, MO attributes, DB attributes, General attributes if applicable (Place or time of occurrence), etc.

The integration points with web Application will be the following:

a) Whenever a new photograph is uploaded in the web Application (any module), the system should populate the FRS tool with the photograph and make it available. Thereafter the tool will be able to convert the photograph into desired format by the users of the tool.
b) Alerts should be triggered whenever a new upload is done.
c) Uploads may be done in single photograph or in batches of photos.

d) The integration end point will be a mobile application (FRS Mobile App)

7.5.4 Tollscope

The Tollscope is an envisaged application under development by the department. The scope of work of the SI shall be to integrate the Tollscope application with the core web application platform through API/web service.

A brief description of application functionalities is given as follows:

1) The Tollscope is an application that will capture and process all ANPR camera feeds installed at Exit and Entry toll checkpoints to and from a city.
2) The Tollscope application will run a search in real time against all such vehicles that have been previously involved in crime and return remarks and findings about the vehicle.
3) Necessary alerts will be shared with all concerned officers and officials manning the toll checkpoint.
4) In accordance with subsequent SOP (standard operating procedure) action to be taken instructions will be shared with the next patrolling officer or toll checkpoint.

7.5.5 Fingerprint Database

Currently, the architecture of the Fingerprint enrolment and authentication is as given below:

1) Chance prints are captured by the Fingerprint staff at the scene of crime
2) The chance prints are then scanned and uploaded on the Fingerprint identification software.
3) In case of suspects and accused arrested, the fingerprints are taken manually and sent to the SDFPB (Single digit fingerprint bureau) at the district headquarters.
4) These fingerprint slips are scanned and uploaded on the FP software
5) The FP experts view and authenticate the received fingerprints.
6) The FACTS sends the details to the central NAFIS server for further integration with the central server.

A new and upgraded Fingerprint authentication system is currently being developed by the department. The scope of the SI will be to integrate the web application with the newly developed system and the underlying Fingerprint database. The scope of the SI will also include

integration of the state database with the central NAFIS system which has been described in a following section.

The SI shall study the new Fingerprint system and develop APIs to integrate it with the web Application. The web Application should be able to send a fetch query to the new system from a relevant module and the Fingerprint details should be populated into the forms. The SI shall design, modify or let the admin modify an existing form where the data will be populated in the application

The SI shall enable capture of fingerprints of accused at the time of arrest through the application and send the same to Fingerprint server for verification and authentication by the Fingerprint experts.

The admin or user of web Application should also be able to send a requisition to system or any external databases like financial institutions, transport department, UIDAI, etc. in case the fingerprint needs to be mapped with such personal identity databases. The development of all such necessary APIs should be done by the SI.

7.6 Integration with Central Systems

7.6.1 ICJS

The Interoperable Criminal Justice System (ICJS) was implemented by NCRB to achieve interoperability between critical pillars of investigation and judiciary – Forensics, Prisons, Courts, and Prosecution. It was a 4 -fold process:

1. Developing separate applications for each of the above pillars for a process movement from manual to digital
2. Developing a centralized application ICJS to integrate all the systems and applications across the 4 pillars
3. Integrating the systems through APIs to achieve quick data transfer between the pillars
4. Integrating ICJS with all state CAS software - CCTNS

The integration of ICJS with the state CAS is underway by different states. The SI scope of work for this project will include integrating the 4 pillars of the ICJS with the newly developed web application platform.

The integration will enable information exchange between Police and other pillars of ICJS like prisons, forensics, courts and prosecution. The APIs available in NAPIX should be developed to consume and share data to and from other pillars.

7.6.2 NCCRP

NCCRP, or the National Cyber Crime Reporting Portal, was launched by MHA/NCRB. The objective of this portal is to enable citizens to raise cybercrime related complaints and grievances. This gives the State and National Cyber Cells a dedicated single window to tackle all Cyber related crimes in the country, especially since the crime rates under this category has increased in number over time.

As part of scope of work, the SI shall integrate the NCCRP portal with

1. SCRB's Online Complaint System
2. An interface for the Cybercrime officers to view, assign and dispose the complaints received through NCCRP as per the requirements given by the department.

This integration will cater to a range of services, such as:

1. Receive and channelize Cybercrime related complaints from NCCRP to Online complaint module
2. Action taken on the complaints received from NCCRP should be shared with NCCRP portal through APIs.

7.7 Integration with other Systems of Police Department

7.7.1 SPMCR (Master Control Room)

The web application will be integrated with the Master Control Room. The MCR is the incoming helpline call system of the department to which citizens place distress calls. Based on the

information from the call received and tracking coordinates, police squad is sent to the location for help or rescue.

The MCR system should be able to access needful information from the investigation module. This can be for various purposes like:

a) Preparedness of the police teams based on past crime information in the area – by Quick retrieval of analytics and crime charts information from the Search & Analytics module. Such data may help the MCR to prepare for additional risks better
b) Passing on additional information while addressing the distress, e.g., intelligence related to crime type, pattern related to distress call and past crime, suspicious geo clusters in the area, suspicious people / criminal or addresses.

Such information may help the department rescue the victim faster and take control of the area more efficiently.

7.7.2 e-Challan

SI shall enable sharing of information through APIs as per the requirement of the department in future.

7.7.3 RADMS/iRAD

RADMS is a software developed with the Police, Highways and Transport departments as the stakeholders for collecting, comparing and analyzing road accident data. It is a comprehensive traffic management system which helps to study and analyze road accidents in a systematic and scientific way.

The RADMS software is currently being used by the staff at the Police stations, however, a new upgraded version of the same named as IRAD will be going live and operational soon. Both the systems have shared objectives and hence the SI scope of work will include integrating the existing RADMS system eventually to be transitioned into the new IRAD system with CCTNS by Push and pull capability through information interchange between the web Application investigation module and RADMS accident module

7.8 Integration with external Databases

The web application shall be integrated not only with SCRB and Police department systems and applications, but also need to be integrated with external systems that belong to other departments at state and central level, systems and databases that are not related to Crime or Police, but whose data requires information interchange between the Police department and other departments depending on various scenarios – crime investigation, driving with expired/revoked driving license, individual verification, premise verification, license checks, etc.

The SI scope of work will include development of required APIs and web services to integrate all such systems with the core web application to share required information back and forth as agreed and decided by the respective departments. The required approvals for integration with external databases shall be obtained by SCRB.

The list of other department databases to be integrated is as below:

1. VAHAN and Samanvay
2. Personal Identity Databases such as Passport verification services, Aadhaar verification services, Driving License, PAN, Voter ID etc.
3. Hospitals & Health Centers- To send a requisition to any healthcare institution, as well as receive any document or communication shared by them
4. Regional Transport Office – To fetch vehicle owner details from Vehicle Number.
5. Licensing Authorities- To fetch license validity information for the officers to be able to instantly view the validity status and take necessary action on-the-go.
6. Revenue, Tax, Census etc.

7.9 Integration with Communication channels & Payment Gateway

The web application shall be integrated with communication channels such as E-mail services, Short Messaging Services etc. to enable communication between users across various modules in the application. The web application shall also be integrated with Payment Gateway services

such as PayGov (or any other payment gateway assigned by TN police) as citizens avail paid services from the Police Department through citizen services portal.

8. CCTNS 2.0 - Project Requirements & Deliverables

The scope of work of this RFP is to select SI who shall procure, install and commission the hardware and infrastructure for department units, and, design, develop, install, test and deploy the CCTNS 2.0 application software and successfully Implement & Operate, Maintain & Manage the System till end of contract period. The scope has been divided into Implementation Phase & O&M Phase.

Based on the above detailed Envisaged Development and Integration Modules for the CCTNS 2.0 Software, mentioned below is an indicative list of activities to be performed by the System Integrator.

8.1 Implementation Phase- Overview

The project implementation phase starts from the date of signing of contract with the successful SI till the date of Go-Live. The SI shall design, develop, install, test and commission in the Police Stations, Higher Offices & Special Units as per the detailed technical, functional and non-functional specifications and schedule of requirements as given in this RFP. The SI shall peruse the storage and server infrastructure at the State Datacenter that is currently being used for CIPRUS operations, to host the new web application modules and any other systems to be developed in the future, for the necessary IT compute & support services at all the locations in scope as per the RFP requirements.

The following lists out the Project tasks and high-level deliverables for the System Integrator (hereafter referred to as SI):

1) CCTNS 2.0 System - Design, Documentation, Prototype Development, Installation, Development, Configuration & Integration of all system components

2) Integration of CCTNS 2.0 system with existing internal & third-party applications

3) Operation and maintenance of existing servers at TNSDC (State Datacenter) and new servers to be supplied in Phase 2

4) The migration of legacy data from current CIPRUS 1.0 database to the envisaged CCTNS 2.0 database structure. The SI shall be responsible for creating or updating master data and migration of historical investigation data for functioning of the envisaged system.

5) Testing of applications, including test cases preparation and test reports for various tests as specified for the all newly developed CCTNS 2.0 system

6) UAT Support - Setting up UAT environment & assisting SCRB and police station staff and other user categories during UAT phase.

7) The SI may use the currently functioning CA EMS Helpdesk whose perpetual licenses have been procured but support for the current version of EMS by CA Technologies has

expired. The SI may use the existing system provided its support is procured by the SI. In case the SI is unable to procure or provide support for the existing system, the SI will have to procure a new EMS software for use. A detailed specification of the existing CA EMS is mentioned in Annexure 4 in this volume of the RFP.

8) The SI shall carry out the necessary Change Management & Capacity Building for the project before pilot as well as full-scale roll out- SCRB Staff and Other external stakeholders for effective rollout of the end-to-end system.

9) The SI shall also support the TPA in successful audit completion (Security & Performance audit, Non-Functional requirements, audit etc.) & certification prior to Pilot Roll out and Full Scale Roll out.

10) The SI shall perform Project documentation and Knowledge Management across the complete scope of the project including but not limited to hardware and site infrastructure commissioning, issues reported and governance mechanism, knowledge repository of resolution of critical issues, application development knowledge articles, test case scenarios and strategy, project milestones and all deliverables submitted, etc.

11) Pilot Implementation and Rollout- The envisaged web application shall be rolled out on a pilot basis comprising of some rollout districts and police stations. After pilot implementation, signoff and issue resolution, full scale implementation will resume. Details of implementation schedule has been listed out in Section 9.1.

12) Post the pilot implementation, the system shall run through a stabilization period of 45 days, during which the system should meet the pilot operational SLA requirements mentioned in this RFP. The SI shall support the security, performance, vulnerability & non- functional requirements audit done by third Party Audit Agency appointed by SCRB. Only on compliance to the same the system shall deem to be stable for hosting at TNSDC and fit for full scale Rollout.

Note: -

13) In each phase, the selected System Integrator shall take formal approval of SCRB for deliverables (including documentation); only then shall the selected System Integrator commence with the next phase.

14) It is to be noted that System Integrator would be required to visit the various offices/locations of the Department across the state to ensure successful completion of their obligations under the Project. It is the responsibility of the selected System Integrator to plan these visits at their own cost.

8.2 Operation & Maintenance Phase- Overview

This phase shall start from the date of Go-Live and extend for 5 years Operation & Maintenance. The following outlines the broad areas of scope of work for the SI in this phase:

a) Operations & Maintenance of the web application during the contract period.

b) Operations & Maintenance of the servers for uptime and utilization during the contract period.

c) Coordination with OEMs, Network Service Providers, State Data Center and any other vendor partners.

d) Operations & Maintenance of Helpdesk

e) Knowledge Management.

f) Exit Management & Knowledge Transfer.

During the project tenure, the SI has to submit stage-wise reports, as specified in various sections of this Volume of the RFP and it shall be done strictly in accordance with the scope of work.

8.3 System Study & Solution Design

The SI shall prepare a detailed document on the implementation of the web application with respect to design, development, configuration and integration as per the requirement of SCRB.

a) The SI would be required to study the existing system and functioning of the SCRB in a manner that will enable the selected SI to meet all the requirements of this RFP.

b) The SI shall gain an understanding of the existing system and requirements of the proposed system through structured questionnaires, interviews with user groups, primarily Crime & SCRB supervisory officers, SCRB PMU and Station staff.

c) On gathering the requirements, SI shall analyze these requirements to ensure the requirements are complete, accurate, consistent and unambiguous.

d) On completion of the study, the SI is encouraged to suggest to the SCRB additional functionality (over and above that mentioned in this RFP) or clarity that may be included in designing the proposed system to meet the operational requirements of the Department.

e) The functionality of the proposed system would thereby be agreed with the SCRB before beginning the design of the system.

As part of the System Study, the SI shall be responsible for Preparation of below documents by studying the processes related to crime investigation, other workflow processes related to Police activities, and interactions related to other external systems of the CIPRUS system:

Milestone	Scope of Work for System Integrator
Inception Report & Project Plan	The SI shall prepare & submit the Inception Report and Project-plan for the implementation of the complete computerization solution indicating the following details **a)** Understanding of project scope & assumptions, dependencies &

Milestone	Scope of Work for System Integrator
	constraints. **b)** Project Team structure, Manpower and Deployment plan of the various resources at each location. **c)** Team composition with Roles & responsibilities of each member. **d)** Communication structure & review meeting plan. **e)** Project plan giving details on schedule for various tasks, activities, subtasks, timelines, interim and final milestone deliverables, resource deployment plan etc. (SCRB reserves the right to change the sequence of tasks, sequence of development of modules as per their requirement). **f)** Prepare Project Monitoring plan. **g)** Call out dependencies on SCRB or any other organization for each of the major tasks envisaged in the project. **h)** Management and control mechanism for the project. **i)** Project Risks & Mitigation Plans. **j)** Preparation of Technical Architecture Document (Application, Network, and Security). **k)** Prepare Server and Storage management Strategy. **l)** Prepare Legacy data migration and integration Strategy **m)** Prepare Data backup, archival, retention and disposal policy. **n)** Project Plan for Application Implementation. **o)** Preparation of the IT Infrastructure Security plan. **p)** Preparation of IT Infrastructure deployment plan for Application.

Milestone	Scope of Work for System Integrator
	The SI needs to identify the stage and activities where they will need time from SCRB Project Governance Office or SCRB staff and ensure the same is communicated well in advance for 100% involvement from SCRB side.
Updating Functional Requirements Specification	**a)** The SI shall study the existing functionalities of each process. The SI shall be provided with high level design documents, concept notes and high-level module workflows by SCRB PMU based on which the SI shall design the System Requirements Specification document. The SI needs to jointly reference PMU envisaged module preparatory studies, RFP FRS, and conduct other discussions with SCRB to build application and database design based on the same. b) The SI if need be may interact with relevant SCRB staff and other detachment teams from police stations to study, analyze and conclude implications of real-world challenges and experiences of using the current application vis a vis the need areas for the envisaged system. c) The SI in consultation with SCRB shall conduct an analysis of the existing FRS and capture all the changes/ updates required in the base version of the FRS based on their study of modules as explained in this RFP. d) The SI should include the list of additional functions that would result in further improvement in the overall application performance resulting into better experience for internal and external users of the application. **e)** Based on the functional requirements revised by SI, they need to identify the all the modules and submodules required to be developed for the proposed SCRB System. **f)** SCRB reserves the right to add/ remove/ modify the Functional requirement specification of the proposed System at any point during the

Milestone	Scope of Work for System Integrator
	tenure of the project.
HLD, LLD, SDD, Data architecture document & SRS preparation	**a)** The SI shall prepare and submit a High-Level Design (HLD) Document, Low Level Design (LLD) document, System & Software Requirement Specification (SRS) and System Design Document (SDD). **b)** A comprehensive HLD document shall contain (but not limited to) Data Flow drawings, proposed system architecture, Entity Relationship (ER) diagrams and other data modelling documents, Logical and physical database design, Data dictionary and data definitions and, Application component design including component deployment views, control flows, etc. as per the standard laid down by Government of India/Tamil Nadu. **c)** A comprehensive LLD shall detail each and every module of the system with the functional logic involved such as (but not limited to) **d)** Application flows and logic. e) Module wireframes **f)** GUI design (screen design, navigation, etc.). **g)** A comprehensive SRS shall define what the software will do and the expected performance. The document shall indicate the additions/ modification that need to be made to the business process in view of project implementation. The Detailed System Requirement Specifications (SRS) detailing processes of SCRB based on functional and nonfunctional requirements. h) SRS shall be reviewed by the PMU & SCRB Strategic Project Management Team. Based on their recommendation, SCRB Project Governance office would approve the SRS with which the SI would develop the application. i) The SRS approved by the Department will form the baseline for all subsequent phases of application development and deployment from an Application requirements perspective (e.g. for testing, identifying "change" to requirements etc.). Detailed Collaboration and class diagrams

Milestone	Scope of Work for System Integrator
	also to be prepared. **j)** Technical Architecture Document (Application, DC & DR Hosting, Network, Application Security and Deployment architecture). **k)** Database Architecture detailing interface and integration architecture, Database architecture, including defining data structure, clustering/ mirroring, back up strategy, data archival, data dictionary as per requirements of data storage in English. The SI is required to update documents such as FRS / HLD/ LLD/ SRS etc. as and when any enhancements / modifications/ upgrade/ Change request implementations are being made to the SCRB applications to reflect the latest enhancements/modifications made to the application till the end of the contract period.
System design	**a)** Based on the requirements study completed, the design of the System shall be done by the selected System Integrator. **b)** The SI shall design an Integrated System architecture to meet functional and nonfunctional requirements proposed by SCRB. **c)** The SI shall ensure the envisioned System has seamless integration among all the modules developed as a part of proposed System and with legacy in-house and external applications. d) The SI shall adopt appropriate load balancing and techniques in the System design for meeting the requirements of the RFP. **e)** The SI need to prepare proposed Application architecture, Network architecture, Security architecture, Database schema and database structures, Deployment architecture, User Interface, Unified Modeling Language (UML) diagrams, Object-oriented analysis and design approach. **f)** The SI shall use Service-oriented architecture (SOA) style and

Milestone	Scope of Work for System Integrator
	principle of software solution design.
Data Migration Plan	The SI shall access the legacy data, come up with Data Migration strategy, and plan from legacy databases from all locations- comprising of timelines, resources and support required from SCRB.
Change Management & Capacity Building Plan	The SI shall prepare change management plan for SCRB and external stakeholders and Capacity building/ Training plan for Pilot and full-scale Training.
Requirements Traceability Matrix	The SI shall ensure that developed system is fully compliant with the requirements and specifications provided in the RFP such as functional, non-functional and technical requirements. For ensuring this, the SI shall prepare and maintain a Requirements Traceability Matrix based on Functional Requirements Specifications (FRS), Non-Functional Requirements Specification, and Technical Requirements and shall be updated, expanded and fine-tuned by the SI periodically ensuring compliance with the requirements.

The above list of tasks is indicative. The full detail of Project Deliverables, documents and reports to be submitted to SCRB has been listed out in Section 8.23 (Project Deliverables, Documentation & Knowledge Management)

8.4 Application Design, Customization/ Development, Configuration, Installation & Integration

The SI shall be responsible for Design, Development, Testing, Deployment and Maintenance of all the Applications for proposed system, which includes the following:

1) **Core Modules –** The SI shall design and develop the core modules like Investigation, CSR and Regulatory framework modules where user shall capture all master information related to crimes in the State
2) **Tools and Portals on CCTNS Platform –** The SI shall design and develop all the tools and portals that Police Officers, Citizens and other external users like Courts, Insurance Companies, etc. will use for specific purposes, for example, field mobile applications for officers, citizen services portal for citizens, etc.
3) **Core Admin Modules –** The SI shall design and develop a robust backend admin architecture where various sub modules like dashboard building, form and report generation capabilities will reside. The admin module will also ensure integrity of the database through proper data validation and correction workflows.
4) **Integration with SCRB Applications –** The SI shall integrate the core web application platform with other applications already functional or being developed by SCRB through other parties and agencies. (ex. E-beat, SOPs, Crime Analytics tool, FRS, etc.)
5) **Integration with Central Systems –** The SI shall integrate the core web application platform with other central systems for data sync, sharing and periodic reporting purposes to NCRB, MHA, etc.
6) **Integration with other Systems of TN Police –** The SI shall integrate the web application platform with other systems being operated by Tamil Nadu Police like iRAD, traffic analytics, e-challan system, etc.
7) **Integration with external Databases –** The SI shall integrate the web application platform with other external department databases which the department shall need to access information like Aadhar, Voter ID, PDS, PAN, Passport, etc. and also provide provision to share documents online with other departments like Courts, Forensics, Hospitals etc. as and when required.
8) **Integration with Communication Channels & Payment Gateway-** The web application shall be integrated with communication channels such as E-mail services, Short Messaging Services etc. to enable communication between users across various modules in the application. The web application shall also be integrated with Payment Gateway services such as PayGov (or any other payment gateway assigned by TN police) as citizens avail paid services from the Police Department through citizen services portal.

These components need to be developed, integrated and maintained along with all of the necessary modules, utilities, system drivers and documentation in line with industry standards as mentioned in Section 8.22.

8.5 Demo of System Components

The SI shall create prototype of SCRB system components to simulate the important use cases of each module of the SCRB system component under development. This activity shall be performed during the initial stage of application development of each module and shall be showcased to SCRB, where the users can experience a working user interface and they can suggest any change in features or graphical user interface, if needed. This activity shall help in getting valuable feedback in developing the final application.

1. The SI shall demonstrate the working prototype to the SCRB Project Governance Office and other key stakeholders for initial evaluation. The feedback shall be taken for application development.

2. If the user is not satisfied with the current prototype, SI needs to refine the prototype according to the user's feedback and suggestions.

3. This phase will not be over until all the requirements specified by the user are met. Once the user is satisfied with the developed prototype, a final system is developed based on the approved final prototype.

8.6 Details of Existing Portals, Apps and Website

In accordance with the integration modules, the SI will have to perform the following 2 scenarios:

1) For all existing systems that will be disposed off and new system will be rebuilt with revised specifications, all legacy data to be securely migrated to the new platform

2) For all systems that have been envisaged for the future, or are under development currently, the SI shall develop the module from scratch and integrate with the core module.

A list of existing systems is given below that will need to be developed with revised requirements, Retaining the core functionalities:

Category	Portal/ Apps	Details
Web portal	SCRB CCTNS WEBSITE	Managed by- NIC Owned by- SCRB Hosted- TNSDC
Login based portal	OFFICERS' PORTAL	
Web portal	CITIZEN SERVICES PORTAL	
Mobile application	FIELD OFFICERS' MOBILE APP	
Internal SCRB Application	MISSING PERSON UIDB TOOL	

8.7 Application Testing

Once the application development has been completed by the SI, the SI shall thoroughly test the complete system at their end. The module-wise testing of the complete system shall be performed by the SI. The SI shall prepare the software testing plan, procedure & test cases for conducting test on various modules of the system.

8.7.1 Development, Testing, Staging & Production Environment

1. The SI shall have to provision for a separate development, test, staging and production environment.

2. The SI shall provide user test environment logins to SCRB for the various tools used by the selected System Integrator during the implementation phase of the applications.

3. The Application testing environment shall be used for conducting application testing during implementation and O&M phases for change requests.

4. The development, test and production environment shall be maintained by the selected System Integrator and transferred to SCRB at the end of the Contract.

8.7.2 Indicative list of Testing

The SI shall carryout following software testing for the system developed including:

1) Unit Testing
2) System Testing
3) Integration Testing
4) Functionality Testing
5) Performance Testing (Full Load/ Stress Test)
6) Integrity Testing
7) Security Testing

For the performance and load testing, the System Integrator shall be required to simulate the testing environment using the appropriate tools in its own environment. Under controlled environment, by applying pressure/stress on a system, performance of the system shall need to be evaluated to match the SLAs.

8.7.3 Deliverables from System Integrator

1) The SI shall obtain the UAT sign-off from SCRB on testing approach and plan.

2) The SI shall submit the test reports listed above for review by SCRB.

3) The SI shall fix the bugs/errors found during the testing, document the results of the testing and submit a successful test completion report to SCRB.

Only after the entire functionality, performance and non-functional requirements of the system as mentioned in this RFP or as later approved by SCRB during design phase have been tested satisfactorily by the SI; the System shall be handed over to SCRB for User Acceptance Testing.

8.8 Test Environment

The SI shall maintain an exclusive test environment login during the entire duration of the project for the purpose of conducting UAT and security, performance, VAPT, NFR audits by Third Party Auditors. The test environment logins shall be handed over to SCRB during Exit process.

8.9 User Acceptance Test (UAT)

After successful completion of the application testing by the SI, the complete system access shall be given for User Acceptance testing by identified subject matter experts and senior staff of SCRB. The prime objective of UAT is to make sure the system meets the requirements of FRS and SRS and meets the desired objective of SCRB. For conducting the User Acceptance Testing, the SCRB shall identify the respective staff from the department, who shall be responsible for day-to-day testing operations of the modules developed through the Project.

The SI shall develop the UAT test plan and a detailed User Acceptance procedure. The SI shall prepare a comprehensive list of functional test case scenarios for SCRB to perform the testing. The same shall be reviewed and agreed by SCRB. A high-level approach to be followed by the SI for the acceptance testing is mentioned below:

1. UAT shall be applicable once the web application is operational and all the modules under the Contract are operational and integrated.
2. UAT shall be performed once the entire application is developed.
3. SI shall prepare the sample data for UAT and get a signoff from SCRB.
4. SI to share user manual for UAT for all the internal and external users.
5. UAT shall involve:
    a) Development of Test cases by SI and their approval by SCRB.
    b) Setting up of UAT environment.
    c) Handholding of SCRB officers, other staff and other external stakeholders for performing UAT.
    d) Application functional testing and testing of other Quality-of-Service requirements by Department.
    e) Preparing UAT report by SI.
    f) Documenting recommendations/ changes suggested by users.
    g) Modifications/ Inclusion of new features based on recommendations.

Before the commencement of Acceptance Testing, the SI shall confirm their readiness for UAT. The SCRB shall engage in a comprehensive system review & User Acceptance Testing with functional use-cases & predefined templates. For all tests performed by SCRB users, the SI shall prepare the test reports and submit to SCRB for approval. The Defects identified in any round of UAT by SCRB shall be communicated to the SI. The SI shall do the needful to troubleshoot or resolve the defects and repeat the UAT process. This iterative process for UAT shall be performed till zero defects achieved for the test cases developed.

In case of any observation made during the UAT, SI shall make necessary corrective measures & release a new version of the application. Each version release shall have proper documentation to articulate the type of change made effective in the current release along with the FRS/ SRS/ Traceability matrix update.

The SI shall adhere to following points during the UAT stage:

1. The SI shall ensure that errors detected in previous round of tests are not repeated in successive tests.
2. The software application and test environments required to conduct UAT by SCRB shall be provided by the SI along with all the information and support necessary on-site to complete the UAT. The test environment maintained by the SI shall be transferred to SCRB / New SI at the end of this contract.
3. The SI shall inform SCRB in writing 2 days in advance of the date by which it would be ready for UAT.
4. SCRB reserves the right to appoint a Third-Party Assessment and Acceptance Agency to review and evaluate the System Integrator on test cases and test results.
5. The SI shall maintain documentation including but not be limited to the following:
    a) Test Plan and Procedure
    b) Test cases
    c) Test results and reports
    d) Test assumptions
    e) Test coverage and boundary conditions
    f) Change request and modifications requirement
    g) Version release documentation for SRS update

6. The SI shall provide and ensure all the necessary support for conducting the UAT by the identified staff of SCRB, who are responsible for day-to-day operations of the functions automated through the SCRB Application. The SI shall share the test cases and the testing procedure with the identified staff of SCRB.
7. The SI shall fix the bugs / errors found during the testing, document the results of the testing and submit a report to SCRB.
8. The SI shall share report on implementation of SCRB approved access Control and Authorization requirement.
9. The SI to assist in UAT in the devices installed with the Officers Field Device Mobile Application for the development and integration with applications developed as part of this CCTNS 2.0 project , e.g., integration of Bandobust Manager application with e-Beat

system, to the extent that the integration functionalities are working properly with the apps developed by the SI.

Note: - For all modified / additional requirements- SI needs to follow the same cycle of: Updation of SRS, Application development, testing, UAT etc.

8.10 Business Continuity and Disaster Recovery

The SI is expected to develop and implement a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP). An indicative non-exhaustive list of activities to be performed by the selected SI is mentioned below:

1) The System shall be able to handle long outages of network without affecting the consistency of data at both DC & DR locations.

2) Designing and implementing adequate data backup, business continuity and restoration procedures for the departmental data (including but not limited to the database, attachments and all other data elements created in and generated by the system and users).

3) SI shall provide Centralized Management GUI from where SCRB can manage all the replication processes. SCRB shall be able to analyse the data lag and time lag from the replication console in real time. The System shall have options for:

    a) Real time monitoring of RPO and RTO at database and application level.

    b) Real time monitoring of DC & DR health and alerts.

    c) Provide alerts on event threshold conditions such as RPO deviation and replication log Space full at application level and support policy-based actions for these alerts.

    d) Single dashboard to track DR readiness status to handle all applications.

    e) Central console to start & stop for each application.

f) Report on number of steps and estimate of time for failover recovery for each application & each server.

g) The System shall have feature/ option to generate readymade reports on RPO deviation, RTO deviation, Application DR readiness status, WAN utilization. The System should have the ability to create UI based custom reports, data can be exported in formats like excel/word/pdf/images/dashboards etc.

4) The SI shall ensure that there is no single point of failure and adequate level of redundancy is being built in to meet the uptime and other requirements of this project. While building redundancies, it shall be ensured that failure of a single component of communication link does not result in non-compliance to the RPO & RTO requirements. All the redundancies shall be in auto fail over mode so that if primary component fails, secondary component shall automatically take over.

5) Replication between Data Centre and DR Site as well as changeover during disaster shall be quick for minimal impact on user experience. Ensuring data backup till the last transaction occurring in the system to ensure enhanced service levels. RPO and RTO objectives are as below and shall be strongly adhered to.

RPO = 0 minutes

RTO <=60 minutes

6) The System shall support both synchronous and asynchronous mode of operation and in both the modes and it shall assure 100% data consistency.

7) The SI shall ensure zero data loss over synchronous between the primary DC and Disaster Recovery site.

8) The SI shall enable data replication between SDC and DRC site on real time basis.

9) The proposed Storage replication technology shall not have any distance limitations on asynchronous replication.

10) The Storage Replication capability shall be certified for performing replication to heterogeneous storage models from different OEMs.

11) The replication technology shall support different types of data (structured, unstructured etc.).

12) The solution shall allow for disk-based replication log so that it can be sized depending on SCRB requirements. The disk logging function shall log just the blocks that are getting changed and not the entire track to ensure there is no performance degradation.

13) The proposed System shall always be capable of maintaining data consistency by providing Write Order Fidelity.

14) The System shall support SAN-to-SAN replication.

15) The System shall be flexible to support one-to-many and many-to-one scenarios.

16) The SI shall also ensure daily automatic backup of business and daily transactional data at SDC.

17) Designing and implementing data synchronization procedures for the DR Site. Periodic testing may be done to ensure that all replication and data synchronization procedures are in place all the time. Replication between Data Centre and DR Site as well as changeover during disaster shall be automatic and real-time for minimal impact on user experience.

18) The System shall support both automated failover and manual failover capabilities.

19) The SI shall provide remote management of DC, DR Infrastructure & connectivity.

20) The SI shall ensure that operation related to data such as Backup, Recovery, Restoration, and Synchronization at Disaster Recovery Centre are tested and implemented comprehensively on a regular basis.

21) The proposed System shall facilitate frequent (at least once a quarter) DR drills by utilizing space-optimized snapshots at DR without pausing/suspending replication and shutting down the application at Primary site. The System shall have feature/ option such as:

    a. Automated/manual switchover and switchback capabilities or applications.

    b. Automated drill reports with evidence of control and granular timing of each step.

22) The web application shall provide infrastructure/application based and role-based access control to users.

23) The DR shall be appropriately planned to ensure High Availability of the servers as per SLA prescribed in the RFP.

Other features & Requirements to be provisioned by SI are as follows: -

1) The interaction between the Internet zone and the Intranet zone shall be through a firewall such that all unwanted traffic is prevented from entering this zone.

2) Built-in file replication that is not tied to a specific platform or OS for application environment protection with the following features:

    a) Replication from multiple sources to multiple destination files/folders and nested files & folders

    b) Preserves file attributes & option to skip or copy open files

    c) Maintain DC & DR equivalence. Files deleted on the primary will be deleted on DR

    d) Provides log of replicated file names, pending files and number of files to be replicated and statistics on throughput

    e) Restart replication after a break from last successful replicated point

    f) Replicate only portions of the file that have changed

    g) On the fly compression for reduced bandwidth

h) Ability to provide alerts when specific files change on production systems

8.11 Data Migration and Document Management

8.11.1 Data Migration from Legacy Database

The legacy transactional and master data from the existing CIPRUS 1.0 application that gives the history of crime cases, FIRs and other records that has been stored and in use since deployment of the existing system, are recorded and stored in the current architecture within the existing database managed by the current SI.

The selected System Integrator is required to migrate all the existing data in CIPRUS 1.0 in its current database to the new database system that will be designed, deployed and hosted for web Application-CCTNS 2.0. The System Integrator shall take following steps including but not limited to:

1) Indexing of Database- Capturing Server location, Server Manufacturer name, Server Name
2) Performing the backup
3) Consolidation of data
4) Prepare the Data cleansing and migration plan and submit to SCRB for approval
5) Ensure minimum downtime or performance issues at the time of data cleansing and migration.
6) On SCRB's approval, prepare the requisite migration architecture and then clean and move the data to the new target environment
7) Standardization of the data and generation of Master IDs
8) Ensure the accuracy and completeness of the migrated data. Department reserves the right to verify the accuracy and completeness of the migrated data on its own or through its nominated agencies.

9) Ensure migration of all data is completed before rollout of the new application

The data migration has to be completed for all information from CCTNS 1.0. An estimated total quantum of data to be migrated to the new CCTNS 2.0 system shall be approximately 1 TB, which may however be subject to change depending on the completeness and quality of the existing data.

8.11.2 Data Migration Validation

1) The SI shall have an effective procedure for validating, tracking the progress of data migration activity

2) The SI shall deploy corrective mechanism for discrepancy in data migration activity ensuring zero data loss

3) The SI shall perform validation of complete data before and after migration of data with the source database ensuring there is no missing data, doesn't contain null values and is completely valid

4) The SI shall ensure removing all the discrepancies in the migrated database and making it completely in sync with source database for signoff from the department

5) SCRB reserves the right to independently validate the migrated data with the source database and penalize SI if there is a data loss. The SI will have complete support for data migration from the department and current software developer but the end responsibility of ensuring successful data migration lies with the SI.

8.12 Change Management & Capacity Building

The SI shall be required to provide training on various aspects of newly developed system to enable effective use of the new system to achieve the envisaged outcomes. The scope of work of the selected System Integrator is described in this section of the RFP.

Milestone	Description of Scope of Work for System Integrator
Change Management	1) The SI shall assess the change readiness of the organization & based on it shall refine the change management approach to manage various stakeholder groups on an ongoing basis. 2) The SI shall define structure of the team - leadership as well as execution team to drive the change with clearly assigned roles & responsibilities. 3) The SI shall obtain a sign off on the change management team structure, change management approach from the SCRB Project Management Office. 4) The SI shall facilitate the SCRB Project Management Office for launching the different Change Management interventions as proposed in the change management plan.
Capacity Building	1) Training Plan: The selected System Integrator shall be required to prepare a detailed training plan including the type/ modules of trainings to be conducted, targeted audience, location, dates for training, duration and training content. 2) The training plan shall be submitted to SCRB 2 months in advance (both for pilot level and full-scale level training) and approval from the SCRB. 3) In order to deliver quality training, the SI shall perform the following: a) Training Need Assessment.

Milestone	Description of Scope of Work for System Integrator
	b) Identification of training modules. c) Training Content Development. d) Role wise mapping of modules. e) Training calendar preparation. f) Assessing Change Management Impact. g) Addressing all employee related issues related to migration from As-Is Capture employee feedback & training program improvisation. 4) The SI shall prepare detailed Capacity Building plan for both Pilot and Full Scale Roll out for providing Training to the different stakeholders of the Project. 5) The Capacity Building Plan shall indicate the schedule, scope, resource requirement & participant details of the following trainings including but not limited to: a) Project Management. b) Change Management/ Project Sensitization Training. c) Basic IT training. d) End User Training on various SCRB system and system components. e) Training on SCRB Systems. f) Database and Admin Module Administration g) Train the Trainer (up to 100 personnel)

Milestone	Description of Scope of Work for System Integrator
	6) The Capacity Building Plan shall include mechanism to track the skill & knowledge of different participants. 7) The SI shall obtain a sign off from the SCRB Project Management Office on the proposed Capacity Building Plan including calendar, participants covered in each training, training location, training content etc. 8) The SI shall carry out the different Capacity Building Trainings for the stakeholders as per the schedule provided in the approved Capacity Building Plan. 9) The SI shall carry out the training in two phases: as per the Project timelines: a) Training during Pilot phase. b) Training during Full-scale operation. 10) The SI shall be responsible for the Infrastructure requirement for conducting the training programs – pilot and full-scale trainings 11) The SI shall be responsible for logistics of Trainers. 12) The SI shall share the Training Completion report. Note: All training related activities including training calendar, training materials, logistics, assessment, feedback etc. as detailed in the below sections shall be done for both Pilot & Full-Scale trainings.
Change Management & Capacity Building Plan	1) The SI shall carry out the periodic review of implementation of the change management & capacity-building plan with the SCRB Project Management Office. 2) The SI shall assess the impacts of each change management initiative

Milestone	Description of Scope of Work for System Integrator
	using a multi-dimensional approach (i.e. operational, people, organizational, leadership & management, infrastructure and interrelationships) & submit the findings of the same to the SCRB Project Management Office. 3) The SI shall preform Training assessment, Feedback collection, updation of training curriculum of training material based on feedback. 4) The SI shall track the confidence of the stakeholders in the new skill & knowledge following the Training Sessions and submit the findings of the same to the SCRB Project Management Office. In case the findings suggest that the Trainings were ineffective, the SI shall provide additional training to the stakeholders at no additional cost.
Training Documentation	1) The SI shall submit the course materials, presentations & any other material used in the Training programs to the SCRB Project Management Office. The SI shall provide a detailed online training manual for each module of the newly developed systems. 2) The SI shall prepare & submit the User manual indicating the details of menus & instructions on how to perform specific tasks in the system using screenshots 3) The SI shall prepare workflows for each module/ sub modules and processes 4) The SI shall prepare & submit the System Administration/ Configuration manual indicating the system settings for each module. 5) The SI shall prepare & submit the User Manual indicating the system operational procedures.

8.13 Application Security

The Security features shall include but not limited to-

1) Ensure all security features in place to prevent hacking including Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, Phishing and spear phishing attacks, Malware attack, SQL injection attack, Man-in-the-Middle attack etc.

2) Audit trail and logging of user activities on website for the website administrators and SCRB.

3) Administrator and officials of SCRB should be able to generate security report comprising number of attacks, time of attack, IP, Network, page for which attack was attempted.

4) Feature to block a particular IP / range of IPs or Network from accessing the website.

5) Usage of HTTPS protocol.

6) Make necessary adjustment to CMS default settings.

7) Regular backup of website data.

The TN State Datacenter where the applications shall be hosted has Cybersecurity components embedded within their server and switching infrastructure. The Bidder shall peruse the same existing server-side security components.

The Bidder shall, however, ensure the application end point security and other web security components are built into the systems and they must comply with the application security requirements and guidelines.

A detailed list of Application Security compliance requirements are listed in Annexure 7.

8.14 Third Party Audit

8.14.1 Security & Performance Audit

SCRB reserves the right to get the developed system certified by Third Party Agency at any point of time during the implementation and O&M phase of the contract. The Assessment and Acceptance testing shall be performed by the same Agency referred as Third-Party Audit (TPA) Agency.

The TPA will be performing assessment, acceptance and certification of the system deployed by the SI. They shall also reviewing all aspects of project development and implementation covering software, hardware, site preparation and networking including the processes relating to the design of system architecture, design of systems and sub-systems, coding, testing, business process description, documentation, version control, change management, security, service oriented architecture, performance in relation to defined requirements, interoperability, scalability, availability, adherence to the industry guidelines and standards and compliance with all the Functional, Non-functional, Technical, Security requirements of the RFP and the agreement made with SI.

TPA assessment and certification intends to verify that the System (including all the system components as discussed in the scope of work) meets stated requirements, standards, specifications and performance. The following shall be checked against clear, quantifiable metrics:

1) Functional Requirements.
2) Infrastructure (hardware and network) Compliance Review.
3) Availability of the Project services in the defined locations.
4) Performance Testing including Load Testing.
5) Security Requirements.
6) Manageability.

7) SLA Reporting System.

8) Project documentation (Design, development, configuration, training and administration manuals etc.).

9) Data Quality Review.

The developed system shall satisfy both Third Party Acceptance Testing and Internal User Acceptance Testing.

The Third-Party Agency after obtaining necessary approval will be designing the procedures and parameters for assessment and acceptance of the deployed system.

The assessment shall be done in two stages: before Pilot Stage roll out and before Full Scale Roll out stage. The third-party audit before the Pilot stage rollout will consist of security audit and VAPT. The SI shall provide required necessary support to the assessment agency for conducting audit of the system from various aspects such as-

Audit Criteria	Minimum Requirements
Review of Functional & Non – Functional Requirements	1) Review the system developed by SI against functional requirements signed-off between SCRB & SI. The review shall include all the functional, non-functional and all other requirements stated in the RFP. 2) Audit of Requirement traceability matrix maintained by SI 3) Audit of User Acceptance Testing report with respect to the functional requirements 4) TPA may develop its own testing plans for validation of compliance of system against the defined requirements
Application	Verify the conformity of the Infrastructure (IT, Network & non-IT

Audit Criteria	Minimum Requirements
Infrastructure Compliance Review	infrastructure) supplied by the SI against the application web and database hosting requirements and specifications provided in the RFP and/or as in the proposal submitted by the SI.
Security Audit	1) Audit of network, server and application security mechanisms. 2) Assessment of authentication mechanism provided in the application/components/modules. 3) Assessment of data encryption mechanisms implemented. 4) Assessment of data access privileges, retention periods and archival mechanisms. 5) Server and application security features incorporated etc. 6) Security exposures to internal and external stakeholders. 7) Installation of requisite prevention systems like HIPS, Intrusion Prevention Systems (IPS), etc.
Application Testing	1) Identify the nature and type of transactions being processed by the application systems. 2) Determine systematic measures implemented to control and secure access to the application programs and data including password controls, user authentications, roles and responsibilities, audit trails and reporting, configuration and interface controls, etc. 3) Review of database structure including: a) Classification of data in terms of sensitivity & levels of access. b) Security measures over database installation, password policies and user roles and privileges.

Audit Criteria	Minimum Requirements
	c) Access control on database objects – tables, views, triggers, synonyms, etc. d) Database restoration and recoverability. e) Audit trails configuration and monitoring process. f) Network connections to database.
Performance Testing including Load Testing	1) Testing on parameters such as application response time, report generation time, concurrent sessions supported by the system, disaster recovery drill, etc. 2) Verification of scalability provisioned in the System for catering to the project requirements.
VAPT	Vulnerability Assessment & Penetration Testing.
Availability Review	Review of server uptime, security and availability across all defined locations.
Manageability Review	Usage of Enterprise Management System to verify remote monitoring, administration, configuration, inventory management, fault identification, etc.
Document Audit	Verify project documents submitted by the SI with reference to the Functional & Non- Functional requirements provided in the RFP. The documents include but not limited to: 1) Requirement gathering 2) SRS 3) Gap analysis 4) Design documents 5) Test Cases

Audit Criteria	Minimum Requirements
	6) Source code 7) Installation documents 8) Training and administration manuals 9) Version control
Data Quality	Data quality assessment for data migrated. The sample data for data quality testing shall be decided and informed to the SI by SCRB
Other Audit requirements	Specific qualifications and experience of manpower to be deployed for Helpdesk operations are below: 1) Review of backup process, including schedule, storage, archival and decommissioning of media 2) Review of change management process 3) Incident management process – covering identification, response, escalation mechanisms 4) Anti-virus (malware) controls – patching, virus definition file update 5) General computer controls review

The TPA will design the procedures and parameters for audit after obtaining necessary approval from SCRB. The Audit shall be performed in two stages:

Stage 1: Assessment, Acceptance and Certification of Pilot roll -out

Once the system has been rolled out at the Pilot locations, the SI shall notify SCRB so that the Pilot system may be assessed by the TPA Agency. The Agency would conduct various tests to assess the compliance of the Pilot with the requirements of the RFP. The shortcomings identified by the TPA in the Pilot rollout will be notified by SCRB to the SI at the earliest instance through

an appropriate process to facilitate corrective action. All the gaps identified shall be resolved by the SI after jointly discussing the timelines for resolution. This process shall be iterative till the Pilot rollout is 'Accepted' by the TPA Agency & SCRB. It is the responsibility of the SI to take any corrective action required to remove all shortcomings. Only after the System deployed at the Pilot Site is 'Accepted' by the TPA Agency, a sign-off be provided to SI in the form of Certification on the Pilot rollout and the system be allowed for full-scale roll out.

The TPA Agency shall measure the performance of the system against the Service Level baselines defined in Service Level Agreement Section 2.4 of SLA Volume 3 of the RFP. If the service levels are not meeting the baselines, the TPA may recommend the SCRB to extend the Pilot Roll out till the time Service level baselines are not met.

Stage 2: Assessment, Acceptance and Certification of Full-Scale rollout.

Once the system has been rolled out across the State post pilot acceptance, the SI will notify SCRB so that the full-scale system may be assessed by the TPA Agency. The procedure adopted thereafter is similar to the procedure adopted for acceptance and certification of pilot roll out

The SI shall address all the non-compliances/ bugs identified by the TPA. The TPA shall carryout a compliance audit and continue their process till the SI successfully resolves all the Non-conformance & vulnerability aspects of the application & the application is deemed ready for launch. Any non-conformance & vulnerability aspects identified by the TPA during this exercise shall be immediately mitigated. The timelines for nonconformance resolution shall be fixed after discussing the timelines with SCRB. A comprehensive report needs to be submitted by SI on the closure of the identified bugs/issues.

Note: A sign-off on the Go-Live will be provided by the SCRB only after the completion of Full-Scale Assessment, Acceptance and certification by TPA Agency.

8.14.2 Periodic Security and Performance Audit during O&M

It is to be noted that SCRB may get the System assessed periodically through a Third-Party Assessment and Acceptance Agency even after declaration of 'Go-live' in order to ensure continued success of the Project. The SCRB may onboard an STQC or CERT-IN empaneled TPA agency approved to conduct Security and Performance audit, Acceptance Testing and Certification of the entire system

The cost of engaging this Third-Party Assessment and Acceptance Agency and conducting the Acceptance testing and certification will be borne by SCRB.

The SI shall be required to provide all necessary support to SCRB and the selected Agency for conducting and completing the System Acceptance over the period of contract at no additional cost. Irrespective of involvement of the Third-Party Assessment and Acceptance Agency for acceptance testing and certification, the SI still needs to meet all SLAs as laid out in this RFP document. The indicative list of tests to be performed for the acceptance of the deployed system will be same as the one carried out during implementation phase covered in above section. In addition, The TPA audit will be required during the following scenario:

- Any approved Change Request in DB master, programing code level changes etc., will call for Vulnerability, Security & Performance audit.

In case of any performance degradation identified in this periodic assessment, the SI needs to highlight proactive measures to mitigate the same. Any non-conformance & vulnerability aspects identified by the TPA during this exercise need to be immediately mitigated. The timelines for nonconformance resolution shall be decided after discussing with SCRB. The SI need to make updates/ corrections/ changes for satisfactory closure of TPA comments at no additional cost. In case of any default, there shall be penalty levied as per SLA & Tender conditions.

8.15 Pilot Implementation

Before beginning of Pilot,

SI shall ensure to get SCRB signoff on following-

1) SCRB and SI shall jointly ensure that the hardware and site infrastructure at the police stations and other department offices are fully installed and commissioned and ready for use and installation of necessary drivers and updates required to run the web application.

2) SI shall complete the full acceptance testing of all IT Infrastructure commissioned in all the pilot locations and then start Application pilot rollout.

3) SI shall ensure availability of field devices for Pilot rollout of mobile compatible responsive modules.

4) SI shall ensure completion of UAT and get a signoff from SCRB.

5) SI shall also complete legacy data migration and integration with envisaged database architecture before Application pilot rollout.

6) SI shall ensure readiness of Knowledge repository / SLA Monitoring tool in all pilot locations.

7) Training for the pilot location staff shall be completed before initiating pilot implementation.

8) SI shall share all the user manuals, training documents, reference documents shared with all internal and external stakeholders.

9) SI shall also share Application release documents & System user and maintenance manuals.

10) SI should ensure that the service Helpdesk at SCRB and at Data Centre are setup and operational from the date of contract signing to meet the SLA requirements of this RFP

11) SI shall get Pilot roll out signoff from SCRB.

During Pilot,

1) Application roll out at Pilot Sites.

2) SCRB shall review the performance of the system and identify the gaps/changes in the system. The recommendations shall be accommodated by SI during system stabilization phase.

3) SI shall support TPA audit completion and modifications as per audit observations before end of stabilization period

4) Modifications in the system based on learning and additional requirements from pilot stage

5) Software Configuration report for Pilot Sites.

6) After successful completion of Pilot Implementation, the pilot locations shall continue to run the application till the date of Go-Live.

8.16 Stabilization Period

Post the pilot implementation, the system shall run through stabilization period of 45 days during the period the system shall be able to meet the pilot phase operational SLA requirements mentioned in Volume 3 of this RFP.

The SI shall chronologically consolidate all the Change Request and key learnings in the pilot phase. The SI shall present the same in the form of a comprehensive key learnings report, which shall encapsulate application debugging, change requests, resolutions, lessons learnt during the various stages of Pilot Implementation, Stabilization, Change Management, Training etc. This report shall have an exclusive section on strategy adopted for Full Scale Roll out duly addressing all the lessons learnt in the Pilot implementation. The updated Training content based on the Pilot learning also shall be finalized.

On compliance the above, the system is deemed stable and fit for Full Scale Roll-Out and Go-live signoff will be given by SCRB for full-scale roll out.

8.17 Full Scale Roll-Out, Stabilization & Go Live

On successful completion of Assessment, Acceptance and certification by TPA Agency, SCRB will provide approval for full-scale roll out. Based on the learning from the Pilot implementation,

SI shall prepare a comprehensive application Rollout strategy. The SI shall Rollout the application based on approved Rollout strategy plan.

Before Full Scale Roll Out-: - SI shall ensure to get SCRB signoff on the following-

1) SCRB shall ensure that all the site infrastructure, station hardware and datacenter server and storage requirements are in compliance with the infrastructure requirements for full scale Go-Live of the web application at all locations.

2) SI shall ensure acknowledgment and signoff of all operational and system requirements before Go-live.

3) The full-scale implementation shall involve testing of the application's compatibility and stability on both new and existing machines in the offices. This is an essential activity, as some offices will have existing hardware that will be continued, e.g., balance of desktop computers during Part – 1 of hardware commissioning.

4) SI shall ensure completion of the installation, commissioning and user acceptance of new system application and other software at all locations and submit component wise, location wise acknowledgement/ sign off document.

5) SI shall ensure availability of applications at end user points at all locations

6) SI shall ensure readiness of all APIs, web services, and gateways.

7) SI shall also ensure integration with existing internal and third-party applications.

8) SI shall ensure readiness of Knowledge repository / SLA Monitoring tool at all locations.

9) SI shall ensure completion of Full-scale training, Retraining and get a signoff from SCRB.

10) SI shall share all the revised user manuals, training documents, reference documents shared with all internal and external stakeholders.

11) SI shall get Full-scale roll out signoff from SCRB.

Once the system has been rolled out across the state, it shall go through a stabilization period of 45 days, during the period the system shall be able meet the post implementation operational SLA requirements mentioned in this RFP. On compliance, the system shall be deemed stable and fit for Go-Live.

Before Go Live: -

1) Go Live of the complete system shall be considered only when all the previous milestones have been completed and signed off by SCRB.

2) SI shall ensure that the TPA audit has be completed and the modifications as per the audit observations are completed and SI shall furnish the TPA certification to SCRB.

3) SI shall ensure all the commissioned hardware are fully functional and any defective product shall be replaced /repaired at no additional cost.

4) SI shall ensure that all identified issues during stabilization period shall be corrected.

5) SI shall monitor adherence to SLA during stabilization period and ensure adherence. The report shall be submitted to SCRB.

6) The SI shall submit all the training materials to SCRB for future reference as mentioned in Section “Change Management & Capability building” of this Volume of the RFP.

7) The SI shall submit all the project related document including, SRS, Technical Specification of application & hardware, User Manuals, Intellectual Property Rights, Source Code etc. to SCRB.

The SI shall notify SCRB on readiness for Go-Live. Go-Live is declared by SCRB when the proposed System becomes operational after successful conclusion of all acceptance tests & certification by TPA to the satisfaction of SCRB or as provided in this RFP, a sign-off on the Go-Live should be provided by SCRB.

8.18 Scalability and Software upgrades

One of the fundamental requirements of the proposed system is its scalability. The architecture designed by SI shall be scalable (cater to increasing load of internal and external users and large volume of daily transactions, upload and download) and capable of delivering high performance, with minimum investment. In this context, it is required that the system and its deployment architecture shall provide for Scale-Up, Scale-out and Scale-Down of the servers such as Application Servers, Web Servers, Database Servers and all other System components. The scalability aspect shall be thoroughly tested before full-scale rollout. The complete system shall be designed in such a manner along with lightly coupled component, which makes it easy to extend. The SI shall ensure the system meets following scalability requirement include but not limited to -

1) Ability to support increase volume of transactions/ data- The system shall have features and allow SI to augment the hardware, software and network capabilities to support the increase volume of data and maintain the same service levels as earlier

2) Scalability to include new user, services, integration with future projects of SCRB, and so on.

3) Scalability to include new locations

4) Scalability to include new modules, sub modules, workflow, data sources and so on.

5) Scalability to integrate with more applications from other departments etc. in the future.

The scalability requirement shall be met with no impact to the overall performance and usability of the System ensuring the performance of the system meets the SLA requirements mentioned in this RFP.

The necessary patch updates, software upgrades for already supplied hardware and deployed software by SI, shall be the responsibility of the SI at no additional cost. The SI shall proactively notify SCRB before any patch upgrade.

8.19 High Availability & Offline Mode

The SI shall configure the existing Disaster Recovery setup such that there is no interruption of services at the department offices and police stations. The SI shall ensure High Availability of the system. In case of interruption of network service, the offline transactions shall then be pushed to SDC/DRC automatically when connectivity is restored.

8.20 Operation and Maintenance

The SI shall be responsible for the day-to-day operations & maintenance of the system for the entire period of Contract. The Operations and Maintenance (O&M) phase will be a five-year period commencing from the date of Go-Live, wherein the SI shall Administer, Operate, Maintain & Manage the Application Software and other support services as per the requirements, SLA & contract agreement.

1) The SI shall provide the O&M for all the locations after Go-Live.

2) The SI shall have adequate number technical support team on ground throughout the O&M Tenure to meet the SLA requirement.

3) The SI shall assess the technical team composition and size on a quarterly basis to meet the SLA requirements.

4) The O&M shall be applicable for all the new software supplied to SCRB during the contract period

5) The SI shall have the technical support from all the OEMs throughout the project tenure.

6) The SI shall be required to make necessary changes in application, infrastructure & functionality in cases of changes in Policies, tax laws, statutory laws, Acts, Rules, and Government orders, SCRB of Police Department rules, etc.

During the O&M, The SI shall perform following: -

System Administration & Troubleshooting-

1) Overall monitoring and management of all IT and Non-IT infrastructure deployed by the SI for the Project including Server Infrastructure at SDC & DRC, SCRB locations, system software, application, database, and all other services associated with these facilities to ensure service levels, performance and availability requirements as prescribed in the RFP are met.

2) Replace component due to technical, functional, manufacturing or any other problem with a component of the same make and configuration. In case the component of same make and configuration is not available, the replacement shall conform to open standards, shall be of a higher configuration, and shall be approved by SCRB.

3) Perform system administration tasks such as managing the user access, creating and managing users, taking backups etc.

4) Performance tuning of the system to ensure adherence to SLA mentioned in "Service Level Agreement" Section 2.4 of SLA in Volume 3 of the RFP and performance requirements as indicated in "Non-Functional Requirements" Annexure 2 of this Volume of the RFP.

Overall System

1) Undertake preventive maintenance (any maintenance activity that is required before the occurrence of an incident with an attempt to prevent any future incidents) and carry out the architecture changes wherever needed to keep the performance levels of the hardware and equipment in tune with the requirements of the SLA. Such preventive maintenance shall not be performed during peak working hours of SCRB, unless inevitable and approved in advance by the SCRB.

2) Undertake reactive maintenance (any corrective action, maintenance activity that is required post the occurrence of an incident) that is intended to troubleshoot the system.

3) Escalate and co-ordinate between teams for problem resolution wherever required and necessary.

4) System Integrator shall be required to develop various policies relating to monitoring and management of system infrastructure such as IS (Information Systems) policy, backup and archival policy, System software update policy etc. and have them approved from SCRB during the design and implementation of the project. These policies shall be updated by the SI from time to time during the period of Contract as required to meet the requirements of the Project.

Note: -

Since the Project aims to reuse the common infrastructure created under SDC/ DRC, the SI shall be required to coordinate with SDC teams to ensure that uptime and performance requirements of the RFP are met. However, the SI shall be held solely responsible for performance and service levels of any infrastructure deployed by them as part of this Contract.

8.20.1 Applications, Software and Database

The SI during O&M phase shall Operate, Maintain & Manage the Applications on 24x7 basis as per the requirements, SLA & contract agreement in all the internal and external user locations. This shall include but not limited to test & production environment monitoring, troubleshooting & addressing the functionality, availability & performance issues, implementing the system change requests etc. The SI shall ensure uninterrupted availability of complete system at the end user point; meeting the functional, non- functional, technical & security requirements defined by SCRB in this RFP. The SI shall perform changes and upgrades to application as requested by SCRB. The following is the broad scope for maintenance and support functions with regard to the application.

Requirement	Description of Scope of work for System Integrator
Compliance to SLA	1) The SI shall ensure compliance to uptime and performance requirements of the SCRB applications as indicated in the SLA and any upgrades or major changes to the system shall be planned accordingly by SI for ensuring the SLA requirements.

Requirement	Description of Scope of work for System Integrator
	2) The SI shall submit a report on the performance of the applications against the desired SLA on a quarterly basis, required frequency or on need basis 3) The submission of SLA performance reports shall be made strictly in accordance with the RFP Document and shall get necessary approval from SCRB. The report on SLA Performance metrics shall not only capture those metrics asked in this RFP but also any other essential metric(s) deemed necessary by SCRB or the SI during this phase. 4) In case of any breach with respect to the agreed performance metrics, appropriate penalty shall be levied as per the "Service Level Agreement" section of the Volume of the RFP & other RFP Terms & conditions.
Application Software Maintenance	1) The SI shall address all the errors, bugs and gaps in the functionality offered by the SCRB applications vis-à-vis the approved SRS at no additional cost during the operations & maintenance period. 2) The SI shall identify and resolve problems like application malfunctions, data corruption and performance problems like high page loading time, frequent log outs etc. 3) Performance tuning of the applications to ensure adherence to SLAs and performance requirements as indicated in the RFP. 4) Any changes, upgrades to the system performed during the operations & maintenance phase shall be subjected to comprehensive & integrated testing by the SI to ensure that the changes implemented in the system meets the desired and specified requirements of SCRB and does not impact any other function of the system. 5) The SI shall perform the patch management, testing and installation of software upgrades issued by the OEM/vendors from time to time

Requirement	Description of Scope of work for System Integrator
	6) The SI shall deploy any necessary software updates, upgrades, patches, service packs required to make the software and applications work across all locations. 7) The SI shall submit a Quarterly Report on the changes performed in the system and resolution of issues. 8) Application logs shall be maintained and shared with SCRB on regular basis. 9) Impact assessment to be done by SI approved by SCRB before initiating any modifications, changes or upgrade. 10) Manage patch upgrade, including security upgrade with SCRB approval as and when required with minimal downtime. 11) Ensure configuration management and backups of patch to facilitate rollback in case of problems. 12) The modifications, changes, upgrade shall follow the same process as change request as detailed in Section "Change Request Management" of this Volume of the RFP and "Change Control Note" Section of Volume 3 of this RFP: a) Any change to be performed/ deployed in development & test environment prior to deployment in production environment. b) Any change request performed shall be properly documented in detail and code/ script shall be properly marked/ highlighted with comments.
Application/ Software Warranty	The SI shall provide 100% comprehensive onsite warranty of all the applications and software supplied. This shall include but not limited to upgrades, updates, preventive/ corrective (as needed) maintenance, and regular

Requirement	Description of Scope of work for System Integrator
	health check to meet the SLA requirements from the data of software Installation and commissioning signoff from SCRB till end of contract tenure.
Annual Technical Support (ATS) for Software	1) The SI from time to time shall provide the required Updates / Upgrades / New releases / new versions / Patches / Bug fixes of the software, operating systems, etc. 2) SI shall maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements and maintenance. 3) SI shall have complete manufacturer's technical support for all the licensed software problems and/or questions, technical guidance, defect and non-defect related issues. SI shall provide a single-point-of-contact for software support and provide licensed software support including but not limited to problem tracking, problem source identification, problem impact (severity) determination, bypass and recovery support, problem resolution, and management reporting. 4) All vertical upgrades within supplied IT computer & networking infrastructure shall be responsibility of the SI. 5) SI shall carry out any requisite adjustments / changes in the configuration for implementing different versions of Application Software.
Version Control - Maintain configuration information & System documentation	1) The SI shall maintain version control and configuration information for application software. 2) The SI shall maintain version control for all system documentation. 3) The SI shall maintain and update documentation of the software system including but not limited to: a) Application documentation shall be updated to reflect on-going maintenance and enhancements including FRS and SRS, in accordance with the defined standards.

Requirement	Description of Scope of work for System Integrator
	b) Application response time log. c) User manuals & training manuals shall be updated to reflect on-going changes/enhancements. d) Source Codes of the application shall be updated **Note:** Standard practices shall be adopted and followed in respect of version control and management.
Changes recommended by TPA Agency	Perform all measures to address various issues and challenges reported during the periodic TPA audit (as detailed in "Third Party Audit" section of this Volume of the RFP. The necessary changes shall be completed within the period decided in accordance with the Implementation schedule described in this RFP.
Database Management	1) Undertake end-to-end management of database on an on-going basis to facilitate smooth functioning and optimum utilization including regular database backup and periodical testing of backup data, database administration, database archival conducting configuration review to tune database, database security, maintaining the necessary documentation and managing database schema, disk space, user roles, and storage. 2) Performance monitoring and tuning of the databases on a regular basis including, preventive/ corrective (as needed) maintenance of the database as required. 3) Management of database upgrade or patch upgrade as and when required with minimal downtime on approval of SCRB 4) Regular backups for all databases in accordance with the backup and archive policies and conduct recovery whenever required with appropriate permissions.
User Management	1) The SI is required to design and implement the user management

Requirement	Description of Scope of work for System Integrator
during O&M	processes including creation of user/ group profiles to ensure that the end users are provided only with specific privileges required for designated operations. 2) The SI shall implement the User-ID naming protocol for all the users after obtaining the sign-off with the SCRB Project Governance office. Separate user ID shall be created for each user, Group IDs department/ sections, which uniquely identifies that user/ department/ section across SCRB. 3) The SI shall ensure that during the log-on process, all the updated profiles and antivirus signatures are automatically updated on the end user system without any user intervention. 4) The SI shall ensure that the end users shall only be provided with role-based privileges and access. Such roles & privileges shall be signed-off with SCRB. 5) The SI shall ensure that the end users shall be provided with updated accesses in case of role change (promotion, transfer etc.). Such roles & privileges changes shall be done only on request from SCRB. 6) The SI shall provide selected users with the access to the system administration activities for all activities as described under Core Admin module section under Envisaged development modules in Section 7.3. 7) The SI, at any point of time, shall ensure that only authorized/licensed software/tools are installed on the end user systems/servers. The authorized list of software shall be installed on the end-user systems/server and shall be signed-off between SCRB and SI.

8.21 Change Request Management

The SI shall be responsible for making any changes/ enhancement in the System arising from changes in legislation or regulations or change in user requirements or any other factors as per

the Change Control Schedule, defined in Volume - III of this RFP anytime during the contract period.

1) In case of any changes required, the SI shall prepare a comprehensive report on the effort required to address the same and classify type of change i.e. Strategic, Tactical or Operational. SCRB shall scrutinize the report and evaluate commercials as per Industry Standards. SCRB shall have the right to rule or overrule the recommendations.

2) The SI shall adequately plan & deploy to carry out the change in the agreed timeline.

3) Any change to the application from the System Requirements Specification document agreed and signed-off by SCRB

4) The SI is expected to adopt the relevant procedures, protocols and standards of a mature Software Development Life Cycle (SDLC) including (but not limited to) the following for any enhancement / amendment done to the system (including the web-portal) during the course of the Project.

a) Feasibility study / Proposal for change
b) Requirement study
c) Design
d) Development
e) Unit and Integration testing
f) Performance testing
g) Regression testing
h) User acceptance testing
i) Training
j) Pilot launch
k) Stabilization
l) Go-live

5) The payment shall be finalized based on the effort estimation for the Change Request (indicative format given below)

Indicative approach for Change Request is given below:

SI shall follow the same process as development phase (through Development Environment, Test Environment, Staging Environment & Production Environment).

1) The SI shall share Change Request Note in advance with SCRB before proceeding with any activity in the system.

2) Change Request shall be raised based on type of request or issue criticality or effort.

3) The SI shall perform Impact analysis and share Impact analysis report before proceeding with Change request.

4) Change Request shall comply to the SDLC guidelines.

5) Necessary testing shall be done only in development and testing environment to determine whether the desired results have been achieved. If the change is not successful, remediation methods shall be used to determine what went wrong and to implement a backup plan to alleviate the issues that necessitated the change request.

a) Functional Testing: Ensuring that the application functionality as described by SCRB works adequately.

b) Performance Testing: Ensuring that the application meets expressed performance requirements.

c) Security Testing: Testing for exploitable application security weaknesses that undermine the application security or the security of the infrastructure.

d) Other activities undertaken during implementation phase before rollout and go-live of system.

6) Reproducibility, Transition management, Release management to be implemented for each Change Request.

7) After changes, a detailed test cases list needs to be defined and testing shall be conducted. The SI shall share test cases documents along with complete validation report (indicating the features implemented are working properly) with SCRB for further verifying the changes implemented. The SI shall share revised Reference documents related to changes.

8) Assist in detailed UAT through development and test environments before production deployment

9) Post activity, The SI shall also demonstrate the changes implemented to the SCRB Project Governance Office. The SCRB shall review the change & outcome. Only in the event of no degradation of the performance & control and no compromise in the test results, the changes shall be approved by SCRB.

10) In case of any discrepancy, the same shall be resolved within 1 business day.

8.21.1 Indicative Impact Analysis Checklist

The SI shall maintain an Impact analysis checklist for all the change request as indicated below to apprise SCRB on the impact and benefit change request will bring.

A.1. Impact Analysis Checklist
☐ Do any existing requirement in the baseline conflict with the proposed change?
☐ Do any other pending requirements changes conflict with the proposed change?
☐ What are the business or technical consequences of not making the change?
☐ What are the possible adverse side effects or other risks of making proposed change?
☐ Will the proposed change adversely affect performance requirements or other quality attributes
☐ Is the proposed change feasible within known technical constraints and current staff skills

☐ Will the proposed change place unacceptable demands on any computer resources required for the development, test, operating requirements?
☐ Must any tools be acquired to implement and test the change?
☐ How will the proposed change affect the sequence, dependencies, effort, or duration of any tasks currently in the project plan
☐ Will prototyping or other user input be required to verify the proposed change
☐ How much effort that has already been invested in the project will be lost if this change is accepted
☐ Will the proposed change cause an increase in product unit cost, such as by increasing third party product licensing fee
☐ Will the change effect procurement, warehousing, logistics, wholesale and retail sales, training or any other area
☐ Indicative activities need to perform while implementing Change request is captured in effort calculation table
☐ Identify any user interface changes, additions or deletions required
☐ Identify any changes, additions, deletions required in report, databases or files
☐ Identify the design components that must be created, modified, or deleted
☐ Identify the source code files that must be created, modified, or deleted
☐ Identify any changes required in built that must be created, modified, or deleted
☐ Identify existing unit, integration, system, and acceptance test cases that must be modified or deleted
☐ Estimated the number of new unit, integration, system and acceptance test cases that will be required
☐ Identify any help screens, training materials, or other user documentation that must be created or modified
☐ Identify any other application, libraries, or hardware component affected by the changes

☐ Identify any third-party software that must be purchases or licensed
☐ Identify any impact the proposed change will have on the project's software project management plan, quality assurance plan, configuration management plan, or other plans

8.21.2 Change Request Effort Calculation

SI shall calculate the effort required for implementing the change request in the below indicative format and submit along with Change Request format above to SCRB

Role of personnel	No. of hours	Description
		Update the SRS or requirements database
		Develop and evaluate a prototype
		Create new design components
		Modify existing design components
		Develop new user interface components
		Modify existing user interface components
		Develop new user documentation and help screens
		Modify existing user documentation and help screens
		Develop new source code
		Modify existing source code
		Purchase and Integrate third party software
		Modify build files
		Develop new unit and integration tests

Role of personnel	No. of hours	Description
		Modify existing unit and integration tests
		Perform unit and integration testing after implementation
		Write new system and acceptance test cases
		Modify existing system and acceptance test cases
		Modify automated test drivers
		Perform regression testing
		Develop new reports
		Modify existing reports
		Develop new database elements
		Modify existing database elements
		Develop new data files
		Modify existing data files
		Modify various project plans
		Update other documentation
		Update the requirement traceability matrix
		Reviewed modified work products
		Perform rework following reviews and testing
		Other additional tasks
		Total Effort

8.22 Adherence to Guidelines/ Standards

The complete System shall be designed following open standards, to the extent feasible and in line with overall system requirements set out in this RFP, in order to provide for good inter-operability with multiple platforms and avoid any technology or vendor lock-in.

8.22.1 Compliance with Industry Standards

The proposed System has to be based on and compliant with industry standards (their latest versions as on date) wherever applicable. This shall apply to all the aspects of System including but not limited to design, development, security, installation, and testing. Multiple standards that are capture below. However, the list below is just for reference and shall not be treated as exhaustive.

Standards:

1) Portal development W3C specifications.
2) Information access/transfer protocols SOAP, HTTP/HTTPS.
3) Photograph GIF, IMG, TIFF, JPEG (minimum resolution of 640 x 480 pixels).
4) Scanned documents PDF
5) Biometric framework BioAPI 2.0 (ISO/IEC 19784-1:2005).

Specifications:

1) Fingerprint scanning IAFIS specifications.
2) Digital signature RSA standards.
3) Document encryption PKCS specifications.
4) Information Security - ISO 27001 compliant.

5) Operational integrity & security management -ISO 17799 compliant.

6) IT Infrastructure management - ITIL / EITM specifications.

7) Service Management - ISO 20000 specifications.

8) Project Documentation - IEEE/ISO specifications for documentation.

9) CMMI complaint project management

The applications/portal to be developed shall have to adhere to the Guidelines/Policies of MeitY, GoI. Some of the important Guidelines/policies are tabulated below.

#	Policy/Guidelines	Link to the Policy/Guideline
1	Policy on Open Application Programming Interfaces (APIs) for Government of India	http://deity.gov.in/sites/upload_files/dit/files/Open_APIs_19May2015.pdf
2	Principles of e-Kranti	http://deity.gov.in/sites/upload_files/dit/files/DPR_on_e-Kranti.pdf
3	Software Development and Re-engineering Guidelines including centralized multi-tenant, integrable through open API and eGov APP store.	http://deity.gov.in/sites/upload_files/dit/files/Application_Development_Re-Engineering_Guidelines.pdf
4	National Cyber Security Policy	http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1)_0.pdf
5	Email Policy	http://deity.gov.in/content/email-policy
6	Software Asset Management	http://deity.gov.in/content/guidelines-software-asset-management-version-03
8	e-Governance guidelines	http://deity.gov.in/content/national-e-governance-plan
9	National IT Policy 2012	http://deity.gov.in/sites/upload_files/dit/files/National_20IT_20Policyt%20_20(1).pdf
10	Policies & Guidelines for State Data Centre	https://meity.gov.in/content/policy-guidelines-

	(SDC)	state-data-centre-sdc
11	DeitY GoI Central Initiatives for State :e-District, SP & SSDG, Digital-Locker, Digitize India, e-sign,), MSDG, PayGov India, National Payment Gateway platform, Mobile-Seva etc.	http://deity.gov.in/
12	Guidelines for Indian Government Websites	https://web.guidelines.gov.in

8.22.2 Third Party Audit for Compliance

SCRB reserves the right to get the System certified by Third Party Agency at any point of time during the implementation period. The agency shall perform audit of the developed System and check for compliance and adherence to these industry standards/ specifications, policies and guidelines.

The SI shall address all the non-compliances identified by the TPA. The TPA shall carryout a compliance audit and continue their process till the SI successfully resolves all the Non-conformance aspects of the application & the application is deemed ready for launch. Any non-conformance & vulnerability aspects identified by the TPA during this exercise shall be immediately mitigated & closed in 2 weeks' time. A comprehensive report needs to be submitted by SI on the closure of the identified non-compliance

Note: A sign-off on the Go-Live shall be provided by SCRB only after the completion of Full-Scale Assessment, Acceptance and certification by TPA Agency.

8.23 Project Deliverables, Documentation & Knowledge Management

The SI shall prepare, submit and get following documents/ deliverables signed off before moving to the next stage of the implementation/ deliverable milestone

1) The SI shall deploy a Knowledge repository tool for effectively managing the documents related to the project with features including but not limited to Version Control, Backup and Search feature. SI shall ensure submission of documents before the agreed timelines for the relevant milestone.

2) The SI shall prepare the formats/templates for each of the deliverables based upon industry standards and the same shall be reviewed and approved by SCRB prior to its use for deliverables. All documents are to be kept up to date during the course of the project.

3) The SI shall maintain a log of the internal review of all the deliverables submitted. Soft copy of logs shall be submitted to the Project Governance Office on fortnightly basis.

4) The documentation shall be in line with defined industry standards. The SI shall obtain sign-off on all the deliverables (documents and milestones), including design documents, standard operating procedures, security policy, procedures from the Department, etc. and shall make necessary changes as recommended before submitting the final version of the documents.

5) The payment shall be withheld if the SI has not submitted and received a signoff from SCRB on required deliverables and documentation of all previous and current milestone

6) The Sign-off / approval of the various documents by the SCRB or any of its nominated agencies does not however absolve the SI of his responsibility to meet the service levels and other requirements as specified in this RFP.

7) The below list is indicative, and SI shall submit all the documents/ deliverables covered in detail in various section in this volume of the RFP

Project Stage	Indicative Deliverables
Contract Stage	Performance Bank Guarantee (5 % of Total Contract value).
Study & Design Stage	1) Detailed Project Plan.

Project Stage	Indicative Deliverables
	2) Risk Management and Mitigation Plan. 3) Manpower Deployment Plan. 4) Gap analysis report on existing infrastructure, network and hardware recommendations. 5) Site Inspection Report on the reusability of existing site infrastructure 6) Part wise hardware procurement & Software deployment plan separately for pilot and full-scale rollout. 7) Make & model of OEM proposed. 8) IT Infrastructure Security plan. 9) IT Infrastructure deployment plan. 10) IT Infrastructure Management Policy and related SOPs in line with the ITIL (Information Technology Infrastructure Library) standards. 11) Storage management policy. 12) Helpdesk / Technical support plan. 13) Business Continuity and Disaster Recovery plan including backup plan. 14) Information Systems Security Policy and related procedures in line with the ISO27001 standard. 15) Data migration plan. 16) Manpower deployment plan. 17) Exit Management Plan including plan for Knowledge Transfer.
Application Design & Development and Customization	1) Technical Architecture Document (Application, Network, and Security). 2) Database Architecture Report.

Project Stage	Indicative Deliverables
	3) Software Implementation Plan Document. 4) Detailed Design Plan. 5) Developed and customized application including web-portal for UAT. 6) Application Test plan, Test cases, Test assumptions, Test coverage and boundaries. 7) Test documents. 8) Test reports until zero defects. 9) Application User manual and deployment document. 10) Web APIs. 11) Software installation guide. 12) Application Technical manual, drivers, installable etc. 13) System maintenance manuals. 14) Application Source code.
Helpdesk, Business Continuity, Disaster Recovery, Database Migration, Third Party Integration, SMS, Email and Payment gateway Integration	1) Detailed plan on Helpdesk, Business continuity, Disaster recovery, Data Migration, Integration with in-house and Third party system. 2) Capacity Building and Change Management plan. 3) Completion report on 1) Database migration and validation of databases. 2) Integration with SCRB and other department portals, Third party systems. 3) Report exchange of data and communication with in-house,

Project Stage	Indicative Deliverables
	external and other Third-party system in scope. 4) Maintain integration log for all Third party integration, in house legacy databases and portals. 5) Helpdesk operations & maintenance.
Hardware & Software License Procurement & Commissioning- Pilot	1) SCRB approved Pilot sites. 2) Final BoM (Bill of Material). 3) Configuration files of the infrastructure. 4) PAT Report on IT Infrastructure (DC, DR, Pilot Locations). 5) Documentation on IT Infrastructure and Software license procured and deployed. 6) Infrastructure Deployment / Commissioning Report for Police Stations, SCRB Offices, Acceptance report form SCRB. 7) Readiness of DC, DR before pilot deployment. 8) Completion report on EMS & Remote Device Management setup. 9) Readiness report for IT infra monitoring. 10) Knowledge repository tool readiness report. 11) Business Continuity plan and Disaster Recovery plan. 12) Information security management procedures.
Training Plan Preparation	Detailed Training plan comprising 1) SCRB approved location wise participant name and count for pilot training. 2) Training Materials, User Manual. 3) IT Infrastructure System Operation Manual. 4) IT Infrastructure Maintenance and Troubleshooting Manual.

Project Stage	Indicative Deliverables
	5) End User Manual for SCRB Applications – Final. 6) Sign off from SCRB on identified Training locations, Training assessment approach.
UAT	1) Application Test plans, Test cases, Test assumptions, Test coverage and boundaries. 2) Application User manual & standard operating procedures. 3) Software installation guide. 4) System maintenance manuals. 5) UAT report. 6) UAT Signoff report 7) Completion report on Site preparation & Application.
Training- Pilot Users	1) Change Management workshop completion Report. 2) Training Completion Report. 3) Training Assessment Results. 4) Training Feedback and plan for implementation of changes.
Deployment Phase- Pilot	1) System change over strategy for and transition to new system from existing system. 2) Pilot deployment plan. 3) Pilot rollout report including. a) Site preparation and infrastructure deployment / commissioning report for pilot sites. b) Data Migration report for pilot. c) Helpdesk operationalization report. d) Performance Assessment report for Pilot site.

Project Stage	Indicative Deliverables
	e) Pilot deployment completion report.
Audit- Pilot Rollout	Documents required by TPA for audit purpose.
Application Stabilization & Pilot Rollout Acceptance	1) Report on amendments / enhancements / modifications made based on inputs of Department's / Third Party's Acceptance Testing for pilot rollout. 2) Application Stabilization report. 3) Report on completion of changes in the software. 4) Obtain Pilot Acceptance report from Department.
Hardware & Software License Procurement & Commissioning- Full Scale	1) Final BoM 2) Documentation on IT Infrastructure and Software license procured and deployed. 3) Infrastructure Deployment / Commissioning Report - Acceptance report from SCRB. 4) Factory Acceptance Test (FAT) Report on IT Infrastructure 5) Warranty Certificate. 6) Site Delivery Plan showing exact coordinates of the hardware.
Training Plan Preparation for Full Scale	1) Training plan and schedule. 2) SCRB approved location wise participant name and count for full-scale training. 3) Approval of Training location and Facility. 4) Revised training content as per Pilot feedback (if applicable).
Training- Full Scale	1) Change Management workshop completion Report. 2) Training Completion Report.

Project Stage	Indicative Deliverables
	3) Overview Training Completion report. 4) Training material. 5) Training Materials, System User Manual. 6) IT Infrastructure System Operation Manual. 7) IT Infrastructure Maintenance and Troubleshooting Manual. 8) End User Manual for complete system – Final.
Audit	Documents required by TPA for audit purpose.
Full Scale Rollout	1) Rollout across State ready for acceptance by Department. 2) Report on amendments / enhancements / modifications made based on inputs of Department's Pilot Acceptance Testing. 3) Site preparation and infrastructure deployment report across all locations. 4) Manpower deployment report. 5) Data Migration report for pilot. 6) Data Migration report including Test plans and Test results for Data Migration. 7) Helpdesk operationalization report. 8) Training Delivery report. 9) Performance Assessment report for State-wide-rollout.
Acceptance of State-wide Rollout and Go-live	1) Report on rollout for full scale. 2) Report on amendments / enhancements / modifications made based on inputs of Department's / Third Party's Acceptance Testing for full scale rollout. 3) Final acceptance of System.

Project Stage	Indicative Deliverables
	4) Obtain Go-live Acceptance Report from Department. 5) Training Completion Report. 6) Final Report on the Access rights and control structure. 7) Application Configuration/ customization report –Final. 8) Manpower Deployment Report. 9) Final Report on the Access rights and control structure. 10) IT Infrastructure Integration & Connectivity Report. 11) Performance Assessment report for Data Centre, DR Site and all department office locations. 12) Business Continuity and Disaster Recovery report.
Operations & Maintenance Phase	1) Detailed plan for monitoring of SLAs and performance of the overall system. 2) Fortnightly Progress Report on Project including SLA Monitoring Report and Exception Report. 3) Details on all the issues logged.
Project Closure	1) Project Closure report. 2) Project documents and other artefacts. 3) Document of design standard operating procedures to manage system. 4) Provide the Source Code (all version) related to the Application development / Integration as per the license Agreement. 5) Handover configuration information & System documentation 6) Hardware related documents. 7) SDK for all major software languages such as Android/ Java, .Net, C/C+. SDK shall be compatible with all major OS such as windows,

Project Stage	Indicative Deliverables
	android, Linux etc.

All documents shall be kept up to date during the course of the project. The SI shall maintain a log of the internal review of all the deliverables submitted. Soft copy of logs shall be submitted to SCRB on regular basis.

Confidentiality of Information

The SI need to deploy strict data and information & confidentiality practices for project related and SCRB internal data ensuring all records, documents, data, reports, presentations, software and infrastructure related information are restricted in movement. The SI need to plan for proper handover in case of any of the project member is no longer associated with the project ensuring outgoing resources are not carrying project and SCRB related data in any form- Physical or Digital.

8.24 Acceptance Procedure for Deliverables

Deliverables shall be reviewed and accepted in accordance with the following procedure:

1) Notification of readiness of the deliverable shall be given by e-mail by the SI

2) Soft copy (by e-mail) and two (2) printed drafts of all deliverables shall be submitted to SCRB. Source code however need not be submitted in hard copy.

3) The SCRB will review the deliverables and either accept the deliverable or provide feedback on changes to be done in writing within a reasonable period of time (2-3 weeks).

4) The SI shall make the appropriate revisions and shall resubmit the updated final version to the SCRB for their verification and feedback/acceptance.

5) The SI shall strive to submit the deliverables in parts for getting continuous feedback on the deliverables. The SI shall also engage with the SCRB on a continuous basis through meetings

(weekly till 6 months after Go-live and fortnightly after this period) and periodic workshops to ensure that progress may be reviewed, and feedback provided from time-to-time.

Please note that the timelines indicated in this Implementation schedule are timelines for submission of final deliverables. The SI plan to submit the draft versions of deliverables before the timelines indicated above to allow reasonable time for review and acceptance by the time indicated above.

8.25 Exit Management

Knowledge Transfer is an integral part of the scope of work of the System Integrator. This shall be done even in case the Contract with the System Integrator ends or is terminated before the planned timelines.

The Exit Management Period starts (1) 6 months before the Contract comes to an end or (2) In case of earlier termination of Contract, on the date of service of termination orders to the SI. The Exit Management Period ends on the date agreed upon by SCRB or six months after the beginning of the Exit Management Period, whichever is earlier.

The SCRB would eventually decide on one of the following options for managing the Project beyond the Contract period:

a) Replace – Appoint a different agency for undertaking Project maintenance beyond the Contract period through a fresh tender

b) Transfer - The Selected System Integrator will transfer the Project including all assets to the Department and the Department will manage the operations on its own.

c) Extend- In the eventuality that no such alternate arrangements are in place for managing the Project at the end of the Contract period, the System Integrator shall be required to continue delivering services as required under this Project, at the same terms and conditions, even beyond the Contract period (such period not exceeding 1 year) till alternate arrangement is done by the SCRB to manage the operations. (The decision to

extend the Contract with the System Integrator (if applicable) shall be communicated to the System Integrator before the expiry of the Contract.)

Creation and Submission of Initial Exit Management Plan:

1) This Exit Management plan shall be furnished in writing to SCRB or its nominated agency within 90 days from the date of contract signing.

2) The SI shall re-draft the Exit Management Plan annually thereafter to ensure that it is kept relevant and up to date.

Commencing of Exit Management:

The System Integrator during exit shall provide SCRB with a recommended and updated exit management plan, which shall deal with following minimum aspects of exit management in relation to the Project Implementation and the Operation & Management SLA:

1) A detailed program of the transfer process that could be used in conjunction with the replacement of SI 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;

2) The Exit Management Plan shall be presented by the SI and approved by the SCRB.

During the Exit Management Period:

1) The SI during exit shall use its best efforts to deliver the Services. Payments during the Exit Management Period shall be made in accordance with the Payment Schedule.

2) The SI's team during the exit phase shall continue to perform all their obligations and responsibilities, as per the SI's proposal under the RFP, in order to execute an effective transition and to maintain business continuity of SCRB.

3) The SI while exit would be required to do knowledge transfer of the operations & responsibilities to SCRB or its nominated agency or New SI.

4) The SI during exit shall be required to provide necessary handholding and transition support to SCRB staff or its nominated agency or New SI. The handholding support shall include but not be limited to, conducting detailed walkthrough and demonstrations for the IT Infrastructure, handing over all relevant documentation, addressing the queries/clarifications of the new agency with respect to the working / performance levels of the infrastructure, conducting Knowledge Transfer sessions etc.

5) The SI during exit shall permit SCRB or its nominated agency or New SI to have reasonable access to its staff and facilities as reasonably required to understand the methods of delivery of the services employed by the SI and to obtain appropriate knowledge transfer.

6) The SI during exit shall handover source code of application and hardware configuration to SCRB or its nominated agency or New SI.

7) During the exit/transition management process, outgoing SI shall ensure that the SCRB application is handed over in a complete operational condition to the satisfaction of the SCRB.

8) In case the SI during exit is unable to deliver any of the above responsibilities, SCRB may levy penalty.

9) It is to be noted that throughout the contract period, the SI shall ensure that all the documentation including policies, procedures, asset registers, configuration documents etc. are kept up to date and all such documentation is handed over to the SCRB during the exit management process.

Transfer of Project Assets:

1) Before the expiry of the Exit Management Period, all Project Assets including the hardware, software, system software documentation and any other infrastructure shall be updated and cured of all defects and deficiencies as necessary so that the Project is compliant with the specifications and standards set forth in the Agreement, RFP, and any other amendments made during the Contract Period.

2) The SI during exit shall provide SCRB with a complete and up to date list of the Assets to be transferred to the SCRB within 30 days of start of Exit Management Period.

3) Before the expiry of the exit management period, the SI shall deliver relevant records and reports pertaining to the Project and/or SCRB and its design, implementation, operation, and maintenance including all operation and maintenance records and manuals pertaining thereto and complete as on the divestment date.

4) The ownership of the assets (including soft and hard components existing and procured through this tender) at any point of time during the project shall rest with SCRB. The outgoing SI shall ensure the same during exit.

5) The SI while exit shall comply with all other requirements as may be prescribed under applicable laws to complete the divestment and assignment of all the rights, title and interest of the SI in this Project free from all encumbrances absolutely and free of any charge or tax to SCRB or its nominated agencies or the new SI as the case may be.

Confidential Information, Security and Data:

During the exit management period, the outgoing SI shall provide following to SCRB or its nominated agency or new SI:

1) Information relating to the current services rendered and performance data relating to the performance of OEMs in relation to the services.

2) Documentation relating to OEMs.

3) Documents such as Approved SRS, Architecture Document, Use Cases, Sequence Diagrams, Class Diagrams, User Manuals, etc.

4) Details specific to application development environment such as OS (Version), Language used (Examples: HTML and XML and their derivatives XSL and its derivatives, Java/ C#/ AJAX/ JavaScript/ Servlets/ JSP/ JavaBean/ EJB/ Perl/ VBScript), Type of App Server / Web Server and the corresponding software used, IDE and its version, what type of Version Control is used, etc.)

5) Production server configurations for code development and deployment.

6) Access to version control repository of the developed web application code.

7) List all the code development tools, and their versions used for the application code development.

8) List all the frameworks and their versions used for the application code development (Examples: Struts, Spring, Hibernate etc.).

9) List all the third-party products used for the application development.

10) List all the utility functionalities provided by the application and the technologies used to implement those functionalities.

a. Does the application generate printouts? What is the format of those printouts? PDF? MS Excel? MS Word? And/or others?

b. Does the application use single sign-on?

c. What are the technologies used to impose application security (e.g. authentication and authorization)?

d. Does the application provide e-mail functionality? Is Java Mail used to implement the e-mail functionality?

e. Does the application generate reports? What technologies are used? Report? Crystal Report? Or some other technologies?

11) Schema and DDL of the database tables used for the application development.

12) Source code for all the stored procedures used for the application development.

13) List the data persistence and retrieval languages used for the application development (Examples: SQL, PL/SQL, others, etc.)

14) List all the business rules implemented in the application.

15) Document the business rules engines used to implement the business rules in the application.

16) Provide all the images and watermarks used in the application.

17) List all the code testing tools used for unit test, integration test, and module test of the application (Examples: Junit, Easy Mock, etc.).

18) Documentation relating to Project's Intellectual Property Rights.

19) All current and updated data as is reasonably required for purposes of SCRB or its nominated agencies, or its Incoming SI (as the case may be) transitioning the services.

20) All other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable SCRB or its nominated agencies, or its Incoming SI to carry out due diligence in order to transition the provision of the Services to SCRB or its nominated agencies, or its Replacement SI (as the case may be).

21) Before the expiry of the exit management period, the outgoing SI shall deliver to the SCRB or its nominated agency all the relevant updated materials and shall not retain any copies thereof, except that the SI shall be permitted to retain one copy of such materials for archival purposes only.

22) Before the expiry of the exit management period, unless otherwise provided under the MSA, SCRB shall deliver to the outgoing SI all forms of confidential information related to SI, which is in the possession or control of SCRB senior officers or its users.

9. Timelines and Schedule

9.1 Implementation Schedule

The below chart comprises of table giving the breakup of SI deliverables and timelines:

9.1.1 Hardware Infrastructure Implementation and O & M Schedule

Legends:

M = Month

0.5 = 0.5 Month

1 = 1 Month

T = Issuance of the Work Order for Phase - 1

T1 = Issuance of the Work Order for Phase – 2

T2 = Issuance of the Work Order for Phase – 3

Phase 1:

Key Milestones	Months		M0	M1	M2	M3	M4	M5	M6
Issuance of Work Order	**T**	**0**							
Supply of hardware/ server to individual locations and Submission of sealed and signed delivery challans	**T + 4**	**4**							
Commissioning of equipment and Submission of equipment inspection report	**T + 5**	**1**							
Configuration of Monitoring Tool (existing CA EMS or new EMS) and mapping details of each hardware to asset ids, location									
Submission of Site Commissioning Report	**T +6**	**1**							

Phase 2:

Key Milestones	Months		M0	M1	M2
Issuance of Work Order	**T1**	**0**			

Supply of hardware/ server to individual locations and Submission of sealed and signed delivery challans	**T1 + 2**	**2**			
Commissioning of equipment and Submission of equipment inspection report					
Configuration of Monitoring Tool and mapping details of each hardware to asset ids, location					
Submission of Site Commissioning Report					

Phase 3:

Key Milestones	Months		M0	M1	M2	M3	M4	M5
Issuance of Work Order	**T2**	**0**						
Supply of hardware/ server to individual locations and Submission of sealed and signed delivery challans	**T2 + 3**	**3**						
Commissioning of equipment and Submission of equipment inspection report	**T2 + 4**	**1**						
Configuration of Monitoring Tool and mapping details of each hardware to asset ids, location								
Submission of Site Commissioning Report	**T2 +5**	**1**						

9.1.2 Software Implementation and O & M Schedule

Key Milestone	Month(s)	Duration	M0	M0.5	M1	M1.5	M2	M2.5	M3	M3.5	M4	M4.5	M5	M5.5	M6	M6.5	M7	M9–M68
Signing of Agreement	T	0																
Acceptance of Architecture & System Requirement Study (SRS)	T+0.5	0.5																
Completion of Application Development & Testing by System Integrator	T+3.5	3																
Completion of User Acceptance Testing (UAT) by SCRB	T+4	0.5																
SI to make software compliant as per security audit as per the VAPT clause (Section 8.14.1)	T+4.5	0.5																
Hosting of Application Software in TNSDC servers by SI	T+5	0.5																
Completion of Pilot Rollout & Training for users in Pilot locations	T+5	0																
Application Stabilization & Acceptance of Pilot Rollout by SCRB	T+5.5	0.5																
Complete Training for all Users	T+6	0.5																
SI to make software compliant as per independent TPA audit as per TPA	T+6	0																

clause (Section 8.14.2)																		
State-wide Rollout of Application by SI	**T+6.5**	**0.5**																
Acceptance of Go-Live by SCRB	**T+7**	**0.5**																
Application Operations & Maintenance (O&M)	**T+8 to T+68**	**60**																

9.2 Payment Schedule

The below table comprises of the details of payment schedule against deliverables:

9.2.1 Hardware Payment Schedule

1. Payment Schedule and Milestone for Implementation Phase:

#	Payment Milestone for the Implementation Phase	Phase 1		Phase 2		Phase 3	
		Timelines	Payment (as a % of Work Order Value)	Timelines	Payment (as a % of Work Order Value)	Timelines	Payment (as a % of Work Order Value)
1	Issuance of Work Order	T	-	T1	-	T2	-
2	Supply of hardware to individual locations and submission of sealed and signed delivery challans	T + 4 months	40%	T1 + 2 month	-	T2 + 3 months	40%
3	Commissioning of equipment and submission of equipment inspection report • Fixing of Asset Tags and computer cover at all locations • Configuration of Monitoring Tool (existing CA EMS or new EMS) and mapping details of each hardware to asset ids, location and employee	T + 5 months	30%	T1 + 2 month	-	T2 + 4 months	30%

4	Submission of site commissioning report	T + 6 months	30%	T1 + 2 month	100%	T2 + 5 months	30%

2. Payment Schedule and Milestone for O & M Phase:

SNo.	Payment Milestone for the Implementation Phase	Timelines	Payment
1	Submission of SLA report	Quarterly (from date of completion of equipment commissioning)	25% of annual O & M payment of that year payment after deduction of SLA penalties paid every quarter

9.2.2 Software Payment Schedule

1. Payment Schedule and Milestone for Implementation Phase:

SNo.	Key Milestones	Timelines (in Months)	% Payment (of Software Capex Value)
1	Signing of Agreement	T	
2	Acceptance of Architecture & System Requirement Study (SRS)	T + 0.5 Month	
3	Completion of Application Development & Testing by System Integrator	T + 3.5 Months	5%
4	Completion of User Acceptance Testing (UAT) by SCRB	T + 4 Months	15%
5	SI to make software compliant as per security audit as per the VAPT clause (Section 8.14.1)	T + 4.5 Months	
6	Hosting of Application Software in TNSDC servers by SI	T + 5 Months	

7	Completion of Pilot Rollout & Training for users in Pilot locations	T + 5 Months	
8	Application Stabilization & Acceptance of Pilot Rollout by SCRB	T + 5.5 Months	25%
9	Complete Training for all Users	T + 6 Months	
10	SI to make software compliant as per independent TPA audit as per TPA clause (Section 8.14.2)	T + 6 Months	
11	State-wide Rollout of Application by SI	T + 6.5 Months	
12	Acceptance of Go-Live by SCRB	T + 7 Months	30%

Note:

75 % of Software Capex Value will be paid during implementation phase and the remaining 25% of Software Capex Value will be paid equally during the O&M phase at 5% per year.

2. Payment Schedule and Milestone for O & M Phase:

SNo.	Key Milestones	Timelines (in Months)	% Payment
1	Application Operations & Maintenance (O&M)	T + 8 Months to T + 68 Months	25% of annual O & M payment of that year payment post Go – Live after deduction of SLA penalties paid every quarter

10. SCRB Project Governance Office

The SCRB Project Governance Office shall constitute:

i. Project Steering Committee: The Steering Committee is the Senior Management Committee with designated experts who can provides a tactical and strategic direction for the overall project. The committee shall be the final authority on all matters regarding project implementation in SCRB.

ii. Strategic Project Management Office: The Strategic Project Management Office team shall be responsible for ensuring the overall effectiveness of the project implementation and will be the central repository for all status reporting to the Steering Committee. In order to achieve consistency and accuracy across the project, all initiatives/sub-projects shall comply with the project tracking and control requirements defined by the Project Management Office. The Project Management office shall be responsible for establishing the process, technical, operation and control standards, applying these to project, providing tools to project teams for project control and tracking, and collecting and collating project controls and status throughout the life of project.

The SI shall ensure the required approvals are obtained from the SCRB Project Governance Office wherever required, as mentioned in this RFP. The SI shall align with the Project Governance Office for successful & timely completion of project milestones.

The major objectives & responsibilities of the SCRB Project governance office is listed below:

Team	Roles and Responsibilities
Project Steering Committee	1) Set strategic direction for project implementation. 2) Monitor delivery of a project milestones as per scope and implementation plan & monitor spend against budgets. 3) Manage dependencies among resources and resolve significant resource

	conflicts. 4) Ensure that all significant project initiatives are driven to completion within time and budget and to scope. 5) Ensure that the project strategy is updated on a regular basis in alignment with the organization objectives as well as approving IT policies/standards and the IT business plan. 6) Responsible for reviewing project SLAs. 7) Address scope variations and benefits realization of projects. 8) Approve major project deviations, timeline and payment related decisions. 9) Take key decisions & resolve major issues.
Strategic Program Management Office	1) Assist in issue resolution and manage project interdependencies 2) Oversee ongoing expenditure of project funds. 3) Administer new business cases/Change Requests. 4) Review SLA performance considering defined key performance indicators and report this performance to the business and to IT. 5) Resolve disputes early in co-operation with the legal department.

11. Stakeholder Responsibility Matrix (RACI Matrix)

The roles of the stakeholders shall change over a period as the project will evolve from design to implementation and enter the operations phase. With this background, stakeholders' responsibilities, illustrative organizational structure for the design & implementation phase, operational phase is given below:

Below mentioned Table summarizes the roles and responsibilities of stakeholders involved in the project. The RACI (R – Responsibility, A- Accountability, C- Consulted, I – Informed) method is followed;

#	Activity	SCRB	PMU	Onboarded SI	TPA	Outgoing SI	Integration – External parties
1.	Project Inception Meeting	I	C	R, A			
2.	Signing of Contract with SI	R		R, A			
3.	System Requirement Study (SRS)	I	C	R, A			
4.	Review and approval of System architecture & SRS	C, I	C	R,A			
5.	Project Documentation - HLD, LLD, SDD etc.	I	C	R, A			
6.	Application Design and Development Phase	C, I	C, I	R, A			
7.	Setting up the testing facility with Hardware and manpower	C, I	C	R, A			
8.	Preparation of comprehensive Test-Cases for applications	I	C, I	R, A			
9.	Module-wise Testing (Unit, Performance,	I	C, I	R, A			

#	Activity	SCRB	PMU	Onboarded SI	TPA	Outgoing SI	Integration – External parties
	Integration, system, Integrity, Security testing)						
10	Integration Testing for Workflow Application	I	C, I	R, A			
11	Software Commissioning- Pilot	I	C, I	R, A			
12	Infrastructure User Acceptance Testing- All location of Pilot	R, I	C, I	R, A			
13	Training for Pilot Users	A	I	R, A			
14	Application Stabilization	I	I	R, A			
15	EMS Set Up & Operation	I	I	R, A			
16	Legacy Data Migration and Validation	C, I	C, I	R, A		R, A	
17	Software Rollout - Full Scale	I	I	R, A			
18	Training- Full Scale	R	I	R, A			
19	Appointment of Third-Party Agency (TPA) for Audit	R, A	C	I	I		

#	Activity	SCRB	PMU	Onboarded SI	TPA	Outgoing SI	Integration – External parties
20	Security & Performance Audit of the Application	I	C	A	R, A		
21	Modifications/rectification of the application after third party Security & Performance audit	I	I	R, A	I		
22	Modifications/ Rectification of the application after third party audit	I	C	R, A	I		
23	Third party API permissions	R, A	C, I	I			R, A
24	Go Live	R	C	R, A			
25	O&M	I	C	R, A			
26	Monitoring of SLA adherence during O&M period	I	I	R, A			
27	Knowledge Management	C, I	I	R, A			
28	Project Closure & Exit Management	R	C	R, A			

12. Resource Requirement

Key Resource Requirement

i. Resources proposed on the project must actually be deployed on the assignment. No changes in the resources will be allowed during the contract without explicit written permission of SCRB. Minimum qualifications for each resource are mentioned below, which shall be used for evaluation. However, SI will also be required to provide the resources to support the activities under this project and to meet the desired SLA.

ii. The SI is required to station the key resources at SCRB for the entire duration of the contract.

iii. In case of non-availability of proposed resource at point of time during the contract, the SI is required to provide an alternate resource with at least the requirements proposed in the RFP or higher.

The minimum resource requirement for this tender is as follows, however this is minimum requirement and hence SIs are free to provide additional resources if deemed necessary;

SNo.	Resource Description	No. of Resources	Educational Qualification	Experience	Role
1	Project Manager	1	a. B. E / B. Tech / M. Tech / MBA / MCA b. PMP / Prince 2 Certification	a. Overall, 10 + years of Experience b. 8+ years of experience in implementing large scale government projects in India c. Experience in at least 2 State / Central Government Project Implementation	**Role:** Project Management To be deployed full-time for the entire duration of the contract.
2	Technical Architect & Team Lead- Application Development & Support	1	a. BE/B.Tech/MCA/ M.Tech	8 years or more in design / development / application / solution architecture, development of IT applications for large scale projects	**Role:** Application Development and Management. **Duration:** To be deployed full-time for the entire duration of the contract.
3	Team Lead – Data Center	1	a. B. Tech / MCA with relevant certifications. b. ITIL Certified c. Linux Certification d. Good Communication Skills	a. 5+ years of relevant experience. b. Adequate knowledge and experience in VM ware c. Experience in Windows Servers d. Team Management / Stakeholder Management experience	**Role:** a. Data Center & Disaster Recovery Center Management b. DC Shift Management c. SPOC for DC/DR **Duration:**

					To be deployed full-time for the entire duration of the contract.
4	Team Lead – Service Desk Management	1	a. B. Tech /MBA / MCA with relevant certifications. b. ITIL Certified c. Good Communication Skills d. Proficiency in local language (Tamil) is mandatory – Read, Write & Speak	a. 5+ years of relevant work experience. b. Team Management & Stakeholder Management Experience. c. Adequate knowledge & Experience in handling Incident Management Tools	**Role:** a. Service Desk Management b. Service Desk Shift Management c. SPOC for Service Desk **Duration:** To be deployed full-time for the entire duration of the contract.

5	Data Center - Level 2 Resources	5	a. B. E / B. Tech / M.Sc. (IT/CS) b. Certification in Linux / Networking	a. Min 2-3 years of relevant experience. b. Experience in Linux / Windows Servers c. Adequate knowledge in Networking	**Role:** To be deployed in shifts - 1 resource per shift. DC to be operated from State Data Center premise 24x7 in 3 shifts **Duration:** To be deployed in shifts full-time for the entire duration of the contract.
6	Service Desk – Level 1 Resources	6	a. Any Graduation / Diploma b. Good Communication and call handling Skills c. Proficiency in local language (Tamil) is mandatory. Read/ Write & Speak	a. Min 1 year of relevant experience b. MIS and Reporting c. Adequate knowledge on Ticketing and MIS tools.	**Role:** To be deployed in shifts – 2 resources per shift. General shift timings to have 1 extra resources. Service desk to be operated from SCRB premise 16x7 in 2 shifts To be deployed full-time for the entire duration of the contract

7	Zonal Leads	5	a. Any Graduation / Diploma b. Good Communication and call handling Skills c. Proficiency in local language (Tamil) is a must. Read/ Write & Speak	Any Graduation with Min 2 year of experience in IT hardware Management & trouble shooting	**Role:** To be deployed in the respective zones– 4 zones (North, West, South & Central and Chennai) To coordinate with Zonal Inspectors & Detachments **Duration:** To be deployed full-time during the implementation phase of hardware items

12.1 Full Time Obligation

The SI shall not make any changes to the composition of the Key Personnel and not require or request any member of the Key Personnel to cease or reduce his or her involvement in the provision of the Services during the defined term of the engagement unless that person resigns, is terminated for cause, is long-term disabled, is on permitted mandatory leave under Applicable Law or retires. In any such case, the SCRB's prior written consent would be mandatory.

12.2 Evaluations

The SI shall carry out an evaluation of the performance of each member of the Key Personnel in connection with the Services at least once in each Contract Year. The SI shall provide reasonable written notice to SCRB of the date of each evaluation of each member of the Key Personnel. SCRB shall be entitled to provide inputs to the SI for each such evaluation. The SI shall promptly provide the results of each evaluation to SCRB, subject to Applicable Law.

12.3 Replacements

In case any proposed resource resigns, then the SI has to inform SCRB within one week of such resignation. The SI shall promptly initiate a search for a replacement to ensure that the role of any member of the Key Personnel is not vacant at any point in time during the contract period, subject to reasonable extensions requested by SI to SCRB. Before assigning any replacement member of the Key Personnel to the provision of the Services, SI shall provide SCRB with:

i. A resume, curriculum vitae and any other information about the candidate that is reasonably requested by SCRB; and
ii. An opportunity to interview the candidate.

The SI has to provide replacement resource of equal or better qualification and experience as per the requirements of this RFP

13. Annexure 1 – Web Application-CCTNS 2.0

Application Design Principles

Further to the envisaged functional requirements described in Software Scope of Work detailed in Section 7, the SI should ensure the new web-based application adheres to the following design principles:

Admin user privileges: The current CIPRUS application does not have any automated workflow for data correction and validation. All such requisitions are manually sent, reviewed and corrected. There is no admin user and all changes are done by the software developer. The new web application will have an admin user with certain rights and privileges. The same has been explained in detail in Section 7.3.7. All aspects under the purview of the admin user will be a part of the core development scope of work. Some of the illustrative tasks that the admin user should be able to perform are:

1. Should be able to build new or modify existing case event data forms
2. Should be able to build new and generate static and dynamic reports
3. Should be able to review data change requests, or forward requests to senior officers through the workflow system
4. Should be able to validate and approve data or other minor system changes
5. Should be able to build and generate queries, dashboard, search criteria
6. Should be able to monitor usage
7. Should be able to trigger alerts, emails or invoke chats. The admin should be able to interact with users through the communication module

Usage of the application: There is no provision in the current CIPRUS to track usage. Only login and logout times and user login IDs are maintained. There is no audit trail and logs of detailed user sessions. The SI shall design and develop the new web application in such a manner that all important usage details are captured. A detailed list of usage metrics have been explained in Section 7.3.11. The design objective is to track and measure effective usage of the platform.

Data capture and integrity: The current CIPRUS application does not have any validation mechanism for authenticity of the data captured. The SI should design the system based on the principle that erroneous data entry can be prevented as much as possible. For example, When a photograph of an accused is uploaded by the user, it should comply to a minimum resolution. After accused Aadhaar is provided, accused name should be automatically populated from the Aadhaar database so that typing errors, or any mismatch can be avoided.

The objective of the system shall be to provide multifarious options to the user to capture information under all situations such as network connectivity issues/ application not working/ mobile device not working. For instance, in case of network connectivity issues, the user should be able to login to static pages in the application and enter information in offline mode. The information should be saved in the backend as draft. As soon as the connectivity resumes, the system should push the data to the server and sync it with the live application. In case of Investigating officer mobile device not working, the data could be captured in alternate device and uploaded later into application through I.O login/ once his device is functional, whichever is earliest. The system should have provision to capture this data while recording details of person, time of data capture at source and have necessary approval mechanism for the such deviations.

Database classification The database design and architecture is very important for the flexibility and hybrid nature of the envisaged system. The classification of databases will help design the database relationships and understand the usage of the databases.

The master database is the crime cases database. The crime cases database can be sub-divided into person related, property related and case related databases:

1. The person related databases consists of physical identifier DBs, personal identifier DBs, and personality linked DBs. The person related DBs can be used for crime prevention watch, crime detection and antecedents' verification using person and MO (modus operandi), search and crime case supervision using case dairy documents. The searches can also be used for police verification services offered to citizens.
2. The property related databases consists of properties with and without unique identifier DBs. This DB can be used for property search.

3. The case database consists of place, time and general attribute details.
4. The crime database is used for crime analytics tools and crime statistics in order to devise strategies for crime prevention and control.

Completeness of database: The core principle behind the new web application is to have an end to end complete database. Currently, the information required for document generation is only entered by the users, and other non-document generating information even though critical is optional. Hence, users skip to enter them. This hampers crime detection. The objective of the new application will be to capture all the data required for crime detection/prevention, analytics and supervisory purpose.

14. Annexure 2 – Non-Functional Requirements

The below Non-Functional Requirements are indicative requirements for complete System. Based on these requirements, the system shall be conceptualized and designed. The SI shall ensure adherence to the below listed Non-Functional Requirements before implementation of the system:

14.1 Architecture Requirement

S.No.	Requirements
1.	The System shall be envisioned, designed, developed, implemented, deployed and maintained to comply with the security, scalability, reliability, business continuity, flexibility, modularity and interoperability requirements
2.	The System shall be highly scalable and capable of delivering performance even when the number of concurrent users or the transaction volume increases
3.	The System shall be flexible for customization to accommodate any new requirements via change requests in the form of add-ons, patch upgrades etc.

4.	The System shall have real time data update across modules/ sub modules and shall be accessible to all users immediately

14.2 General Requirement for Application

S.No.	Requirements
1.	The System shall be highly scalable and capable of delivering high performance as & when transaction volumes/concurrent users/total users increases without compromising on the response time. The Proposed Webservers shall be placed in High Availability mode.
2.	The IT Infrastructure shall have ability to withstand all single point of failure by providing clustering features
3.	The IT Infrastructure shall support the use of fault tolerant multiprocessor architecture & cluster processing
4.	The IT Infrastructure shall support auto-switching to available server in case of server Failure/ Overload
5.	The IT Infrastructure shall support distributed processing
6.	The IT Infrastructure shall support load balancing
7.	In DC/ DR it shall be possible to configure data replication synchronously or asynchronously The database shall support continuous replication in synchronous and asynchronous mode
8.	The System proposed shall include servers with latest CPU architecture offered by the hardware provider
9.	The IT infrastructure shall support all operating systems
10.	The IT infrastructure in the proposed solution shall be scalable to support architecture

S.No.	Requirements
	development and upgrade needs during and post implementation.
11.	The staging/ pre-production environment in the proposed System shall be needed for conducting tests and trainings during pre and post implementation
12.	The System shall support N-tier architecture (with minimum 3-tier architecture)
13.	The application shall be Web based and built on enterprise application platform
14.	The System shall require minimum installation
15.	The application shall have flexibility for customization based on SCRB's requirement
16.	The application shall be developed based on the SCRB approved FRS, SRS, LLD, HLD, Architecture documents
17.	The System shall run on native desktop browser with additional plug in's that shall be freely downloadable and shall support at the minimum Chrome, Opera, MS IE, Netscape, Mozilla Firefox, Safari etc.
18.	The User Interface shall require only standards compliant browsers with standard support for JavaScript and HTML. Full-fledged functionality of applications shall be accessible through standard browser without any additional software installation.
19.	The System shall perform all functions with keyboard support as well as mouse.
20.	The proposed System shall have the following operating flexibility; 1) Accommodate multiple levels of Organization structure (including add to roles, remove from roles, temporary and dual roles) 2) Switching between online and offline mobile modes of operation without loss of data 3) Multiple processing capabilities

S.No.	Requirements
	4) To modify and reorganize all menus 5) Multi-user logging in remote location 6) Facility for rearranging fields & deleting fields, which are not required by users 7) Open work group environment where users can access same information at the same time
21.	The System shall be platform independent and must be deployable on most of the databases.
22.	The System shall be operating system independent and support most of the available OS.
23.	The System shall be capable of connecting to various other systems in the distributed environment.
24.	The System shall accommodate the requirement to build APIs on the platform depending on SCRB requirement to share data to and from external databases and applications.
25.	The System shall support standard views to provide access to data over a unified access on portal.
26.	The System shall support secure data formats and wire protocols like SSL
27.	The System shall support multi-tiered architecture and shall be installable on different servers for logical or functional load sharing.
28.	The System shall support 24x7 availability with high availability hardware platform
29.	The System shall provide multi-dimensional selection option for query, dashboard and report builders.
30.	The System shall provide predefined unit of measure fields and valid values.
31.	The System shall provide color-coded field values at the time of multiple selections to easily detect errors in entered/ selected data.

S.No.	Requirements
32.	The System shall provide online taxonomy editing to allow restructuring and refine existing taxonomy.
33.	The System shall provide drag and drop tools to manage Hierarchies and taxonomy.
34.	The System shall provide audit trail for any restructuring in repository.
35.	All fields and data from legacy applications must be accessible to the user.
36.	The System shall enable users with uniform, role-based, and secure access to any kind of application, service, and information.
37.	The System shall enable and facilitate the creation of a portal over the Web to allow users access to information, applications and services.
38.	The System shall provide easy means for customization of the portal look and feel
39.	The System shall support widely used Internet and Web services standards, such as Java, JavaScript, J2EE, XML etc.
40.	The System shall support all standard databases
41.	The System shall be based on open architecture
42.	The System shall provide an application architecture, which can be integrated with third party / legacy applications using a middleware technology.
43.	The System shall have high availability with no single point of failure.
44.	The System shall be Unicode compliant
45.	The System shall be supported on TCP / IP / SMTP and other protocols
46.	The System shall be supported by the IP4 & IP6 network

S.No.	Requirements
47.	The System shall be extendible based on future requirements or requirements not met by standard functionality
48.	The System shall support upgrade to the later versions of the base version.
49.	The future versions of the System shall support functionalities provided in the earlier versions and give higher or equal user experience than the earlier version
50.	The System shall allow Owner to implement modules/ add-ons, which are not implemented as part of this project, at a later date. Integration between such modules with the modules already implemented shall not require any development effort.
51.	The System shall have ability to support for approval and approval thresholds.
52.	The System shall be natively built based on 64-bit CPU and 64-bit operation system
53.	The System shall include tools / mechanism for Application, System, Database, and Network administration and performance measurement activities as per specifications given in the RFP.
54.	The SI to mention bandwidth required per user connection session for all different modules
55.	The System shall have the ability to utilize workflow capabilities for routing, knowing status and be able to view the document flow with duration at each level.
56.	The System shall not clash with any other software for functioning e.g. Anti-Virus, Firewall, MS-Office
57.	The System shall have the ability to serve mailing requirements using third party mail server or mail server as an integral part of System
58.	The System shall have the ability to support in deploying Custom JSP and Servlets on Application Server

S.No.	Requirements
59.	The System shall have the ability to support remote operation of System administration and Security Management
60.	Load and stress testing tool shall be an integral part of the System
61.	Third party testing tools (like Mercury, Silk etc.) shall be able to be used as a service with System's load and stress testing integration
62.	The System shall have context sensitive help capability.
63.	The System supplied to SCRB shall be free from viruses, worms, Trojans, spy-ware etc. till the end of this contract.
64.	The System at the primary TNSDC and Disaster Recovery center shall have production, development, test landscape.
65.	The System shall support objects like images, videos, PDF's, HTML's, XML, WORDDOC, CSVs and other binary objects.

14.3 General Requirement of the Database

S. No.	Requirements
1.	The System shall support the all major database systems, e.g., Microsoft SQL, IBM DB2, Oracle, and Sybase
2.	The database shall support all RDBMS stored procedures and adhere to all such standards
3.	The database shall be able to handle structured data, unstructured data including multimedia formats such as images, videos, audios etc.

S. No.	Requirements
4.	The database shall have audit trail and log management capability.
5.	The database shall provide high availability 24x7
6.	The System shall be able to modify previously entered data in the database based on the requirement
7.	The database shall provide disaster recovery feature to synchronize business and transaction data to disaster recovery center
8.	The modified data in a database shall be updated for all users accessing it within 2 seconds.
9.	The database shall allow to modify the structure of the database based on the requirement
10.	The System shall provide health monitoring mechanism for database ensuring application availability and performance as per requirement

15. Annexure 3 – List of Police Stations, Special Units, Higher Offices and Training Center locations

SNo.	Zone	District	Police Station	Special Unit	Higher Office	Training Centre		Total
						D.T.C	PRS	
1	Chennai	Chennai city	170	47	6	2		225
2		Chennai Rlys	23	0	110	1		134
3	South	Madurai District	44	11	13	1		69
4		Dindigul	42	10	12	1		65
5		Theni	35	8	9	1		53

6		Ramnad	48	10	11	1		70
7		Sivagangai	44	7	8	1		60
8		Tirunelveli	70	9	14	1		94
9		Thoothukudi	56	9	12	1	1	79
10		Madurai city	25	10	16	1		52
11		Viruthunagar	54	9	11	1		75
12		Tirunelveli city	10	5	8	1		24
13		Kanyakumari	38	11	8	1		58
14	West	Coimbatore	36	11	10	1	1	59
15		Coimbatore city	18	10	15	1		44
16		Tiruppur city	9	2	2	1		14
17		Tiruppur	28	5	10	1		44
18		Erode	40	8	9	1		58
19		Nilgiris	32	6	9	1		48
20		Salem city	18	4	10	1		33
21		Salem	35	11	10	1		57
22		Namakkal	29	7	8	1		45
23		Dharmapuri	27	7	6	1		41
24		Krishnagiri	34	9	9	1		53
25	Central	Thanjavur	47	12	13	1		73
26		Thiruvarur	33	8	9	1		51
27		Nagapattinam	32	14	8	1		55
28		Ariyalur	18	4	6	1		29
29		Perambalur	9	6	5	1		21
30		Trichy city	18	12	12	1		43
31		Trichy district	35	5	11	1	1	53
32		Karur	18	7	7	1		33
33		Pudukottai	43	9	10	1		63
34		Trichy Rlys	24	0	4	1		29
35	North	Thiruvallur	34	10	9	1		54
36		Kancheepuram	44	12	11	1		68

37		Vellore	67	14	13	1	1	96
38		Thiruvannamalai	46	8	11	1		66
39		Viluppuram	56	14	12	1		83
40		Cuddalore	52	11	11	1		75
41	SCRB					1		
42	Police Headquarters					1		
43	TNPA					1		
44	PTC					1		
Total			**1541**	**372**	**488**	**45**	**4**	**2450**

16. Annexure 4 – CA EMS (Enterprise Management System) License Details

S #	Product Name	Usage Device	License Type
1	CA Network Flow Analysis	50 Server	Perpetual
2	CA Unified Infrastructure Mgmt Server and Application Pack - On Prem	1 Server	Perpetual
3	CA Unified Infrastructure Mgmt Server Pack - On Prem	24 Server	Perpetual
4	CA Spectrum Device Based Suite	50 Device	Perpetual
5	CA Performance Management	50 Device	Perpetual
6	CA Unified Infrastructure Mgmt SNMP Collector FOC for SysEdge migration	1 Server	Perpetual
7	CA Service Desk Manager Full License	5 Concurrent User	Perpetual
8	CA Privileged Identity Manager	18 Managed Device	Perpetual
9	CA Application Performance Mgmt	12 Processor	Perpetual
10	CA Unified Infrastructure Mgmt Server and Application Pack - On Prem	4 Server	Perpetual

17. Annexure 5 - Change Control Note Format

SI shall submit the details of Change Control Note in the below format to SCRB for approval.

Change Control Note	**CCN Number:**
Part A: Initiation	
Title:	
Originator:	
Sponsor:	
Date of Initiation:	
Details of Proposed Change	
(To include reason for change and appropriate details/specifications. Identify any attachments as A1, A2, and A3 etc.)	
Authorized by SCRB	Date:
Name:	
Signature: Received by	Date:
Name:	
Signature:	

Change Control Note	CCN Number:
Part B : Evaluation	
Change Control Note	
(Identify any attachments as B1, B2, and B3 etc.) Changes to Services, System architecture, implementation timelines, documentation, training, Service levels, component working arrangements and any other Contractual issue.	
Brief Description of solution:	
Impact:	
Deliverables:	
Timetable:	
Future Impact of not implementing proposed change	
Services unavailable during the Change request activity	
Post Implementation risk and risk probability	
Description of Post Implementation risk (other requirement effected) and potential mitigation plan	
Charges for implementation:	
Details of manpower to be provided (Provide CVs of manpower to be deployed in proforma as in Section C of CCN)	

Change Control Note	CCN Number:
Other Relevant Information: (including value-added and acceptance criteria)	
Authorized by the System Integrator	**Date:**
Name:	
Signature:	
Part C : Authority to proceed	
Change Control Note	**CCN Number :**
Implementation of this CCN as submitted in part A, in accordance with part B is: (tick as appropriate)	
Approved Rejected Requires Further Information (as follows, or as Attachment 1 etc.)	
For SCRB	**For the System Integrator**
Signature	Signature
Name	Name
Title	Title

Change Control Note	CCN Number:
Date	Date

18. Annexure 6 – Current User Count, User Roles & Privileges

User Count

S.No	Name of the Role	Designation shortcut	No of Users created so far
1	Director General of Police	DGP	1
2	Additional Director General of Police	ADGP	39
3	Commissioner of Police	COP	7
4	Inspector General of Police	IG	13
5	Deputy Inspector General of Police	DIG	22
6	Joint Commissioner of Police	JCP	8
7	Additional Commissioner of Police	ADC	10
8	Superintendent of Police	SP	60
9	Deputy Commissioner of Police	DCP	41
10	Additional Superintendent of Police	ADSP	88
11	Additional Deputy Commissioner of Police	ADCOP	5
12	Deputy Superintendent of Police	DSP	477
13	DCRB (DCRB DSP)	DET	51
14	Assistant Commissioner of Police	ACP	182
15	IS Assistant Commissioner of Police	ISACP	2
16	IS Inspector of Police	ISIOP	15
17	Station House Officer	SHO	2798

18	IS Moderator	IMDTR	1
19	Moderator	MDTR	77
20	District Legal Services Authority	DLSA	58
21	MCOP	MCOP	290
22	Regional Transport Office	RTO	30
23	State Transport Corporation	STC	40
24	Insurance Companies	INS	151
25	Admin Users	ADMIN	5
26	Super User	NIC	10
27	Mobile Service Provider	MSP	3
28	ADGP ADMIN	ADGPA	1
29	City Commissioner Office - Browsing	COFFB	2
30	City Commissioner Office - Gym	COFFG	2
31	City Commissioner Office - Video	COFFV	1
32	City Commissioner Office -Arms	COFFA	2
Total			**4492**
	Common Service Centre	No user	
	Crime against Women and Children	Yet to create	

User Roles & Privileges in Existing System:

S.No	Name of the Role	Designation shortcut	Multi User Creation	Roles and privileges		
				Menu : Case progress summary, Review Reports, Statements	Menu : Know any FIR	Menu : Query Search

Police Officials						
1	Director General of Police	DGP	No	State wide	State wide	State wide
2	Additional Director General of Police	ADGP	Yes	State wide (exclude CBCID, Q-Branch)	State wide (exclude CBCID, Q-Branch)	
3	Commissioner of Police	COP	No	Jurisdictional view		
4	Inspector General of Police	IG	No	Jurisdictional view		
5	Deputy Inspector General of Police	DIG	No	Jurisdictional view		
6	Joint Commissioner of Police	JCP	No	Jurisdictional view		
7	Additional Commissioner of Police	ADC	No	Jurisdictional view		
8	Superintendent of Police	SP	No	Jurisdictional view		
9	Deputy Commissioner of Police	DCP (can create user account for L&O, Crime)	No	Jurisdictional view		
10	Additional Superintendent of Police	ADSP	No	Jurisdictional view		
11	Additional Deputy Commissioner of Police	ADCOP	No	Jurisdictional view		
12	Deputy Superintendent of Police	DSP	No	Jurisdictional view		
13	DCRB (DCRB DSP)	DSP DCRB	No	Jurisdictional view		

				(SP/ DC Role)		
14	Assistant Commissioner of Police	ACP	No	Jurisdictional view		
15	Crime against Women and Children		Yes	Jurisdictional view		
16	IS Assistant Commissioner of Police	ISACP	No	No Such menu	No such menu	
17	IS Inspector of Police	ISIOP	No	No Such menu		
18	Station House Officer	SHO (can create user account for L&O, Crime)	Yes	Jurisdictional view	Jurisdictional search	
19	IS Moderator	IMDTR	No	No Such menu	No such menu	State wide
20	Moderator	MDTR	No	No Such menu	No Such menu	No Such menu
RTA Document Download Facilities						
Court Authorities						
21	District Legal Services Authority	DLSA	No	Menus: Download cases, MIS Report (RTA Cases)		
22	MCOP	MCOP - SCRB Usage	No			
Transport Authorities						
23	Regional Transport Office	RTO	Yes	Dashboard, Summary Report, Yearwise Report of RTA cases and Download Mobile app		
24	State Transport Corporation	STC	Yes	Menus: Download cases, MIS		

				Report (RTA Cases)
Insurance companies				
25	Insurance Companies	INS	Yes	Menus: Download cases, MIS Report (RTA Cases)
ADMIN USER				
26	Admin Users	ADMIN	Total 5 Logins and have menus to upload the details. admin01 is dedicative for PVR	
27	Super User	NIC	Yes	Contains all menus.
Other User				
28	Mobile Service Provider	MSP	No	created on 2012 - not yet used
29	ADGP ADMIN	ADGPA	dummy user	
30	City Commissioner Office – Browsing	COFFB	created on 2012 - not yet used	
31	City Commissioner Office - Gym	COFFG		
32	City Commissioner Office - Video	COFFV		
33	City Commissioner Office -Arms	COFFA		

19. Annexure 7 – Application Security Requirements

S.No.	Minimum Specifications
1	The proposed solution should be positioned in the leader quadrant from last three published Gartner Magic quadrant report for Endpoint Protection
2	Endpoint solution should have capability of Anti-Virus, Vulnerability Protection, Firewall, Device control, Application Control, Virtual Patching, DLP from day one.
3	Proposed solution should have Pre, Post and Runtime machine learning capability

4	Proposed solution should have True file type scan along with Proactive outbreak prevention and Command & Control callback detection
5	File reputation - Variant protection - Census check - Web reputation
6	Advanced malware and ransomware protection: Defends endpoints—on or off the corporate network—against malware, Trojans, worms, spyware, ransomware, and adapts to protect against new unknown variants and advanced threats like crypto malware and fileless malware
7	Endpoint vulnerability protection should scan the machine and provide CVE number visibility and accordingly create rule for virtual patch against vulnerability
8	Behavior monitoring along with ransomware protection engine, ransom ware engine should have feature to take backup of ransom ware encrypted files and restoring the same
9	Proposed solution should have IPv4 and IPv6 support
10	Endpoint solution should have data loss prevention with pre-defined templates for HIPAA, PCI-DSS, GLBA etc. for compliance requirements and should have capability to create policies on basis of regular expression, key word and dictionary based
11	Offers visibility and control of data in motion of sensitive information—whether it is in email, webmail, instant messaging (IM), SaaS applications, and most networking protocols such as FTP, HTTP/HTTPS, and SMTP
12	Prevents potential damage from unwanted or unknown applications (executables, DLLs, Windows App store apps, device drivers, control panels, and other Portable Executable (PE) files)
13	Provides global and local real-time threat intelligence based on good file reputation data correlated across a global network
14	Contains broad coverage of pre-categorized applications that can be easily selected from application catalog (with regular updates)
15	Uses application name, path, regular expression, or certificate for basic application whitelisting and blacklisting
16	Uses intelligent and dynamic policies that still allow users to install valid applications based on reputation-based variables like the prevalence, regional usage, and maturity of the application

17	Ensures that patches/updates associated with whitelisted applications can be installed, as well as allowing your update programs to install new patches/updates, with trusted sources of change
18	Should have roll-your-own application whitelisting and blacklisting for in-house and unlisted applications
19	Limits application usage to a specific list of applications supported by data loss prevention (DLP) products for specific users or endpoints and collects and limits application usage for software licensing compliance
20	Proposed solution should not send any file/sample with cloud to inspect and analyze for any threat
21	Features system lockdown to harden end-user systems by preventing new applications from being executed
22	Should be capable of recommending rules based on vulnerabilities on endpoint and create dynamic rules automatically based on System posture and endpoint posture
23	Blocks known and unknown vulnerability exploits before patches are deployed and Provides protection before patches are deployed and often before patches are available
24	Vulnerability Protection virtually patches known and unknown vulnerabilities, giving you instant protection, before a patch is available or deployable
25	Automatically assesses and recommends required virtual patches for your specific environment
26	Dynamically adjusts security configuration based on the location of an endpoint
27	Blends signature-less techniques, including high-fidelity machine learning, behavioral analysis, variant protection, census check, application control, exploit prevention, and good file check with other techniques like file reputation, web reputation, and command and control (C&C) blocking
28	Shields operating system and common applications from known and unknown attacks
29	Organizes vulnerability assessments by Microsoft security bulletin numbers, CVE numbers, or other important information

S.No.	Minimum Specifications
1	The solution must provide single platform for complete server protection over physical, virtual (server/desktop), & cloud:
2	Complete protection from a single integrated platform: addresses all of the 'Gartner top ten server security priorities'
3	Provides layered defense against advanced attacks and shields against known and unknown vulnerabilities in web and enterprise applications and operating systems.
4	Single management console to manage workloads across physical, virtual and cloud
5	The proposed solution must be able to perform machine learning to discover new threats before file is executed
6	The proposed solution must be able to monitor behavior of running process to detect malicious behaviors
7	The Proposed Solution Should Support Behavior Monitoring
8	The Proposed Solution should Support Realtime monitoring and should be able to detect and clean malware even if it is stagnant and not executing
9	The proposed Solution should be able to Detect Malware at Disk IO
10	The Proposed Solution Should support Manual and Scheduled Scans.
11	Must be able to provide scan assessment engine to discover OS & application vulnerabilities on a server and determine which vulnerabilities have not been mitigated & recommend rules to shield to shield applications & systems with advanced deep packet inspection technology
12	Must feature a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations
13	Must be able to operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities
14	Must provide detailed events with valuable information, including who attacked, when they attacked, and what they attempted to exploit. Administrators can be notified automatically via alerts when an incident has occurred

15	Must be able to provide protection against known and zero-day attacks
16	Must include smart rules to provide zero-day protection from unknown exploits that attack an unknown vulnerability, by detecting unusual protocol data containing malicious code
17	Must include exploit rules to stop known attacks and malware and are similar to traditional antivirus signatures in that they use signatures to identify and block individual, known exploits
18	Must automatically shield newly discovered vulnerabilities within hours, pushing protection to large number of servers in minutes without a system reboot
19	Must be able to provide Application Control in whitelist or blacklist mode
20	Solution should support adding of Blacklisted IOC's (Hashes) for Blocking
21	Solution should have the ability to work in Detect and Block mode
22	Solution should have the ability to show all the running processes and give the option for Allow or Block in intuitive GUI
23	The solution should support Maintenance Mode in which during predefined Downtimes, upgrade etc.. can take place and all processes automatically learnt and Whitelisted
24	Must include an enterprise-grade, bidirectional stateful firewall providing centralized management of firewall policy, including predefined templates
25	Detection of reconnaissance scans
26	Solution Should support Inline and TAP Modes
27	Solution should be able to Configure Stateful and Stateless
28	Solution Should support SSL Decryption
29	Must be able to monitor critical operating system and application such as directories, registry keys, and values to detect and report malicious and unexpected changes in real-time
30	Solution Should Support Realtime Integrity Monitoring
31	Solution Should support Integrity Monitoring for Process, Ports, Files, Attributes, Permissions
32	Solution should enable IM rules based on the posture of the machine and should be dynamic (Like new software installed)

33	The proposed solution should have intelligence to analyze and share key informational events for correlation to SIEM
34	The proposed solution should be positioned in the leader quadrant from last three published Gartner Magic quadrant report for Endpoint Protection
S.No.	**Minimum Specifications**
1	The proposed OEM must be positioned in Leader Quadrant " The Forrester Wave Enterprise Email Security, Q2 2019 Report".
2	The proposed solution should be an appliance based dedicated Email Anti-APT Security solution that provides enterprise message transfer agent (MTA) capabilities SMTP/SMTP-TLS, Anti-malware, BEC/CEO fraud attack prevention, social engineering attack protection, ransomware, unknown malware threats - Sandboxing and anti-phishing.
3	The solution should support domain authentication using DMARC and spam prevention using DKIM and Sender policy Framework
4	Simplifies regulatory compliance and data loss prevention through pre-defined and customizable DLP policies and templates
5	The proposed solution must be purpose built hardware appliance with hardened operating system and must be able to support both incoming as well as outgoing messages.
6	The solution must have SMTP Traffic Throttling to block messages from a single IP address or sender for a certain time when the number of connections or messages reaches the specified maximum. Also provide Firewall against DHA and bounced mail attacks.
7	The proposed solution must have dedicated management port which should be separate from data ports.
8	The proposed solution should be a hardware appliance with redundant power supply.
9	Deployment mode: Solution must support flexible deployment modes -MTA, BCC, SPAN/TAP modes.
10	Solution must be able to analyze, process and inspect at least 400,000 emails/day.
11	File Types Supported : Multiple file types including windows executables, Scripts, Java, office, office with macros, Pdf, image/jpeg files, vbs, dll, lnk, swf All types of Compressed files.

12	Solution must support file size support up to 50 MB in case of sandboxing.
13	Solution should support IPv4 and IPv6 addressing for email message processing and management console and CLI access.
14	Solution must support at least 25 or more sandboxing virtual instances on the email APT appliance to provide consolidated inspection of emails with low false positive rates.
15	Solution must be capable to sandbox file as well as URL's.
16	The proposed solution must support both 32-bit / 64-bit Windows 8 ,8.1 & 10, Windows 2003 ,2008 & 2016 server sandbox images and should allow at least three types of sandbox images for virtual analysis.
17	The proposed solution should investigate URLs embedded in an email message by using reputation technology, direct page analysis, and sandbox simulation if required.
18	The proposed solution support advanced detection technology to discover targeted threats in email messages, including spear-phishing and social engineering attacks. • Reputation and heuristic technologies catch unknown threats and document exploits • File hash analysis blocks unsafe files and applications • Detects threats hidden in password-protected files and shortened URLs • Predictive machine learning technology detects emerging unknown security risks
19	The proposed solution should have capability to uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks.
20	The Proposed solution should be able to detect and analyze URLs which embedded in MS office and PDF attachments.
21	The proposed solution should have anti malware and Anti spam engine
22	The proposed solution should look for known and potential exploits to the intended office application and analyze macros
23	The Proposed solution detect and analyze the URL direct link which point to a file on the mail body.
24	The Proposed solution should be able to detect and analyzed the URL's in mail subject.

25	The Proposed Solution should be able to detect known bad URL before sandboxing
26	The proposed solution should be able to detects, downloads and analyzes files directly linked in the email message body.
27	The Proposed solution should be able to detect true file types.
28	The Proposed solution should have capabilities to detect Ransomware using Decoy files on sandboxes.
29	The Proposed solution should not have any limitation which require all attachments to be sent to sandbox, only suspicious attachments should be sent to sandbox for analysis.
30	The Proposed solution should have an option for timeout/ release of an email if the file analysis on the sandbox is taking over 20 mins.
31	The Proposed solution should support heuristically discovery passwords in email messages or import custom password for inspecting email messages with password protected file.
32	The Proposed solution should support at least 100 predefined passwords for scanning archive files
33	The solution should be able to Block mail message and store a copy in the quarantine area.
34	The Proposed solution should be able to Deliver the email message to the recipient after replacing the suspicious attachments with a text file and tag the email message subject with a string to notify the recipient
35	The Proposed solution should be able to pass and tag the email message
36	The Proposed solution should have option to make policy exceptions for safe senders, recipients, and X-header content, files and URL's
37	The Proposed Solution should be able to define risk levels after investigation of email messages
38	The Proposed solution should allow administrators to be able to see the HTML format reporting on console and download PDF report
39	The Proposed solution should be able to send real time email alert per detection
40	The Proposed Solution should support Real-Time URL click protection.
41	The Proposed Solution should support manual email message submission in" .eml" format for analysis purpose.

42	The Proposed Solution should support Pre-Execution Machine Learning scanning feature which looks at static file features to predict maliciousness in mail & attachment in the mail.
43	Solution should have an option to generate reports on demand or set a daily, weekly, or monthly schedule.
44	The proposed solution should support on premise centralized management for viewing information about detection, message tracking and MTA logs.
45	Solution should be able to integrate with Microsoft Active Directory (AD) for account management
46	Solution should be able to centrally manage and deploy product updates including patches, hotfixes, and firmware upgrade
47	The solution central management should include various methods of sharing threat intelligence data with other products or services including TAXII / Web services.
48	Solution must support custom intelligence ie STIX/TAXII, IOC's, YARA and create suspicious objects repository for Organization.

CRIME & CRIMINAL TRACKING NETWORK AND SYSTEMS (CCTNS)

Tender Reference

ELCOT/PROC/OT/33384/CCTNS 2.0 (SCRB)/ 2020-21

Request for Proposal

For

Selection of System Integrator for Supply, Design, Development, Implementation and Maintenance of CCTNS 2.0

Volume III

Tender Document

Table of Contents

Master Service Agreement

Draft

THIS AGREEMENT is made on this the <***> day of <***> 2020 at _____, India.

BETWEEN

State Crime Records Bureau having its office at 95, Greenways Rd, MRC Nagar, Raja Annamalai Puram, Chennai - 600028, Tamil Nadu hereinafter referred to as '**SCRB**', which expression shall, unless the context otherwise requires, include its permitted successors and assigns) of the one part;

AND

<***>, a Company incorporated under the *Companies Act, 1956*, having its registered office at <***> represented by …… (hereinafter referred to as '***System Integrator***' which expression shall, unless the context otherwise requires, include its permitted successors and assigns) of the other part;

Each of the parties mentioned above are collectively referred to as the '***Parties***' and individually as a '***Party***'.

WHEREAS:

1. SCRB is desirous to execute the Project of Selection of System Integrator for Supply, Design, Development, Implementation & Maintenance of CCTNS 2.0.
2. In furtherance of the same, SCRB undertook the selection of a suitable System Integrator through a competitive Bidding process for implementing the Project and in this behalf issued Request for Proposal (RFP) dated DD/MM/YYYY.
3. <**********> has been selected as the System Integrator on the basis of the evaluation criteria of the aforementioned RFP, to undertake the Project of Supply, Design, Development, Implementation & Maintenance of CCTNS 2.0.
4. A Letter of Acceptance No. _____ dated _____ has been issued to the successful System Integrator <***> by SCRB.

NOW, THEREFORE, in consideration of the mutual covenants, promises, assurances, representations and provisions set forth herein, the parties hereto agree as follows: -

1. Definition and Interpretation

1.1 Definition

Terms and expressions used in this MSA (including the introduction) shall have the meanings set out below in Clause 1.2.

1.2 Interpretation

In this MSA, unless otherwise specified:

1) reference to any statute or statutory provision shall be construed as a reference to the same as it may have been, or may from time to time be, amended, modified or re-enacted;
2) use of any gender includes the other genders;
3) references to clauses, sub-clauses, paragraphs, Schedules and Annexure are to clauses, sub-clauses, paragraphs, Schedules and Annexure to this MSA;
4) a reference to any other document referred to in this MSA is a reference to that other document as amended, varied, novated or supplemented at any time;
5) all headings and titles are inserted for convenience only. They are to be ignored in the interpretation of this MSA;
6) "**Assets**" means all Assets used in providing Services in accordance with this MSA and shall include: -
    a. IT and Non-IT Infrastructure including Hardware, Software, System Software required for delivery of Services under the Project;
    b. All data, documentation, reports, records, source code etc. created during the Project and for the purpose of the Project;
    c. All upgradation/ enhancements and improvements to the above Assets;
7) "**Acceptance**" means acceptance of the proposed solution by SCRB after clearance by SCRB;

8) "**Auditor"** refers to the Statutory Auditor of a company;

9) **"Bid"/ "Proposal"** means the documents in their entirety comprising of the Pre-Qualification, Technical and Commercial Proposal, clarifications to these, Technical Presentation submitted by the Bidder, the System Integrator herein, in response to the RFP, and accepted by SCRB.

10) "**Bidders**" refer to eligible, reputed, qualified IT Agencies/ firms/companies with strong Technical and Financial capabilities for supply, design, development, implementation and maintenance of CCTNS 2.0 as a total IT Solution who may be responding to this RFP.

11) "**Business Day**" means any day that is not a Sunday, or a Public Holiday as declared by Government of Tamil Nadu.

12) "**Clauses**" refers to Clauses of this Agreement. The words "include" and "including" shall not be construed as terms of limitation.

13) "**Company**" shall be construed to include any company, corporation or other body corporate, wherever and however incorporated or established.

14) "**Confidential Information**" means all information including the data (whether in written, oral, electronic or other format) which relates to the technical, financial and business affairs, customers, suppliers, products, developments, operations, processes, data, trade secrets, design rights, know-how and staff of each party and its affiliates which is disclosed to or otherwise learned by the other party in the course of or in connection with this MSA (including without limitation such information received during negotiations, location visits and meetings in connection with this MSA).

15) "**Contract**" means the agreement entered into between SCRB and the "System Integrator" as recorded in the Contract form signed by SCRB and the "System Integrator" including all attachments and annexure thereto; in this document, the word 'Contract' refers to the MSA;

16) "**Contract/ Project Period**" means the time period from the date of signing of Contract till 5 years after Go-live or further extended on mutually agreed basis.

17) "**Day**" means a period of 24 hours running from midnight to midnight. It means "calendar day" unless otherwise stated. Where, because of a difference in time zone, the calendar day in one country differs from another country, then the calendar day shall be deemed to be the calendar day applicable to India.

18) "**Deliverables**" means all the documents, milestones and activities related to the setting up and operations of CCTNS 2.0 project in SCRB, as defined in Volume - I & II of the RFP, and as required as per this MSA.

19) "**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.

20) "**EMD**" refers to the amount to be deposited by the Bidders to ELCOT to demonstrate commitment and intention to complete the process of selection of System Integrator for supply, design, development, implementation and maintenance of CCTNS 2.0 in SCRB;

21) "**Effective Date**" means the date on which this MSA is signed.

22) "**End of Contract**" refers to the date on which the Contract Period comes to an end.

23) "**Force Majeure**" means the clauses that excuse a party from liability if some unforeseen event beyond the control of that party prevents it from performing its obligations under the Contract. Typically, force majeure clauses cover natural disasters or other "Acts of God" or War.

24) "**Go-live**" means the date as declared by SCRB on which the CCTNS 2.0 application becomes operational after successful conclusion of all acceptance tests as provided in the RFP and subject to the satisfaction of SCRB. Planned date of Go-live is 7 months from the date of signing of Contract.

25) "**GoTN**" shall mean Government of Tamil Nadu, India and shall include its legal representatives, successors and permitted assignees.

26) "**SCRB Assets**" means all Assets made available to the System Integrator by SCRB or by any person designated by SCRB.

27) "**Internal Users**" refers to all users of the System who are internal to SCRB including police stations, special units, higher offices and training centres.

28) "**Intellectual Property Rights**" means any patent, copyright, trademark, trade name, design, trade secret, permit, service marks, brands, propriety information, knowledge, technology, licenses, databases, computer programs, software, know how or other form of intellectual property right, title, benefits or interest whether arising before or after the execution of this Contract and the right to ownership and registration of these rights.

29) "**Kick-off Meeting**" means a one-time meeting convened by SCRB to discuss and plan the execution of this Project with the System Integrator immediately after signing of this MSA.

30) "**Letter of Acceptance**" refers to the letter issued by State Crime Records Bureau, Government of Tamil Nadu to the successful System Integrator indicating its selection as the System Integrator for the CCTNS 2.0 Project.

31) "**MSA**" means this Master Service Agreement, together with the recitals and all Schedules and the contents, requirements, specifications and standards of the Volume-I, Volume – II & Volume III of the RFP (as may be amended, supplemented or modified in accordance with the provisions hereof) and the proposal of the selected System Integrator.

32) "**Month**" means "calendar month" unless otherwise stated. Where, because of a difference in time zone, the calendar month in one country differs from another country, then the calendar month shall be deemed to be the calendar month applicable to India.

33) "**Net-worth**" refers to Paid-up share capital + Reserves and Surpluses (Excluding Revaluation Reserves) – Preliminary and Pre-operative expenditure, accumulated losses and miscellaneous expenditure to the extent not written off, as per the annual report and as adjusted with any qualifications in the auditors' report.

34) "**Operations and Maintenance**" means the operation, maintenance and handholding of the Project by the System Integrator as required to meet the service levels and other requirements of the RFP;

35) "**Parties**" means the SCRB and the System Integrator and "Party" means either of the parties.

36) "**Performance Bank Guarantee**" means the irrevocable and unconditional bank guarantee provided by the System Integrator from any scheduled bank in favour of "_____" payable at Chennai for an amount equal to 5% of the Total Contract Value.

37) "**Project Engagement Document**" means a written document in the form of a work order or a letter of acceptance issued to the System Integrator by SCRB, or any other written document approved from time to time by SCRB to evidence the parties' intention to engage System Integrator to provide Services to SCRB under the SLA in accordance with this MSA and to describe the Services to be performed including a statement of work.

38) "**Proprietary Information**" means processes, methodologies and technical and business information, including drawings, designs, formula, flow charts, data and computer programs already owned/licensed by either party or granted by third parties to a party hereto prior/ after the execution of this MSA.

39) "**Required Consent**" means the written consents, clearances and licenses, rights and other authorizations as may be required to be obtained by the System Integrator, for all tasks/activities/software/hardware and communication technology under the Project; from all the concerned departments/agencies, etc. as the case may be;

40) **"RFP"** means the Request for Proposal released vide Bid document ELCOT/ PROC/ OT/ 33384/ CCTNS 2.0 (SCRB)/ 2020-21 dated _____, containing the technical, functional, commercial and operational specification for the Implementation of CCTNS 2.0 project of SCRB, issued in 3 Volumes (referred to as Volume I, Volume II and Volume III) and including all clarifications, corrigendum, explanations and amendments issued by SCRB in respect thereof.

41) "**Service**" means facilities/Services to be provided as per the requirements specified in this Master Service Agreement and any other incidental Services, such as application

development, installation, implementation, training, maintenance, provision of technical assistance and other such obligations of the System Integrator covered under the MSA.

42) "**Service Level**" means the level of Service and other performance criteria which will apply to the Services as set out in the MSA effective during the term of the MSA.

43) "**Service Level Agreement**" means Agreement(s) executed by and between the SCRB and the System Integrator for delivering various services as set out in this MSA;

44) "**Sign-off**" shall mean a written documentation issued by SCRB evidencing the acceptance, approval or completion of any Deliverable including any documentation or testing, that may be required in terms of the MSA.

45) "**State-wide rollout**" refers to the day when the System Integrator completes the rollout of the new system at all locations across the state as per requirements of the RFP and is ready for acceptance testing by SCRB.

46) **System Integration** refers to the process through which the engaged business entity (firm/company) will design and build computing systems customized to the needs of SCRB as stated in the RFP by combining communication infrastructure, hardware and software products from one or more vendors. The hardware and software products may be new or existing systems and may be built afresh from scratch or packaged products.

47) "**System Integrator**" / "**SI**" means the Company with whom the Contract has been entered into for providing Services as specified in this Master Service Agreement and shall be deemed to include the System Integrator's successors, representatives (approved by SCRB), their, executors, and administrators and permitted assigns, as the case may be, unless excluded by the terms of the Contract.

48) "**System Integrator's Representative**" means the person or the persons appointed by the System Integrator from time to time to act on its behalf for overall co-ordination, supervision and execution of Project.

49) "**Term**" means the duration of this MSA.

50) "**Time**" refers to Indian Standard Time.

51) "**Total Contract Value"/ "Contract Value**" refers to the value finally agreed between SCRB and the System Integrator for the delivery of Services mentioned in the RFP (after negotiations with the selected System Integrator) which will be the maximum value payable to the System Integrator on this Contract.

1.3 Measurements and Arithmetic Conventions

All measurements and calculations shall be in the metric system and calculations done to 2 (two) decimal places, with the third digit of 5 (five) or above being rounded up and below 5 (five) being rounded down except in money calculations where such amounts shall be rounded off to the nearest Rupee.

1.4 Ambiguities within Agreement

In case of ambiguities or discrepancies within this MSA, the following principles shall apply:

a. as between two clauses of this MSA, the provisions of a specific clause relevant to the issue under consideration shall prevail over those in a general clause;
b. as between the provisions of this MSA and the Schedules, the MSA shall prevail, save and except as expressly provided otherwise in the MSA or the Schedules; and
c. arithmetic errors shall be corrected.
d. as between any value written in numerals and that in words, the lower of the two shall be considered.

1.5 Priority of Documents

This MSA, including its Schedules, represents the entire Agreement between the parties as noted in this clause. If in the event of a dispute as to the interpretation or meaning of this MSA it should be necessary for the parties to refer to documents forming part of the bidding process leading to this Agreement, then such documents shall be relied upon and interpreted in the following descending order of priority:

(a) Any Clarification/ Amendments issued by SCRB on the MSA, SLA and NDA, Schedules and Annexures.

(b) This MSA along with the SLA Agreement, NDA Agreement, Schedules and annexure

(c) Request for Proposal and Corrigendum to the Request for Proposal (if any).

2. Conditions Precedent

2.1 Provisions to take effect upon fulfilment of conditions precedent

Subject to express terms to the contrary, the rights and obligations under this MSA shall take effect only upon fulfillment of all the Conditions Precedent set out below. However, SCRB may at any time at its sole discretion waive fully or partially any of the conditions precedent for the System Integrator.

2.2 Conditions Precedent of the system integrator

The System Integrator shall be required to fulfill the Conditions Precedent within 15 Business Days from issue of the Letter of Acceptance to the System Integrator. The Conditions Precedent are as follows:

(a) to provide a Performance Bank Guarantee and any other guarantees to SCRB; and

(b) to provide SCRB certified true copies of its constitutional documents (Memorandum of Association (MOA), Articles of Association (AOA), etc.) and board resolutions authorizing the execution, delivery and performance of this MSA by the System Integrator.

2.3 Extension of time for fulfillment of Conditions Precedent

(a) The parties may, by mutual agreement extend the time for fulfilling the Conditions Precedent and the term of this MSA.

(b) For the avoidance of doubt, it is expressly clarified that any such extension of time requested by the System Integrator for reasons solely attributable to him, shall be subject to imposition of penalties on the System Integrator linked to the delay in fulfilling the Conditions Precedent.

2.4 Non-fulfillment of the System Integrator's Conditions Precedent

(a) In the event that any of the conditions precedent of the System Integrator have not been fulfilled within 15 Business Days from the date of issue of Letter of Acceptance and the same have not been waived fully or partially by SCRB, this MSA shall cease to exist.

(b) In the event that the MSA fails to come into effect on account of non-fulfillment of the System Integrator's conditions precedent, SCRB shall not be liable in any manner whatsoever to the System Integrator and SCRB shall forthwith forfeit the Performance Bank Guarantee and the EMD.

(c) In the event that possession of SCRB facilities has been delivered to the System Integrator prior to the fulfillment of the conditions precedent, upon the termination of this MSA, such shall immediately revert to SCRB, free and clear from any encumbrances or claims.

3. Performance Bank Guarantee

Performance Bank Guarantee is governed for supplies and services as follows:

(a) System Integrator shall carry out the Services in conformity with this MSA, the RFP, generally accepted professional and technically accepted norms relevant to CCTNS 2.0 Projects and to the entire satisfaction of SCRB.

(b) In the event of any deficiency in Services, the System Integrator shall promptly take necessary action to resolve it, at no additional fees to SCRB.

(c) The Earnest Money deposited at the time of Bid submission would be given back to the System Integrator on submission of Performance Bank Guarantee.

System Integrator shall deposit the Performance Bank Guarantee as follows:

(a) 5% of Total Contract Value in the form of an irrevocable unconditional bank guarantee as per the format provided in the RFP from a Scheduled Bank

(b) The Performance Bank Guarantee should be furnished within 21 Business Days from the date of issue of Letter of Acceptance and should be valid till 70 months.

(c) No interest will be paid by ELCOT/ SCRB on the EMD & Performance Bank Guarantee.

4. Project Initialization

4.1 Scope of Work

(a) Subject to the Terms and conditions of this MSA and System Integrator shall perform all its obligations hereunder to provide the Services and products defined and described in Volume – I & II of the RFP (hereinafter referred to as "Services") to SCRB.

(b) If any Services, functions or responsibilities not specifically described in this Contract are an inherent, necessary or customary part of the Services or are required for proper performance or provision of the Services in accordance with this MSA, they shall be deemed to be included within the scope of the work to be delivered for the charges, as if such Services, functions or responsibilities were specifically described in this MSA.

(c) SCRB reserves the right to modify (add/ delete) the scope of work or amend/delete/add any of the terms and conditions in relation to the scope of work and may issue any such directions which are not necessarily stipulated therein if it deems necessary for the fulfillment of the scope of work. Any changes to the scope of work will be governed by the Change Control Schedule of the MSA to be mutually agreed upon by both parties as covered in Section "Change Control Schedule" of this Volume (Volume III) of the RFP.

4.2 Agreement Owners

The following personnel are notified as the MSA Owners:

	TITLE	TELEPHONE	WEBSITE AND EMAIL
SCRB			
SYSTEM INTEGRATOR			

Contact List

Additional Director General of Police (ADGP), State Crime Records Bureau will be the primary contact regarding operation of this Master Services Agreement (MSA) from SCRB. Similarly, an authorized signatory of the System Integrator will be nominated to be the primary contact regarding operation of this Master Services Agreement (MSA) from the selected System

Integrator's side. The primary contact from both parties is referred to as the Principal Contact in this MSA, the contact details of the Principal Contacts are:

SCRB Principal Contact:

Additional Director General of Police (ADGP)
State Crime Records Bureau
95, Greenways Rd, MRC Nagar, Raja Annamalai Puram,
Chennai, Tamil Nadu 600028

System Integrator Principal Contact: _____

Any changes to the listed contacts must be communicated and updated prior to the change occurring to the Principal Contact of the other party.

4.3 Commencement and Duration of the Contract

This MSA shall come into effect on the Effective Date and shall continue, unless terminated earlier in accordance with the provisions hereof, for a period of 5 years after Go-live of the Project.

SCRB would eventually decide on one of the following options for managing the Project beyond the Contract Period.

(a) Replace – Appoint a different agency for undertaking system maintenance beyond the Contract Period through a fresh tender

(b) Transfer - The System Integrator will transfer the Project including all Assets to SCRB and SCRB will manage the operations on its own.

In the eventuality that no such alternate arrangements are in place for managing the Project at the end of the Contract period, the selected System Integrator will be required to continue delivering services as required under this Project, at the same terms and conditions mentioned in the signed Contract and RFP, even beyond the Contract period (such period not exceeding 1 year) till alternate arrangement is done by SCRB to manage the operations.

The decision to extend the Contract with the System Integrator (if applicable) will be communicated to the System Integrator atleast 3 months before the expiry of the Contract.

4.4 Statutory Requirement

(a) During the tenure of this contract, the System Integrator shall refrain from indulging in activities which are in contravention of any law, act and/ or rules/ regulations, there under or any amendment thereof governing inter-alia customs, excise, taxes and levies, stowaways, foreign exchange etc. and shall keep SCRB indemnified in this regard.

(b) The System Integrator will ensure that an updated location-wise list of all assets deployed by the System Integrator for the purpose of the Project is always available. The System Integrator will seek SCRB's approval before installing any hardware at any location and will also not alter / change / replace any hardware component deployed for the purpose of the Project without prior consent of SCRB.

(c) No party to this MSA shall at any time performs, or omit to perform, any act which it is aware, at the time of performance, shall place the other party in default under any insurance policy, mortgage or lease governing activities at any location provided by SCRB.

4.5 System Integrator's Obligations

(a) The System Integrator's obligations shall include all the activities as specified by SCRB in the scope of work and other sections of the RFP and MSA and changes thereof to meet SCRB's objectives and operational requirements. It will be the System Integrator's responsibility to ensure the proper and successful implementation, performance and continued operation of the proposed solution in accordance with and in strict adherence to the terms of this MSA, the RFP and the proposal.

(b) The System Integrator shall ensure that the System Integrator's team is competent, professional and possesses the requisite qualifications and experience appropriate to the task they are required to perform under this Contract. The System Integrator shall ensure that the Services are performed in accordance with the terms hereof and to the satisfaction of SCRB.

(c) Except as otherwise provided for herein or with the prior written approval of SCRB, the System Integrator and/or System Integrator's team shall not: -

i. systematically collect and use any SCRB data, Deliverables, Assets or SCRB contents/contents of services and information, including the use of any data mining, or similar data gathering and extraction methods;

ii. market, sell, or make commercial or derivative use of SCRB data, Deliverables or Assets, SCRB contents/contents of services and information;

iii. publish, publicly perform or display, or distribute to any third party any SCRB data, Deliverables or SCRB contents/contents of Government services and information, including reproduction on any computer network or broadcast or publications media; or

iv. use, frame, or utilize framing techniques to enclose any portion of SCRB data, Deliverables or SCRB contents/contents of services and information (including images, any text or the layout/design, form or content of any page or otherwise).

4.6 SCRB Obligations

(a) Additional Director General of Police (ADGP) of State Crime Records Bureau, or his/her authorized representative shall act as the nodal point for implementation of the Project and for issuing necessary instructions, approvals, commissioning, acceptance certificates, payments etc. to the System Integrator.

(b) SCRB shall provide requisite approvals to the System Integrator from time to time, which may include approval of Project plans, implementation methodology, design documents, specifications, or any other document necessary in fulfillment of this MSA.

(c) SCRB shall interface with the System Integrator, to provide the required information, clarifications, and to resolve any issues as may arise during the execution of the CCTNS 2.0 Project.

(d) SCRB shall provide requisite data related to its functioning, facilitate obtaining of approvals from various governmental agencies, in cases, where the intervention of SCRB is proper and necessary.

4.7 System Integrator's Team

(a) System Integrator shall provide and deploy personnel on the site for carrying out the work, only those manpower resources who are skilled and experienced in their respective areas, with equal or higher qualification prescribed in Section 2.7 - Technical Evaluation Criteria of Volume – I of this RFP and Section 12 - Resource Requirement of Volume - II of this RFP and who are competent to execute or manage/ supervise the work in a proper and timely manner.

(b) The System Integrator would keep SCRB updated with the details of the staff deployed on the Project. The System Integrator will ensure that the roster schedule of all deployed manpower for each day at the required locations is made available to SCRB for view by authorized SCRB Official. No change to the deployed manpower shall be done by the System Integrator without written approval from SCRB except where such removal and/or replacement becomes necessary due to exceptional circumstances like disability, resignation, termination, death, etc. of the resource.

In any case, the provisions in the undertaking in Annexure 8.4 (3)(d) (Undertaking of Key Personnel proposed for the Project) of Volume I of the RFP shall apply.

(c) SCRB may at any time request the System Integrator to remove from the work / site the System Integrator's representative or any person(s) deployed by the System Integrator for professional incompetence or negligence or for being deployed for work for which he/she is not suited. The System Integrator shall accede to SCRB's request and shall not again deploy any person so objected to on the work or on the sort of work in question (as the case may be) without the written consent of SCRB.

(d) The System Integrator shall maintain backup staff and shall promptly provide replacement of every person removed, pursuant to this section, with a substitute who is equally competent or higher in competence from the pool of backup personnel.

(e) In case of change of any staff, the System Integrator 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. The

System Integrator shall also ensure that such a change does not adversely impact the quality and timelines of the Project.

5. Project Management

5.1 Approvals and Required Consents

(a) The parties shall co-operate to procure, maintain and observe all relevant and customary regulatory, corporation and governmental licenses, clearances and applicable approvals (hereinafter the "Approval") necessary for the System Integrator to provide the Services. The costs of such approvals and required consents shall be borne by the System Integrator.

(b) SCRB shall facilitate the System Integrator in obtaining the Required Consents wherever SCRB intervention is relevant and necessary. The System Integrator shall, however, not be relieved of its obligations to provide the Services and to achieve the service levels even until the Required Consents/ Approvals are obtained if and to the extent that the System Integrator's obligations are dependent upon such Required Consents/ Approvals.

5.2 Reporting Progress

(a) System Integrator shall nominate a Project Manager who would be a single-point contact for SCRB for monitoring day-to-day progress on the Project. The Project Manager would be required to interact regularly with SCRB to address issues or provide updates on the Project progress. To facilitate this interaction, SCRB Team would be constituted by Additional Director General of Police (ADGP), State Crime Records Bureau. The members of this SCRB team will have clearly defined roles. The System Integrator's Project Manager shall interact with the respective team members of SCRB for the project. The Project Manager shall be allocated full-time for the Project and will be stationed at Chennai atleast till the time of Project Go-Live

(b) The System Integrator agrees not to change its Project Manager without consent from SCRB. In the notified and approved absence of System Integrator's Project Manager, the System Integrator shall appoint an alternate resource on the Project for the role of the Project Manager.

(c) Review meetings will be held with SCRB to take stock of the progress made in the Project and discuss any issues / challenges being faced by the teams. All-important team members of the System Integrator involved during that stage of the Project will be present for these review meetings. Apart from the proposed review meetings, SCRB may schedule any other meetings from time to time. The selected System Integrator should ensure that the relevant team members are available for any such meetings scheduled by SCRB. SCRB shall draw the minutes of these meetings to record key proceedings and decisions of these meetings.

(d) Weekly status reports on the progress made during previous week, key activities planned in next week, progress against planned milestones, issues and escalations, if any etc. shall be submitted to the SCRB by the System Integrator's Project Manager during the entire duration of Contract.

(e) The System Integrator agrees that SCRB may change the periodicity of such reports. Formats for such reporting will be discussed and agreed with SCRB at the commencement of this MSA.

(f) In case the progress of Project falls behind schedule or does not meet the desired requirements for reasons solely and entirely attributable to the System Integrator, the System Integrator shall deploy extra manpower, resources, infrastructure to make up the progress or to meet the requirements at no additional cost to SCRB.

5.3 Notices

(a) All notices, requests, demands and other communications under this MSA or in connection herewith shall be given to or made upon the respective parties as follows:

To System Integrator:

_____

To SCRB:

Additional Director General of Police

State Crime Records Bureau

95, Greenways Rd, MRC Nagar, Raja Annamalai Puram,

Chennai, Tamil Nadu 600028

Or to such other person or addresses as any of the parties shall have notified to the others.

(b) All notices, requests, demands and other communications given or made in accordance with the provisions of this MSA shall be in writing in person or by letter, fax or email.

(c) Any notice or other document shall be deemed to have been delivered to the other Party

i. On the date and time of delivery when delivered in person between the hours of 10.00 am and 6.00 pm at the address of the other Party set forth above or on the next working day thereafter if delivered outside such hours

ii. At the date and time of transmission, if sent by fax, provided the fax is accompanied by a confirmation of transmission,

iii. 3 Business Days from the date of posting if delivered by Post / Letter

iv. as and when it is sent from the designated email address of the Party as communicated in the MSA Section-Agreement Owners, of this Volume of the RFP if sent by email or other electronic communication

(d) Either Party to this MSA may change its address, telephone number, facsimile number, email address and nominated contact for notification purposes by giving the other reasonable prior written notice of the new information and its effective date.

5.4 Commencement and Duration of Service Level Agreement

1. A separate agreement shall govern the Service levels for the entire Project.
2. The Service Level Agreement shall be executed along with the MSA and commence from the effective date of the MSA and shall, unless terminated earlier in accordance with the terms hereof or thereof or unless otherwise agreed by the parties, expire on the date on which this MSA expires.
3. A Service Level Agreement (SLA) is included herein as a part of this document.

5.5 Use and Upkeep of Assets

During the term of this MSA the System Integrator shall: -

(a) take all reasonable and proper care of the Assets;

(b) Keep all the tangible Assets in good and serviceable condition (reasonable wear and tear excepted) and/or the intangible Assets suitably upgraded subject to the relevant standards as stated in Volume I and II of the RFP from the date the System Integrator takes control of and/ or first uses the Assets and during the entire term of the MSA.

(c) Ensure that any instructions or manuals supplied by the manufacturer of the Assets for use of the Assets and which are provided to the System Integrator will be followed by the System Integrator and any person who will be responsible for the use of the Assets; and

(d) Take such steps as may be recommended by the manufacturer of the Assets and notified to the System Integrator or as may be necessary to use the Assets in a safe manner; and

(e) Provide a well-prepared documentation for users in the form of a user's manual, a clear plan for training, educating and hand holding the users and shall form part of handholding phase until bringing up the users to use software solution with speed and efficiency; and

(f) Train the team identified by Department, which will be in place during handholding and will be responsible for trouble shooting all post-implementation and maintenance activities.

(g) To the extent that the Assets are under the control of the System Integrator, keep the Assets suitably housed and in conformity with any statutory requirements from time to time applicable to them; and

(h) Not, knowingly or negligently use or permit any of the Assets to be used in contravention of any statutory provisions or regulation or in any way contrary to law; and

(i) Use the Assets exclusively for the purpose of providing the services as appropriate; and

(j) Not sell, offer for sale, assign, mortgage, encumbrance, pledge, sub-let or lend out any of the Assets; and

(k) Use the Assets only in accordance with the terms hereof and those contained in the SLAs; and

(l) Maintain standard forms of comprehensive insurance including insurance for the Assets, data, software, etc. in the joint names of SCRB and the System Integrator, where SCRB shall be designated as the 'loss payee' in such insurance policies;

(m) Transfer the ownership of the Assets (not already with SCRB which shall include the solution and Software including the source code and associated documentation which is the work product of the development efforts involved in the Project) to SCRB at the appropriate time (in synchronization with the submission of Deliverables thereof by the System Integrator) or in accordance with the terms of this MSA; and

(n) Ensure the integration of the software with hardware to be installed and the existing Assets in SCRB, in SDC and DRC in order to ensure the smooth operations of the entire solution architecture to provide efficient services to all the users of the proposed System in an efficient and speedy manner; and

(o) Obtain a sign off from SCRB at each stage as it is essential to close each of the above considerations.

5.6 Insurance

1. The System Integrator should take a specific insurance policy from a Third party for the Project providing insurance coverage against loss of or damage to

   (a) equipment or Assets procured or developed in whole or in part for fulfillment of obligations under this MSA

   (b) the System Integrator's Assets and property used in the performance of the services, and

   (c) any documents prepared by the System Integrator in the performance of the services.

   (d) SCRB's liability and workers' compensation insurance in respect of the staff of the System Integrator/ System Integrator's team, in accordance with the relevant provisions of the applicable law, as well as, with respect to such staff, any such life, health, accident, travel or other insurance as may be appropriate; and

2. The System Integrator should also take an insurance policy for the complete project tenure to provide coverage for all risks including the following:

(a) Fire and Theft Policy

(b) Policy for loss or damage to assets due to Force Majeure events like earthquake, rioting, etc. of value equal to the cost of replacement of assets.

(c) Policy of insurance in respect of claims for personnel injury to or death of any person employed by the selected System Integrator and arising out of such employment.

3. The System Integrator shall bear all the statutory levies like customs, insurance, freight, etc. application on the goods during their shipment from respective manufacturing/ shipment site of the OEM to the port of landing.

4. All charges including transportation charges that may be applicable till the goods are delivered at the respective site of installation shall also be borne by the System Integrator.

5. The System Integrator during the Term of this Contract:

(a) shall take out and maintain, at his own cost but on terms and conditions approved by SCRB, insurance with financially sound and reputable insurers against the risks, and for the coverage, as specified above where SCRB shall be designated as the 'loss payee' in such insurance policies;

(b) shall pay all premium in relation thereto and shall ensure that nothing is done to make such insurance policies void or voidable

(c) at the SCRB's request, shall provide evidence to SCRB showing that such insurance has been taken and maintained and that the current premiums therefore have been paid.

5.7 Change of Quantities

SCRB will have the option to increase (as per solution requirement) or decrease (to any extent) the quantities of hardware/equipment/material to be supplied by the System Integrator on this Project. The change in scope of work (increase / decrease) will be governed by the Change Control Schedule mentioned "Change Control Schedule" in this Volume (Volume III) of the RFP. The Change of Quantity should be in compliant to The Tamil Nadu Transparency in Tenders Act 1998 and The Tamil Nadu Transparency in Tenders Rules, 2000 as amended from time to time.

5.8 Contract Amendments

No variation in or modification of the terms of the Contract shall be made by written amendment signed by both the parties i.e. the System Integrator and SCRB.

5.9 Ownership of Equipment

(a) The infrastructure procured by the System Integrator as part of the project shall be the assets of SCRB.

(b) The system software licenses should be procured in the name of SCRB during the Contract Period.

6. Project Acceptance

6.1 Audit, Access and Reporting

(a) The Parties shall comply with the Audit, Access and Reporting Schedule provided in Schedule - 5 to the MSA.

(b) SCRB may carry out routine, random and periodic audits and inspections, by itself or through authorized representatives of the Project / Services related documents, data, locations, accounts, information at its own expense and cost; SCRB, shall endeavor to minimize inconvenience and disturbance to the System Integrator in the process of such audits and inspections.

(c) SCRB may carry out non-timetabled audits necessary as a result of an act of fraud by the System Integrator, a security violation, or breach of confidentiality obligations by the System Integrator.

(d) The System Integrator shall provide SCRB, or its representatives reasonable access, including leased premises used for the Project, documents, records and systems reasonably required for audit and shall provide all such persons with routine assistance in connection with the audits and inspections. The SCRB shall have the right to copy and retain copies of any relevant records at its own expense and cost. The System Integrator shall extend full support to co-operate with them.

(e) In case the System Integrator is not able to meet the SLA requirement during the Pilot Roll out stage, SCRB may direct System Integrator to extend the "Application Stabilization phase for Pilot locations" and defer the "Acceptance of Pilot roll out" to till the time Service level baselines defined in Service level section are not met or reached to satisfactory level of SCRB.

(f) In case the System Integrator is not able to meet the SLA baselines, SCRB may direct System Integrator to extend the "Application Stabilization phase for Full Scale roll out" and defer the "Acceptance of Full Scale Roll out" till the time Service level baselines defined in Service level section are not met or reached to satisfactory level of SCRB.

(g) All such audits shall be conducted upon a reasonable prior notice which shall not be less than 30 days. SCRB shall ensure that SCRB's auditors agree to comply with the confidentiality obligations specified in this MSA and shall remain liable for non-performance or breach of such confidentiality obligations by its auditors.

6.2 Verification

SCRB, shall have the right, as shall be reasonably necessary, to verify, -

(i) the security, integrity and availability of all SCRB data processed, held or conveyed by the System Integrator on behalf of SCRB and the users and documentation related thereto;

(ii) that the actual level of performance of the Services is the same as specified in the Service Level Agreement;

(iii) that the System Integrator has complied with the relevant technical standards, and has adequate internal controls in place; and

(iv) the compliance of the System Integrator with any other obligation under the MSA and/or the Agreements.

6.3 Acceptance Criteria

All Deliverables on this Project shall be reviewed and accepted in accordance with the following procedure:

(a) Notification of readiness of the Deliverables shall be given by e-mail as well as printed on company letter head by the System Integrator

(b) Soft copy (by e-mail) and two (2) printed drafts of the Deliverable materials shall be submitted to the SCRB by the Project Manager of the System Integrator.

(c) SCRB will review the Deliverables and either accept the Deliverables or provide feedback on changes to be done in writing within a reasonable period of time.

(d) The System Integrator shall make the appropriate revisions and shall resubmit the updated final version to SCRB for their verification and feedback/acceptance.

(e) The System Integrator should strive to submit the Deliverables in parts for getting continuous feedback on the Deliverables. The System Integrator should also engage with SCRB on a continuous basis through meetings (weekly till 6 months after Go-live and fortnightly after this period) and periodic workshops to ensure that progress may be reviewed, and feedback provided from time-to-time.

(f) The System integrator should plan to submit the draft versions of Deliverables before the scheduled timelines to allow reasonable time for review and acceptance.

6.4 Final Testing and Certification

The Project shall be governed by the mechanism of final Acceptance testing and certification to be put into place by SCRB, guided by the following principles:

(a) SCRB reserves the right to nominate a technically competent agency ("Third Party Assessment and Acceptance Agency") for conducting final Acceptance testing and certification;

(b) Such Third Party Assessment and Acceptance Agency will lay down a set of guidelines following internationally accepted norms and standards for testing and certification for all aspects of Project development and implementation covering software, hardware and networking including the processes relating to the design of solution architecture, design of systems and sub- systems, coding, testing, business process description, documentation, version control, change management, security, service oriented architecture, performance in relation to compliance with SLA metrics, interoperability, scalability, availability and

compliance with all the technical and functional and non-functional requirements of this Agreement and the RFP;

(c) The testing will be done in 3 stages:

Stage 1: Assessment and Acceptance of Pilot

Once the system has been rolled out at the Pilot location (planned timelines is T + 5.5 months, where T is the date of signing of Contract), the System Integrator shall notify SCRB, so that the Pilot system may be assessed by SCRB's Third Party Assessment and Acceptance Agency. The Third-Party Agency would conduct various tests to assess the compliance of the Pilot with the requirements of this Agreement and the RFP. The shortcomings identified by the Agency in the Pilot rollout completed by the System Integrator will be notified by SCRB to the System Integrator at the earliest instance through an appropriate process to facilitate corrective action. All gaps identified shall be resolved by the System Integrator within timelines. This process shall be iterative till the Pilot rollout is 'Accepted' by the Third-Party Assessment and Acceptance Agency. The System Integrator agrees to take any corrective action required to remove all shortcomings. Only after the solution deployed by the System Integrator at the Pilot Site is 'Accepted' by the Third-Party Assessment and Acceptance Agency, then the system will be rolled out across the State.

Stage 2: Assessment and Acceptance of State-wide rollout

Once the System has been rolled out across the state post pilot Acceptance, the System Integrator will notify SCRB so that the state-wide system may be assessed by the SCRB's Third-Party Assessment and Acceptance Agency. The procedure adopted thereafter will be similar to the procedure adopted for Acceptance of pilot.

(a) SCRB may get the solution assessed periodically through a Third-Party Assessment and Acceptance Agency even after declaration of 'Go-live' in order to ensure continued success of the Project.

(b) The System Integrator commits to provide all the requisite support and co-operation to SCRB and the Third-Party Assessment and Acceptance Agency for the completion of this assessment.

(c) Such an involvement of and guidance by the Third-Party Assessment and Acceptance Agency shall not, however, absolve the System Integrator of the fundamental responsibility of designing, developing, installing, testing and commissioning the various components of the Project to deliver the Services in perfect conformity with this Agreement

(d) Irrespective of involvement of the Third-Party Assessment and Acceptance Agency for Acceptance testing and certification, the System Integrator agrees that the total responsibility for defect free operations of the System and of meeting the SLAs as laid out in this Agreement and this RFP.

Stage 3: Periodic Assessment and Acceptance during O&M

(a) SCRB may get the solution assessed periodically through a Third-Party Assessment and Acceptance Agency during O&M stage in order to ensure continued success of the Project.

(b) The System Integrator commits to provide all the requisite support and cooperation to SCRB and the Third-Party Assessment and Acceptance Agency for the completion of this assessment.

(c) Such an involvement of and guidance by the Third-Party Assessment and Acceptance Agency shall not, however, absolve the System Integrator of the fundamental responsibility of designing, developing, installing, testing and commissioning of the various components of the Project to deliver the Services in perfect conformity with this Agreement

(d) Irrespective of involvement of the Third-Party Assessment and Acceptance Agency for Acceptance testing and certification, the System Integrator agrees that the total responsibility for defect free operations of the System and of meeting the SLAs as laid out in this Agreement and this RFP.

7. Project Finances

7.1 Terms of Payment

(a) In consideration of the Services and subject to the provisions of the MSA and SLA, the System Integrator shall be eligible to receive payments in accordance with the Terms of Payment Schedule of the MSA.

(b) It is clarified here that SCRB will pay for the Services as stated in accordance with the Terms of Payment Schedule and SCRB would also calculate a financial sum and debit the same against the Terms of Payment as defined in the Payment Schedule as a result of the failure of the System Integrator to meet the service level defined in the Service Level Agreement, such sum being determined in accordance with the terms of the Service Level Agreement.

Except as otherwise provided for herein or as agreed between the parties in writing, SCRB shall not be required to make any payments in respect of the Services other than those covered by the Terms of Payment Schedule.

7.2 Invoicing and Settlement

1. The System Integrator will submit its invoices in accordance with the following principles:

   (a) Generally, and unless otherwise agreed in writing between the parties or expressly set out in this MSA or the Service Level Agreement, the System Integrator shall raise an invoice for successful delivery of Services on a milestone basis till Go-live and on a quarterly basis after Go-live as per the Payment Schedule defined in Terms of Payment Schedule in this Agreement.

   (b) The invoice shall be submitted along with the necessary approval/signoff/acceptance/ certification provided by the concerned parties for the respective Deliverables linked with the payment milestone, failing which SCRB reserves the right to reject the invoices.

   (c) Along with the invoice, the System Integrator is required to submit the Deliverables linked with the payment milestone in softcopy and hardcopy formats, as applicable failing which SCRB reserves the right to reject the invoices.

   (d) Any invoice presented in accordance with this Schedule shall be in a form agreed with SCRB.

2. Invoices shall be accurate and all adjustments (if any) to payments to be made to the System Integrator shall be applied to the next payment invoice of the System Integrator.

3. The System Integrator shall waive any charge for a service that is not invoiced within six months after the end of the month in which the Terms of Payment as stated in the Terms of Payment Schedule relating to such service are authorized or incurred, whichever is later.
4. Payment for invoices shall be made within 30 days of the receipt of correct and valid invoice by SCRB, which has to be upon completion of the said activities, and after obtaining the signoff from SCRB for the required Deliverables and is subject to penalties/ adjustments based on the System Integrator's performance. The penalties are imposed on the System Integrator as per the SLA criteria specified in Section 2.4 of the Service Level Agreement.
5. SCRB shall be entitled to delay or withhold payment of any invoice or part of it delivered by the System Integrator where
   (a) SCRB disputes such invoice or part of it provided that such dispute is bonafide.
   (b) SCRB disputes any previous invoice or part of it that it had not previously disputed under Clause 16 of this document provided that such dispute is bonafide.

The withheld amount in both the above cases shall be limited to that which is in dispute. The disputed amount in both the above cases shall be referred to the procedure as set out in Clause 16.

Any exercise by SCRB under this clause shall not entitle the System Integrator to delay or withhold provision of the services.

7.3 Prices and Tax

The prices should be mentioned without any qualifications whatsoever and should include all taxes as may be applicable in relation to the activities proposed to be carried out. It is mandatory that such charges wherever applicable/ payable should be indicated separately.

7.4 Currency of Payment

Payment shall be made in Indian Rupees only.

7.5 Tax

(a) SCRB shall be responsible for withholding taxes from the amounts due and payable to the System Integrator wherever applicable. The System Integrator shall pay for all taxes in connection with this MSA and SLAs.

(b) SCRB shall provide the System Integrator with the original tax certificate of any withholding taxes paid by SCRB on payments under this MSA. The System Integrator agrees to reimburse and hold SCRB harmless from any deficiency (including penalties and interest) relating to taxes that are its responsibility under this paragraph.

(c) In the event of any increase of the rate of taxes due to any statutory notification/s during the term of the MSA shall be borne by SCRB. In the event of any decrease of rate of taxes due to any statutory notification/s during the term of the MSA shall be passed on by System Integrator to SCRB.

(d) Any increase in Currency rate due to exchange variations shall be borne by the System Integrator.

(e) The parties shall cooperate to enable each party to accurately determine its own tax liability and to minimize such liability to the extent legally permissible. In connection therewith, the parties shall provide each other with (i) any resale certificates, (ii) any relevant information regarding use of out-of-state materials, equipment or services and (iii) any exemption certificates or information reasonably requested by the other party.

8. Breach and Rectification

8.1 Events of Default by the System Integrator and Breach of Contract

The failure on the part of the System Integrator to perform any of its obligations or comply with any of the terms of this MSA shall constitute an event of default on the part of the System Integrator. The events of default as mentioned above may include inter - alias the following

(a) The System Integrator has failed to adhere to any of the requirements of the MSA and the RFP, or if the System Integrator has fallen short of matching such standards/ targets as

SCRB may have designated with respect to any task necessary for the execution of the scope of work under this MSA and the RFP. The above-mentioned failure on the part of the System Integrator may be in terms of failure to adhere to timelines, standards, specifications, requirements or any other criteria as defined by SCRB in the MSA and the RFP.

(b) The System Integrator has failed to remedy a failure to perform its obligations in accordance with the specifications issued by SCRB despite being served with a default notice which laid down the specific deviance on the part of the System Integrator to comply with any stipulations or standards as laid down by SCRB.

(c) The System Integrator/ System Integrator's team has failed to comply with or is in breach or contravention of any applicable laws.

(d) If the System Integrator fails to comply with any final decision reached as a result of arbitration proceedings pursuant to Clause 16 on issuance of a notice of not less than thirty (30) days.

(e) If the System Integrator in the judgment of SCRB has engaged in corrupt or fraudulent practices in competing for or in executing this MSA

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

Where despite the issuance of a default notice to the System Integrator by SCRB the System Integrator fails to remedy the default to the satisfaction of SCRB, the same shall be considered breach of Contract. SCRB reserves the right to terminate the Contract or where it deems fit, issue to the defaulting party another notices to take corrective action or proceed to adopt such remedies as may be available to SCRB.

8.2 Termination

This MSA may be terminated under the following conditions:

8.2.1 Termination for Convenience

By SCRB - By giving the System Integrator not less than 30 (thirty) days written notice of termination;

1. SCRB may at any time terminate the Contract for any reason by giving the System Integrator a notice of termination that refers to this clause.
2. Upon receipt of the notice of termination under this clause, the System Integrator shall either as soon as reasonably practical or upon the date specified in the notice of termination:
    a. cease all further work, except for such work as SCRB may specify in the notice of termination for the sole purpose of protecting that part of the System already executed, or any work required to leave the site in a clean and safe condition;
    b. remove all System Integrator's Equipment from the site, repatriate the all System Integrator's, remove from the site any wreckage, rubbish, and debris of any kind;
3. in addition, the all System Integrator shall:
    a. deliver to SCRB the parts of the System executed by the all System Integrator up to the date of termination;
    b. to the extent legally possible, assign to SCRB all right, title, and benefit of the System Integrator to the System, or Subsystem, as at the date of termination, and, as may be required by SCRB.
    c. deliver to SCRB all non-proprietary drawings, specifications, and other documents prepared by the System Integrator as of the date of termination in connection with the System.

8.2.2 Termination for default

By SCRB: –

1. If System Integrator commits any material breach of any term of this RFP and which in the case of a breach capable of being remedied has not been remedied up to the satisfaction of SCRB, within 30 days of written notice to remedy the same;
2. If the System Integrator is not able to deliver the services as per the SLAs defined in this RFP which translates into Material Breach, then SCRB may serve 30 days written notice

for curing this Material Breach. In case the Material Breach continues, after the expiry of such notice period, SCRB will have the option to terminate this Agreement. Further, SCRB may offer a reasonable opportunity to the System Integrator to explain the circumstances leading to such a breach.

Change of Control at System Integrator Organization

- In the event that System Integrator (Bidder) undergoes such a change of control, SCRB may, as an alternative to termination, require a full Performance Guarantee for the obligations of System Integrator (Bidder) by a guarantor acceptable to SCRB. If such a guarantee is not furnished within 30 days of SCRB's demand, SCRB may exercise its right to terminate this Agreement in accordance with this Clause by giving 15 days further written notice to the System Integrator.
- The termination provisions set out in this Clause shall apply mutatis mutandis to the Service Level Agreement.

8.2.3 Termination for bankruptcy:

1. SCRB may serve written notice on System Integrator at any time to terminate this MSA with immediate effect in the event of a reasonable apprehension of bankruptcy of the System Integrator:

2. The System Integrator shall in the event of an apprehension of bankruptcy immediately inform SCRB, well in advance (at least 4 months) about such a development;

Termination shall be without prejudice to any other rights or remedies a party may be entitled to hereunder or at law and shall not affect any accrued rights or liabilities of either party nor the coming into force or continuation in force of any provision hereof which is expressly intended to come into force or continue in force on or after such termination.

8.3 Effects of Termination

(a) If SCRB terminates this Agreement pursuant to failure on the part of the System Integrator to comply with the conditions as contained in this Clause and depending on the

event of default, Performance Bank Guarantee furnished by System Integrator may be forfeited.

(b) The termination provisions set out in this MSA shall apply mutatis mutandis to the Service Level.

(c) Upon termination of this MSA, the parties will comply with the Exit management Schedule, as outlined in this MSA.

(d) Upon the expiration or termination of this MSA, System Integrator shall undertake the actions set forth in this MSA to assist SCRB to replace services as provided hereunder:

(i) In respect of System Integrator third party Intellectual Property Rights, the System Integrator undertakes to secure such consents or licenses for SCRB from such third parties as are necessary to enable SCRB or its replacement System Integrator (any other agency that is selected for maintaining the system in place of the System Integrator, if applicable) to receive services substantially equivalent to the Services hereunder.

(ii) The System Integrator shall transfer to SCRB, in accordance with the terms of this MSA, Assets or Deliverables including the software, if any, (and including any data, ownership, source code and associated documentation which is the work product of the development efforts involved in the Implementation of Project) in which SCRB has the right, title and interest and that is in the possession or control of the System Integrator.

(iii) In the event of this MSA being terminated (as mentioned in Section 8.2 or due to Force Majeure as mentioned in Section 9.4) earlier than the planned Contract period, the System Integrator shall be eligible to receive payments as described in the Payment Schedule for the work completed and approved by SCRB.

(iv) The System Integrator's team and/or all third parties appointed by the System Integrator shall continue to perform all their obligations and responsibilities as stipulated under this MSA, and as may be proper and necessary to execute the scope of work under the MSA in terms of this MSA, the RFP and System Integrator's Bid, in order to execute an effective transition and to maintain business continuity.

(v) In the event that SCRB terminates this MSA due to default or material breach of this MSA on the part of the System Integrator, then SCRB shall be entitled to invoke the Performance Bank Guarantee submitted for this Project and pursue such other rights and/or remedies that may be available to SCRB under law.

(vi) Notwithstanding anything contained herein above and without prejudice to the right to terminate this MSA, if the System Integrator fails to set up and operationalize the system at the Stations locations, SCRB may in its sole discretion, engage another agency/System Integrator to fulfill the remaining obligations (or part of the remaining obligations) as may be decided, at the risk and cost of the System Integrator. The additional cost incurred by SCRB shall be recoverable from the Performance Bank Guarantee or any amount payable or due to the System Integrator, and in case such Performance Bank Guarantee or amount is not adequate, the System Integrator shall make good the shortfall.

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

(viii) The action as provided in this clause shall not be construed or treated as waiver of any right of SCRB and the right to terminate this MSA shall subsist even if an action in accordance with this clause had been taken.

9. Protection and Limitation

9.1 Warranties

The System Integrator warrants and represents to SCRB that: -

(a) it has full capacity and authority and all necessary approvals to enter and to perform its obligations under this MSA;

(b) this MSA is executed by a duly authorized representative of the System Integrator;

(c) it shall discharge its obligations under this MSA with due skill, care and diligence so as to comply, with this MSA in its entirety.

(d) for the entire Contract/ Project Period on all the items supplied as per requirements of the MSA and the RFP, the System Integrator would give comprehensive and support for all hardware items supplied. The warranty would ensure that the goods/ articles would continue to comply to the Minimum Technical specifications as prescribed in Technical Qualification Proposal in Volume - I of this RFP for the entire duration of the Contract.

(e) all infrastructure procured by the System Integrator for this Project adheres to the minimum service level requirements. IT Infrastructure proposed by the System Integrator which will not meet the minimum service level requirements will be upgraded without any additional fee to SCRB.

(f) ensure adequate regular supply of spare parts needed for a specific type of machinery and equipment.

(g) none of the hardware items proposed for this Project are second-hand or used items.

(h) none of the hardware items proposed for this project shall be declared as “End of Sale”/ “End of Life” by the respective OEM in next two years as on date of submission of proposal.

(i) The System Integrator should ensure that the proposed hardware items are supported by the respective OEM during the entire contract period. If the product is not-supported by the OEM during the period mentioned for any reason, the System Integrator will be required to replace the product with a suitable higher alternate for which support is provided by the OEM at no additional cost to SCRB and without impacting the performance or timelines of the Project.

(j) all hardware items procured by the System Integrator for this Project is purchased within last two months from the date of deployment and documentary proof for OEM warranty and proof of purchase should be produced at the time of deployment of Hardware Items

(k) all hardware items procured by the System Integrator for this Project is ready and functional before commencing any kind of services

(l) all servers procured by the System Integrator for this Project is compatible with infrastructure at SDC and DRC.

(m) none of the hardware items for this Project would be pledged/mortgaged/liened by the System Integrator.

(n) With respect to all third-party products and services purchased by the System Integrator for SCRB in connection with the provision of the Services, System Integrator will pass through or assign to SCRB the available rights which System Integrator obtains from the manufacturers and/ or vendors of such products and services (including warranty and indemnification rights), all to the extent that such rights are assignable, but provided always that System Integrator shall on a best efforts basis endeavor to obtain the assignment of such rights for the benefit of SCRB.

9.2 Third Party Claims

(a) The System Integrator (the "Indemnifying Party") undertakes to indemnify SCRB, as the case may be, (the "Indemnified Party") from and against all losses, claims or damages on account of bodily injury, death or damage to tangible personal property arising in favour of any person, department or other entity (including the Indemnified Party) attributable to the Indemnifying Party's performance or non-performance under this MSA.

(b) The indemnities shall be subject to the following conditions, namely: -

(i) the Indemnified Party, as promptly as possible, shall inform the Indemnifying Party in writing of the claim or proceedings and provides all relevant evidence, documentary or otherwise;

(ii) the Indemnified Party shall, at the cost of the indemnifying party, give the Indemnifying Party all reasonable assistance in the defense of such claim including reasonable access to all relevant information, documentation and staff;

(iii) Provided that the Indemnified Party may, at its sole cost and expense, reasonably participate, through its State Government Pleader or otherwise, in such defense;

(iv) if the Indemnifying Party does not assume full control over the defense of a claim as provided in this clause, the Indemnifying Party may participate in such defense at its sole cost and expense, and the Indemnified Party will have the right to defend the

claim in such manner as it may deem appropriate, and the cost and expense of the indemnified party will be included in losses.

(c) The Indemnified Party shall not prejudice, pay or accept any proceedings or claim, or compromise any proceedings or claim, without the written consent of the Indemnifying Party.

(d) All settlements of claims subject to indemnification under this MSA shall: -

1) be entered into only with the consent of the Indemnified Party, which consent will not be unreasonably withheld and include an unconditional release to the Indemnified Party from the claimant or plaintiff for all liability in respect of such claim; and

2) include any appropriate confidentiality Agreement prohibiting disclosure of the terms of such settlement.

(e) The Indemnified Party shall account to the Indemnifying Party for all awards, settlements, damages and costs (if any) finally awarded in favour of the indemnified party, which are to be paid to it in connection with any such claim or proceedings.

(f) The Indemnified Party shall take steps that the Indemnifying Party may reasonably require to mitigate or reduce its loss as a result of such a claim or proceedings.

(g) in the event that the Indemnifying Party is obligated to indemnify the Indemnified Party pursuant to this clause, the Indemnified Party will be entitled to invoke the Performance Bank Guarantee, if such indemnity is not paid, either in full or in part, and on the invocation of the Performance Bank Guarantee, the Indemnifying Party shall be subrogated to all rights and defenses of the Indemnified Party with respect to the claims to which such indemnification relates.

9.3 Limitation of Liability

(a) Neither party shall be liable to the other party for any indirect or consequential loss or damage (including loss of revenue and profits) arising out of or relating to the Contract.

(b) Except in the case of Gross negligence or Willful misconduct on the part of the Selected System Integrator/System Integrator's team or on the part of any person or firm acting on

behalf of the System Integrator executing the work or in carrying out the services, the System Integrator, with respect to damage including to property and/or Assets/ Sales/ Revenue of SCRB or of any of SCRB's vendors shall regardless of anything contained herein, will be liable for any direct loss or damage that is less than or equal to (A) the Total Bid Value of the Project or (B) the proceeds the System Integrator may be entitled to receive from any insurance maintained by the System Integrator to cover such a liability, whichever of (A) or (B) is higher.

For the purposes of this clause, "Gross Negligence" means any act or failure to act by a party which was in reckless disregard of or gross indifference to the obligations of the party under the MSA and which causes harmful consequences to life, personal safety or real property of the other party which such party knew, or would have known if it was acting as a reasonable person, would result from such act or failure to act. Notwithstanding the foregoing, Gross Negligence shall not include any action taken in good faith for the safeguard of life or property.

Gross Negligence will also mean- Loss of SCRB's revenue due to malfunctioning of system deployed by System Integrator as a part of this project

"**Willful Misconduct**" means an intentional disregard of any provision of this MSA which a party knew or should have known if it was acting as a reasonable person, would result in harmful consequences to life, personal safety or real property of the other party but shall not include any error of judgment or mistake made in good faith.

(c) There shall be no limitation of liability in respect of the System Integrator in case of any damages for bodily injury (including death) and damage to real property and tangible personal property, other than as applicable under the relevant laws.

(d) This MSA does not grant or create any rights, benefits, claims, obligations or causes of action in, to or on behalf of any person or entity (including any third party) other than between the respective parties to this MSA, as the case may be.

(e) Any claim or series of claims arising out of or in connection with this MSA shall be time barred and invalid if legal proceedings are not commenced by the relevant party against the other party within a period of 3 years from the date when the cause of action first

arose or within such longer period as may be permitted by applicable law without the possibility of contractual waiver or limitation.

(f) SCRB shall be entitled to claim the remedy of specific performance under this MSA.

This right to claim for any damage shall be without prejudice to other rights and remedies available to SCRB under the contract and law

SCRB shall be entitled without prejudice to its other rights and remedies, to deduct from the price payable to the System Integrator and also to encash the PBG, provided the total amount recovered does not exceed the Total Contract Value or the insurance cover, whichever is higher

9.4 Force Majeure

9.4.1 Definition of Force Majeure Event

A Force Majeure Event shall mean the occurrence of any event (after the Effective Date) which is beyond the reasonable control and influence of a party and which causes a delay and/or inability for that party (the Affected Party) to fulfill its obligations under this Contract including:

1. an act of hostilities, or warlike operations (whether declared or undeclared), invasion, armed conflict, or act of foreign enemy, and civil war occurring within India;
2. lockout, embargo, import restriction, port congestion, lack of usual means of public transportation and communication, industrial dispute, shipwreck, shortage or restriction of power supply, epidemics, quarantine, and plague;
3. earthquake, landslide, volcanic activity, fire, tidal wave, typhoon or cyclone, hurricane, storm, lightning, or other inclement weather condition, nuclear and pressure waves, or other natural or physical disaster;
4. a revolution, riot, insurrection, civil commotion, sabotage, or terrorism within India, by persons other than the personnel of the selected System Integrator.
5. any strike or industrial action that is not solely restricted to personnel of the selected System Integrator.

6. storm, tempest, flood or nuclear, chemical or biological contamination of the Site unless the source or cause of such cases is the result of actions and/or omissions of the System Integrator;
7. pressure waves cause by devices travelling at supersonic speeds; and
8. Fire caused by reason of any of the events listed above;

But regardless of the extent to which the above conditions in the first paragraph of this Section are satisfied, Force Majeure shall not include:

1. a mechanical breakdown; or
2. weather conditions which should reasonable have been foreseen by the Affected Party claiming a Force Majeure Event and which were not unusually adverse; or
3. non-availability of or increase in the cost (including as a result of currency exchange rate fluctuations) of suitably qualified and experienced manpower, equipment or other resources, other than the non-availability of equipment due to an event that affected SI, would have come within the definition of Force Majeure event under Section 9.4.1; or
4. economic hardship or lack of money, credit or markets. Or
5. events of physical loss, damage or delay to any items during marine, air or inland transit to the Site unless the loss, damage or delay was directly caused by an event that affected System Integrator, would have come within the definition of Force Majeure Event under Section 9.4.1; or
6. late performance or other breach or default by the SI (including the consequences of any breach or default) caused by the acts, omission or default would have come within the definition of Force Majeure Event under Section 9.4.1 if it had happened to the System Integrator hereunder; or
7. a breach or default of this Contract (including the consequences of any breach or default) unless it is caused by an event that comes within the definition of Force Majeure event under Section 9.4.1; or
8. the occurrence of a risk that has been assumed by a Party to this Contract; or

9. any strike or industrial action that is solely restricted to the System Integrator Personnel, or

10. the negligence or willful recklessness of the SI,

9.4.2 Limitation on the definition of Force Majeure Events

Any event that would otherwise constitute a Force Majeure Event pursuant to Section 9.4.1 shall not do so to the extent that the event in question could have been foreseen or avoided by the Affected Party using reasonable bona fide efforts, including, in the case of the SI, obtaining such substitute goods, works, and/or services which were necessary and reasonable in the circumstances (in terms of expense and otherwise) for performance by the SI of its obligations under or in connection with this Contract

9.4.3 Claims for Relief

(a) If due to a Force Majeure Event a Party is prevented in whole or in part from carrying out its obligations under this Contract, such Party shall notify the other Party accordingly (Force Majeure Notice). The Affected Party shall not be entitled to any relief for or in respect of a Force Majeure Event unless it has notified the other Party in writing of the occurrence of the Force Majeure Event as soon as reasonably practicable and in any event within seven (7) days after the Affected Party knew, or ought reasonably to have known, of the occurrence of the Force Majeure Event.

(b) Each Force Majeure Notice shall

(i) fully describe the Force Majeure Event;

(ii) specify the obligations affected by the Force Majeure Event and the extent to which the Affected Party cannot perform those obligations;

(iii) estimate the time during which the Force Majeure Event will continue; and

(iv) specify the measures proposed to be adopted to remedy or minimize the effects of the Force Majeure Event.

(c) Following issuance of the Force Majeure Notice and while the Force Majeure Event continues:

(i) the obligations which cannot be performed because of the Force Majeure Event will be suspended and the Affected Party shall be released from such obligations under this Contract; and

(d) The suspension of performance shall be of no greater scope and of no longer duration than is reasonable required by the Force Majeure Event.

9.4.4 Mitigation of Force Majeure Events

Upon receipt of a Force Majeure Notice, each Party shall:

(a) remedy or minimize the effects of the Force Majeure Event to the extent reasonably practicable; and

(b) take all action reasonably practicable to mitigate any loss suffered by the other Party as a result of the Affected Party's failure to carry out its obligations under this Contract;

9.4.5 Resumption of Performance

When the Affected Party can resume performance of its obligations under this Contract, it shall give to the other Party written notice to that effect and shall promptly resume performance of its obligations under this Contract.

9.4.6 Termination upon subsistence of Force Majeure Event

If any Force Majeure Event subsists for a period of sixty (60) days or more within a continuous period of three hundred sixty-five (365) days, either Party may terminate this contract by giving the other Party thirty (30) Days written notice. On termination of this Contract under this Section 9.4.6, all consequences of Termination set out at Section 8.3 shall apply.

9.5 Confidentiality

(a) SCRB may permit the System Integrator to come into possession of confidential public records as per the needs of the Project and the System Integrator shall maintain the highest level of secrecy, confidentiality and privacy with regard thereto.

(b) Additionally, the System Integrator shall keep all the details and information confidential with regard to the Project, including systems, facilities, operations, management and maintenance of the systems/ facilities to the extent necessary/required as per regulations/law.

(c) SCRB shall retain all rights to prevent, stop and if required take the necessary punitive action against the System Integrator regarding any forbidden disclosure.

(d) The aforesaid provisions shall not apply to the information which is: -

(i) already in the public domain;

(ii) which has been received from a third party who had the right to disclose the aforesaid information; and

(iii) is required to be disclosed by the receiving party under the compulsion of law, or by order of any court or government or regulatory body to whose supervisory authority the receiving party is subject;

(iv) independently developed by receiving party without the use of Confidential Information and without the participation of individuals who have had access to Confidential Information;

(e) This clause shall survive the expiry or earlier termination of this MSA and apply mutatis mutandis to SCRB on any information shared by the System Integrator.

9.6 Data Protection

(a) The System Integrator will comply with the directions issued from time to time by SCRB and the standards related to the security and safety, insofar as it applies to the provision of the Government services.

(b) The System Integrator shall also comply with IT security and standards defined in the MSA and the RFP.

(c) The System Integrator shall endeavor to report forthwith in writing to SCRB all identified attempts (whether successful or not) by unauthorized persons either to gain access to or interfere with SCRB data, facilities or confidential information.

(d) The System Integrator shall report in writing to SCRB any act or omission which it is aware that could have an adverse effect on the safety and information technology security of the Project's facilities.

10. Intellectual Property Rights

(a) **Products and fixes:** All products and related solutions and fixes provided pursuant to this work order shall be licensed according to the terms of the license Agreement packaged with or otherwise applicable to such product. System Integrator would be responsible for arranging any licenses associated with products.

(i) "**Product**" means any computer code, web-based services, or materials comprising commercially released, pre-release or beta products (whether licensed for a fee or no charge) and any derivatives of the foregoing which are made available to SCRB for license which is published by product owner or its affiliates, or a third party.

(ii) "**Fixes**" means product fixes that are either released generally (such as commercial product service packs) or that are provided when performing services (such as workarounds, patches, bug fixes, beta fixes and beta builds) and any derivatives of the foregoing.

(b) SCRB shall retain exclusive intellectual property rights to the software (including source code of customizations/ enhancements/ amendments done), forms and the compilations that were developed or generated during the course of the Project to which SCRB has sovereign rights and nothing herein shall or will be construed or deemed to grant to the System Integrator any right, title, license, sub-license, proprietary right or other claim against or interest in, to or under (whether by estoppels, by implication or otherwise) to the aforesaid rights.

(c) All right, title and interest in and to, and ownership in, Proprietary Information of System Integrator, which is provided to SCRB for the Project including source code of any pre-existing application of the System Integrator, shall remain solely with the System Integrator. SCRB shall be entitled to use such System Integrator Proprietary Information only in connection with the services or to the extent necessary for the Project's normal operational, repair and maintenance purposes related to the services. SCRB shall not have the right to resale or redistribute such Proprietary Information of the System Integrator.

(d) However, any software that may be acquired from third parties during the term of the MSA and that which may be developed by the System Integrator during the course of the MSA

specifically for the Project shall not be considered as System Integrator's Proprietary Information by SCRB.

(e) Accordingly, all right, title and interest in and to, and ownership in, any modifications, enhancements, customizations of the System Integrator's pre-existing work that may have been done by the System Integrator during the course of the MSA specifically for the Project or as a result of Services rendered by the System Integrator hereunder shall remain solely with SCRB.

(f) All right, title and interest in and to, and ownership in, Proprietary Information of the Project which is provided to System Integrator by SCRB; and all modifications, enhancements and other derivative works of such Project Proprietary Information ("Proprietary Information"); any modifications, enhancements, customizations of the System Integrator's pre-existing work that may have been done by the System Integrator during the course of the MSA specifically for the Project or as a result of Services rendered by the System Integrator hereunder shall remain solely with SCRB. System Integrator shall be entitled to use such Proprietary Information only during the MSA term and only for the purposes of providing the services or to the extent necessary for System Integrator's normal operational, repair and maintenance purposes related to the services. SCRB shall retain ownership of all Intellectual Property Rights related to this Project Proprietary Information.

(g) With respect to ownership of the Deliverables, the parties agree that the following shall apply:

(i) Deliverables provided to SCRB by System Integrator during the course of its performance under this MSA, which includes but is not limited to software as defined in this MSA, in which, subject to the foregoing provisions of this clause, all right, title and interest in and to such Deliverables, shall, as between the System Integrator and SCRB, immediately upon creation, vest in SCRB. To the extent that the System Integrator Proprietary Information is incorporated within the Deliverables, the System Integrator and its employees engaged hereby grant to SCRB a worldwide, perpetual, irrevocable, non-exclusive, transferable, paid-up right and license to use, copy, modify (or have modified), transport to SCRB's facilities, and prepare from them, use and copy derivative works for the benefit of and internal use of SCRB, of such System

Integrator Proprietary Information. SCRB's rights pursuant to the preceding sentence include the right to disclose such System Integrator Proprietary Information to third party contractors solely for use on the Project provided that all such third-party contractors execute, deliver and comply with any customary confidentiality and non-disclosure Agreements reasonably required by SCRB.

(h) SCRB hereby grants to the System Integrator a non-exclusive right and license to access and use the Stations and information solely for the purpose of providing services on this Project. Subject to conditions mentioned in this clause, such right and license shall terminate upon the expiration or termination of this MSA.

(i) Without limiting the generality of Clause 10(b) and except to the extent otherwise expressly agreed by the parties to this MSA in writing, nothing contained in this MSA shall or will be construed or deemed to grant to the System Integrator any right, title, license or other interest in, to or under (whether by estoppels, by implication or otherwise) any logo, trademark, trade name, service mark or similar designations of SCRB or its respective affiliates/nominees or any confusingly similar designations of SCRB.

(j) Subject to any sole or exclusive rights granted by SCRB to a third party prior to the effective date, SCRB grants to the System Integrator in their performance of Services for SCRB, non-exclusive, paid-up, royalty-free right and license during the term of this MSA, but not the right to sub-license, to use SCRB data including the right to copy, perform, display, execute, reproduce, modify, enhance and improve SCRB data to the extent reasonably necessary or useful for the provision of Services hereunder.

(k) System Integrator shall not use SCRB data to provide services for the benefit of any third party, as a service bureau or in any other manner.

(l) System Integrator shall indemnify, defend and hold harmless SCRB and their staff, from and against any and all losses arising from claims by third parties that any Deliverable (or the access, use or other rights thereto), any equipment, software, information, methods of operation or other intellectual property created by System Integrator pursuant to this MSA, or the SLAs or a Project Engagement Definition under the MSA (i) infringes a copyright enforceable in India, (ii) infringes a patent issued in India, or (iii) constitutes

misappropriation or unlawful disclosure or use of another Party's trade secret under the laws of the India (collectively, "Infringement Claims"); provided, however, that this will not apply to any Deliverable (or the access, use or other rights thereto) created by

(i) SCRB by itself or through other persons other than System Integrator;

(ii) Third parties (i.e., other than System Integrator) at the direction of SCRB.

(m) SCRB shall have no liability or obligation to the System Integrator under Clause 10(g) above to the extent the Infringement Claim is based upon any use of the equipment, software, information, methods of operation or other intellectual property (or the access, use or other rights thereto) for the benefit of any party (including any use by System Integrator or its nominees outside the scope of the Services) other than for the Project.

(n) Notwithstanding any provisions of this MSA to the contrary, the foregoing remedies constitute the parties' sole and exclusive remedies and each party's entire liability, with respect to Infringement Claims.

(o) Upon the expiration or any termination of this MSA, System Integrator shall undertake the actions set forth below in this clause to assist SCRB to procure replacement services equivalent to Services provided hereunder.

(i) Further the System Integrator undertakes to negotiate in good faith with SCRB and any relevant replacement System Integrator in respect of commercial terms applying to all System Integrator’s Intellectual Property Rights and which SCRB and any relevant replacement System Integrator require to enable to provide or receive services substantially equivalent to the Services hereunder.

(ii) In respect of System Integrator third party Intellectual Property Rights, System Integrator undertakes to assist SCRB to secure such consents or licenses from such third parties as are necessary to enable the Project to receive services substantially equivalent to the Services hereunder. The obligations of the System Integrator under this clause shall be considered part of the Services performed by the System Integrator under the obligations contained in the Exit Management Schedule.

11. Non-Solicitation

Neither party will, without the consent of the other party, employ or offer to employ (whether under a Contract of Service or under a Contract for Services) any person engaged or previously engaged by the other in a technical or managerial capacity in relation to the Project, during the subsistence of this MSA.

12. Change of Control

(a) In the event of a change of control of the System Integrator during the term, the System Integrator shall promptly notify SCRB of the same.

(b) The Contract with the System Integrator will get transferred to the surviving entity. In the event that the net worth of the surviving entity is less than that of System Integrator prior to the change of control, SCRB may within 30 days of becoming aware of such change in control, require a replacement of existing Performance Bank Guarantee furnished by the System Integrator from a guarantor acceptable to SCRB. The value of Performance Bank Guarantee, if required to be revised, would be decided by SCRB at that time.

(c) If such a guarantee is not furnished within 30 days to SCRB requiring the replacement, or the surviving entity unable to execute the Contract in its fullest, SCRB may exercise its right to terminate the SLA and/ or this MSA within a further 30 days by written notice, to become effective as specified in such notice.

(d) Pursuant to termination, the effects of termination as set out in Clause 8.3 of this MSA shall follow.

For the avoidance of doubt, it is expressly clarified that the internal reorganization of the System Integrator shall not be deemed an event of a change of control for purposes of this clause unless the surviving entity is of less net worth than the predecessor entity.

13. Publicity

Neither party shall use any name, mark or symbol of the other in any publicity release or advertising material or for any other purpose whatsoever without securing the prior written consent of the other. Neither party shall use the other party's name or refer to the other party directly or indirectly in any media release, public announcement or public disclosure relating to

this MSA or their subject matter, including in any promotional or marketing materials, customer lists, referral lists or business presentations without written consent from the other party for each such use or release.

14. Severability and Waiver

If any provision of this MSA or the SLAs, or any part thereof, shall be found by any court or administrative body of competent jurisdiction to be illegal, invalid or unenforceable the illegality, invalidity or unenforceability of such provision or part provision shall not affect the other provisions of this MSA or the SLAs or the remainder of the provisions in question which shall remain in full force and effect. The relevant Parties shall negotiate in good faith in order to agree to substitute for any illegal, invalid or unenforceable provision a valid and enforceable provision which achieves to the greatest extent possible the economic, legal and commercial objectives of the illegal, invalid or unenforceable provision or part provision within 7 days.

Failure to exercise or enforce and delay in exercising or enforcing on the part of either Party to this MSA or the SLAs of any right, remedy or provision of this MSA or the SLAs shall not operate as a waiver of such right, remedy or provision in any future application nor shall any single or partial exercise or enforcement of any right, remedy or provision preclude any other or further exercise or enforcement of such right, remedy or provision or the exercise or enforcement of any other right, remedy or provision.

Forbearance, indulgence or relaxations by any party at any time to require performance of any provision of this MSA shall not in any way affect, diminish or prejudice the right of such party to require performance of that provision and any waiver by any party or any breach of any provisions of this MSA shall not be construed as a waiver or an amendment of the provisions itself, or a waiver of any right under or arising out of this MSA.

15. Non-Assignment

(a) System Integrator shall not sub-contract the following on this Project:

(i) Application development / maintenance including all components of the application including web-portal, Helpdesk & Reporting Solution

(ii) Data Migration

(iii) Data Centre management / Disaster Recovery Center Management

(iv) Hardware procurement, deployment and commissioning

(v) Helpdesk Operations

(vi) Project management.

(b) System Integrator shall not sub-contract any work to be performed under this MSA without SCRB's prior written consent and approval.

(c) Even in case of appointment of any sub-contractors, System Integrator shall be fully responsible or liable for performance of its obligations under this MSA.

(d) In case of any such appointment of sub-contractor, the System Integrator shall be the principal employer for all claims arising from the liabilities statutory or otherwise, concerning the sub-contractors.

(e) The System Integrator undertakes to indemnify SCRB from any claims on the grounds stated hereinabove.

16. Arbitration and Dispute Resolution

(a) The System Integrator shall make every effort to resolve amicably by direct informal negotiations, any dispute or difference whatsoever arising between the parties to the Agreement out of or relating to the construction, meaning, scope, operation or effect of the Agreement or validity of the breach thereof.

(b) If, after thirty (30) days from the commencement of such direct informal negotiations, SCRB and the System Integrator have been unable to resolve amicably a Contract dispute, either party may require that the dispute be referred for resolution to the formal mechanism.

(c) Arbitration for any such dispute shall be conducted in accordance with the provisions of Arbitration and Conciliation Act, 1996 or any statutory modification or re-enactment thereof.

(d) All legal proceedings, if necessary, related to any of the parties shall be lodged in the court of appropriate jurisdiction at Chennai only.

(e) Any fact or condition, which may not have been mentioned in terms and conditions and may arise during the Contract Period, shall be decided as per the State Govt. policy/ rules. In case

rules/ policies do not provide any such situation, the issue will be referred for the arbitration as per the procedure mentioned in point c, above.

(f) The Arbitration and Conciliation Act 1996 and the rules there under and any statutory modification or reenactments thereof, shall apply to the arbitration proceedings.

17. Conflict of Interest

(a) The System Integrator shall hold SCRB's interests paramount, without any consideration for future work, and strictly avoid conflict of interest with other assignments or their own interests. If during the period of this MSA, a conflict of interest arises for any reasons, the System Integrator shall promptly disclose the same to SCRB.

(b) The System Integrator shall also cause its staff and sub-contractors not to engage either directly or indirectly, in any business or professional activities that would conflict with the activities assigned to them under or pursuant to this MSA.

18. Non-Benefit of Commissions, Discounts

The payment to System Integrator as mentioned in Payment Schedule in Volume II of RFP shall constitute the System Integrator's only payment in connection with this MSA. The System Integrator shall not accept for its own benefit any trade commission, discount or similar payment in connection with the activities pursuant to this MSA or in the discharge of obligations hereunder, and the System Integrator shall use its best efforts to ensure that any of the System Integrator's Staff and agents of either of them, similarly shall not receive any additional payment.

IN WITNESS WHEREOF the parties have, by duly authorized representatives set their respective hands on the date first above written

For System Integrator

Signature of the ……. System Integrator

Witness 1

Witness 2

For SCRB

Signature Signed for and on behalf of and by the order and direction of the Governor of Tamil Nadu

Witness 1

Witness 2

Service Level Agreement

(Draft)

The objective of this section is to provide the draft Service Level Agreement to be signed between the Authorized Representative of SCRB and the System Integrator.

THIS AGREEMENT is made this _____ day of _____ 20…

BETWEEN:

State Crime Records Bureau (SCRB) having its office at the ……. India hereinafter referred to as '**SCRB**', which expression shall, unless the context otherwise requires, include its permitted successors and assigns) of the one part;

AND

<***>**,** a Company incorporated under the *Companies Act, 1956/2013*, having its registered office at <***> represented by …… (Hereinafter referred to as '***System Integrator'*** which expression shall, unless the context otherwise requires, include its permitted successors and assigns) of the other part;

WHEREAS

A. SCRB and [_____] have entered into a Master Services Agreement dated [_____] (the "MSA").

B. In accordance with Clause [_____] of the MSA, SCRB and System Integrator wish to enter into this Service-Level Agreement ('Agreement/SLA') on the following terms.

1. General Provision of the Service Level Agreement

1.1 Definitions

Terms and expressions used in this Service Level Agreement shall have the meanings set out below in Clause 1.2.

1.2 Interpretations

In this Agreement, unless otherwise specified:

1) References to clauses, sub-clauses, paragraphs, Schedules and annexure are to clauses, sub-clauses, paragraphs, Schedules and annexure to this Agreement;
2) References to any statute or statutory provision include a reference to that statute or statutory provision as from time to time amended, extended, re-enacted or consolidated and to all statutory instruments made pursuant to it.
3) Words denoting the singular shall include the plural and vice-versa
4) Use of any gender includes the other genders;
5) A reference to any other document referred to in this Agreement is a reference to that other document as amended, varied, novated or supplemented at any time; and
6) All headings and titles are inserted for convenience only. They are to be ignored in the interpretation of this Agreement.

7) **'Acceptance'** means Acceptance of the proposed solution by SCRB after clearance by the 'Third Party Assessment and Acceptance Agency' deployed by the Department.

8) **"Business Day**" means all the days in calendar year

9) **"Clauses"** refers to Clauses of this Agreement. The words "include" and "including" shall not be construed as terms of limitation.

10) **"Company"** shall be construed so as to include any company, corporation or other body corporate, wherever and however incorporated or established

11) "**Contract"** means the Agreement entered into between SCRB and the "System Integrator" as recorded in the Contract form signed by SCRB and the "System Integrator" including all attachments and annexure thereto;

12) **"Contract Period"** means the time period from date of signing of Contract with System Integrator till 5 Years after Go-live or as further extended by SCRB.

13) "**Day**" means a period of 24 hours running from midnight to midnight. It means "calendar day" unless otherwise stated. Where, because of a difference in time zone, the calendar day in one country differs from another country, then the calendar day shall be deemed to be the calendar day applicable to India.

14) **"Deliverables"** means all the documents, milestones and activities related to the setting up and operations of project in SCRB, as defined in Volume – I & II of the RFP, and as required as per this MSA;

15) **"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;

16) **"End of Contract"** refers to the time when the Contract Period has ended

17) **"Go-live"** means the date as declared by SCRB on which the proposed solution becomes operational after successful conclusion of all acceptance tests to the satisfaction of SCRB or as provided in this RFP. Planned date of Go-live is 7 months from the date of signing of Contract

18) "**Herein**", "**Hereof**", "**Hereunder**" and similar words refer to this Agreement as a whole and not to any particular Clause, Schedule, unless otherwise explicitly stated.

19) "**Month**" means "calendar month" unless otherwise stated. Where, because of a difference in time zone, the calendar month in one country differs from another country, then the calendar month shall be deemed to be the calendar month applicable to India.

20) "**Proposal**"/ "**Bid**" means the documents in their entirety comprising of the pre-qualification Proposal, Technical and Commercial Proposal, clarifications to these, technical presentation/ demo submitted by the Bidder, in response to the RFP and accepted by SCRB,

21) "**RFP"/ "Tender**" means the Request for Proposal released vide Bid document ELCOT/ PROC/ OT/ 33384/ CCTNS 2.0 (SCRB)/ 2020-21 dated_____, and include all clarifications/addendums, explanations and amendments issued by SCRB in respect thereof

22) **"Service Level"** means the level of Service and other performance criteria which will apply to the Services as set out in the SLA parameters effective during the term of this SLA.

23) "**State-wide rollout"** refers to the day when the System Integrator completes the rollout of the new system at all locations across the state as per requirements of the RFP and is ready for acceptance testing by SCRB.

24) "**System Integration**" refers to the process through which the engaged business entity (firm/company) will design and build computing systems customized to the needs of SCRB as stated in this RFP by combining communication infrastructure, hardware and software products from one or more vendors. The hardware and software products may be new or existing systems and may be built afresh from scratch or packaged products.

25) "**System Integrator**"/ "**SI**" means the company with whom the contract has been entered into for providing Services as specified in this Master Service Agreement and shall be deemed to include the System Integrator's successors, representatives (approved by SCRB), their, executors, and administrators and permitted assigns, as the case may be, unless excluded by the terms of the Contract.

26) **"Time"** means Indian Standard Time

27) "**Total Contract Value"/ "Contract Value**" refers to the value finally agreed between SCRB and the System Integrator for the delivery of Services mentioned in the RFP (after negotiations with the selected System Integrator) which will be the maximum value payable to the System Integrator on this Contract.

28) "**Users**" refers to all SCRB staff who would be using the proposed System.

29) "**Workflow**" means the sequence of administrative or other processes through which a piece of work passes from initiation to completion.

30) "**Writing" and "Written**" mean "in documented form", whether electronic or hard copy, unless otherwise stated. Any reference to attorneys' fees shall include fees of the professional assistants of such attorneys.

1.3 Measurements and Arithmetic Conventions

All measurements and calculations shall be in the metric system and calculations done to 2 (two) decimal places, with the third digit of 5 (five) or above being rounded up and below 5 (five) being rounded down except in money calculations where such amounts shall be rounded off to the nearest Rupee.

1.4 Ambiguities within Agreement

In case of ambiguities or discrepancies within this Agreement, the following principles shall apply:

1. as between two clauses of this Agreement, the provisions of a specific clause relevant to the issue under consideration shall prevail over those in a general clause;
2. as between the provisions of this Agreement and the Schedules, the Agreement shall prevail, save and except as expressly provided otherwise in the Agreement or the Schedules; and
3. arithmetical errors shall be corrected, and the corrected figure shall be considered.
4. as between any value written in numerals and that in words, the lower of the two shall be considered.

1.5 Priority of Documents

The parties hereby expressly agree that for the purpose of giving full and proper effect to this Agreement, the MSA and this Agreement shall be read together and construed harmoniously. In the event of any conflict between the MSA and this Agreement, the provisions contained in the MSA shall prevail over this Agreement.

1.6 Structure

This SLA shall operate as a legally binding services Agreement specifying terms which apply to the parties and to the provision of the Services by the System Integrator to SCRB under this SLA and the MSA.

1.7 Objectives of the Agreement

The following are the objectives of the Project:

1. Provide enhanced tools for crime investigation, crime prevention, law and order maintenance and other regulatory functions:
    (a) Utilize IT for efficiency and effectiveness of core policing operations
    (b) Provide information for easier and faster analysis and trends
2. Create a national platform for sharing crime and criminal information and intelligence across the country in between state and central and external agencies.
3. Improved services for general public and other institutions such as:
    (a) Access to police services in a citizen-friendly manner
    (b) Provide fast, accurate and digital modes of service delivery

To meet the aforementioned objectives, the System Integrator will provide the Service levels in accordance with the performance metrics defined by SCRB and as more particularly described in Section 2.4 of this Agreement. Further, this SLA shall govern the provision of the contracted Services to SCRB after the Effective Date.

1.8 Scope of the Agreement

This Agreement encompasses the portion of the Project contracted to the System Integrator as covered in the scope of work in Volume I and II of the RFP. This Service Level Agreement (SLA) will do the following:

- Define objective performance metrics for the Services rendered by the System Integrator
- Establish framework for SLA change management
- Define parties covered by this Agreement

The following parties are obligated to follow the procedures as specified by this Service Level Agreement:

- SCRB
- System Integrator

1.9 Contact List

Additional Director General of Police (ADGP), State Crime Records Bureau will be the primary contact regarding operation of this Service Level Agreement (SLA) from SCRB. Similarly, an authorized signatory of the System Integrator will be nominated to be the primary contact regarding operation of this Service Level Agreement (SLA) from the selected System Integrator's side. The primary contact from both parties is referred to as the Principal Contact in this SLA. At the start date of the Agreement, the contact details of the Principal Contacts are:

SCRB Principal Contact:

Additional Director General of Police (ADGP)
State Crime Records Bureau (SCRB),
95, Greenways Rd, MRC Nagar, Raja Annamalai Puram,
Chennai – 600028, Tamil Nadu

System Integrator Principal Contact: _____

Any changes to the listed contacts must be communicated and updated prior to the change occurring to the Principal Contact of the other party.

1.10 Commencement and Duration of this SLA

This SLA shall commence on the date of signing of Agreement by SCRB and the System Integrator (hereinafter the 'effective date') and shall, unless terminated earlier in accordance with its terms or unless otherwise agreed by the parties, continue for a period of five years after "Go-live" of the Project.

1.11 Updating the Service Level Agreement

(i) This Service Level Agreement is not a fixed document to be produced once and used forever. Instead, it must be re-evaluated and updated as the work environment changes. As technology changes, the Services and systems covered by this Agreement and their performance expectations will change. This document may be reviewed and revised by mutual Agreement between SCRB and System Integrator. Changes to the Service Level Agreement may be required at other times to include new systems, change in operating hours, etc.

(ii) Any and all changes to the Agreement will be initiated in writing between SCRB and the System Integrator. The Service levels in this Agreement are considered to be standard for SCRB and will only be modified if both parties agree to an appended set of terms and conditions.

(iii)Any changes to the Service Level Agreement will be governed by the Change Control Schedule detailed in the MSA and the cost to update the Service Level agreement will be jointly decided and agreed between SCRB and System Integrator.

1.12 Document History

All revisions made to this document will be listed here in chronological order.

Version	Date	Description of Change

2. Scope of Services

2.1 Services Provided to SCRB by System Integrator

The System Integrator will provide services to SCRB on specified days as per the standards defined for each activity in the Service Level requirements detailed in Section 2.4 of this SLA.

2.2 Performance Review

Performance review of the Services rendered by the System Integrator will be done in Project review meetings that will be conducted weekly till 6 months after Go-live and fortnightly after this period till end of Contract. The Principal Contacts of both the Parties or their nominated representatives will attend these Project review meetings to discuss progress made on the project, priorities, service levels and system performance. Additional meetings may be held at the request of either SCRB or the System Integrator. The agenda for these meetings will at least cover:

(i) Service performance

(ii) Review of specific problems/exceptions and priorities

(iii)Review operation of the SLA and determine corrective action to overcome deficiencies.

2.3 Interpretation

Apart from the provisions as set out hereinabove, the terms and conditions stated in the MSA shall apply mutatis mutandis to this SLA. In the event of a conflict in interpretation of any clause in the MSA and the SLA, the provisions of the MSA shall prevail.

IN WITNESS WHEREOF the parties have by duly authorized representatives set their respective hands and seal on the date first above written in the presence of:

Witnesses:

Signed by: Signed for and on behalf of and by the order

and (Name and Designation)

direction of Additional Direction General of Police

Principal Contact of SCRB

Signed by: Signature of the……System Integrator

(Name and Designation)

(System Integrator)

2.4 Service Levels & Penalty Details

The SI may use the existing CA EMS tool/ new tool for SLA measurement of all the SLAs mentioned in this section. The SI may procure support for the existing CA EMS tool since the support for the current version in use has expired (perpetual licenses procured during CCTNS 1.0), OR, the SI may procure a new EMS tool and measure SLA using the same. The SI shall use the EMS tool and develop additional scripts (if required) to monitor and track all the SLAs defined in this section on a regular basis. The SI shall monitor all metrics related to Supply & Rollout of Hardware, Infrastructure and Software Application, UAT, Training and Operations where manual intervention may be required to measure the slippage from SLA. The SLAs will be subject to being redefined, to the extent necessitated by field experience at the Police Stations and other units and the development of technology practices globally. Such revisions in SLA calculation and monitoring would be made by SCRB in consultation with SI.

The SI shall submit the Performance Report on periodic basis to SCRB using CA EMS tool or new tool and will include the summary of all incidents reported and the associated SI performance for that period.

The SI shall also submit periodic MIS reports, reporting the activities periodically at SCRB locations including operator availability (as calculated by the CA EMS or new tool). The reporting shall cover all the reports required to monitor the SLAs detailed in the RFP.

1) The SI shall also submit these reports to PMU as and when required.

2) All reports (current period and historical) shall be accessible to the authorized officers within SCRB and PMU at any time.

3) The exact formats and the parameters for reporting shall be discussed jointly between the SI and SCRB.

There shall be a monthly meeting between representatives of the SI and SCRB to review the services being provided. The objective of the meeting will be to ensure that all relevant

information affecting service provision is exchanged. The service level review shall not be a substitute or replacement for normal informal dialogue.

Each service level review meeting agenda shall include the minimum following items:

1) A review of the service performance against agreed targets in the period since the last meeting.

2) The status of specific service issues raised or outstanding at the previous meeting.

3) A review of work-in-progress against long-standing service problems or issues to be resolved.

4) Any new problems or issues.

5) Identification of any discernable trends.

6) Any action points required for the next meeting.

7) Any longer-term plans required.

8) Any minor changes required to the services, service levels or the agreement.

2.4.1 Calculation of Service Availability

1) The availability of systems or services is a measure of the length of time the systems or services are available to SCRB and shall be assessed as the proportion of the Scheduled Working Hours of Service that a service is actually available, measured over each specified period.

2) Availability means that applications, hardware and servers for which the SI is responsible, are available for use at the end user points by all user groups. Loss of service availability (an "Outage") shall be deemed to have occurred when the system or a defined component of the system is unavailable.

3) SCRB may require services to be available outside Scheduled Hours of Service and at times and for reasons, which cannot be specified in advance. To cover this need, the SI shall agree to provide services of short duration outside Scheduled Hours of Service by prior arrangement at mutually agreed times.

4) The SI shall measure Service availability and data regarding system downtime shall be collected automatically by the SI using the EMS tool.

5) Service availability shall be reported on a regular basis. The figures for actual and planned service hours shall then be aggregated to calculate service availability over longer periods and to allow a rolling average to be calculated. Calculated service availability statistics shall be used as input to Quarterly Service Review Meetings between SCRB and SI.

6) If the SI fails to meet the Minimum Service Levels as reported on a monthly/quarterly basis for a Service Level, it shall be considered as Service Level violation.

7) The business hours are from 9 AM to 6 PM on all working days (Mon-Sat) excluding Public Holidays observed by the State.

2.4.2 Service Level Violation Penalty

Implementation Phase:

1) Penalty during Pilot Rollout Phase- the SI shall adhere to all the below mentioned Service Level for the locations where the new system will be rolled out.

2) If the performance of SI in respect of any parameter falls below the service baselines during pilot, a penalty shall be imposed for the breach as per the Service level subsection.

3) All penalties during the Pilot Rollout phase shall be accumulated on a monthly basis and shall be adjusted against the forthcoming payments milestone. The total maximum deduction by way of penalty shall not exceed 10% of the milestone payment value (without penalties) to be made for the milestone payment.

4) In case the SI is not able to meet the SLA requirement during the Pilot Rollout stage, SCRB may direct SI to extend the “Application Stabilization phase for Pilot locations” and defer the

"Acceptance of Pilot Rollout" till the time Service level baselines defined in Service level section are not met or reached to satisfactory level of SCRB.

5) After the Service baselines are met or reached to the satisfactory level of SCRB, SCRB shall give acceptance of Pilot Rollout.

6) Similar process as mentioned above shall be followed for Full Scale Rollout as well.

O&M Phase:

1) SI shall get 100% of the Contracted value if the service level metrics are fully complied. SI shall get lesser payment, if the performance of SI in respect of any parameter falls below the prescribed lower performance limit based on the Penalty clauses as mentioned in Section 2.4.6.

2) Unless stated otherwise, all penalties incurred will be accumulated for every month and total value corresponding to all penalties in this time period shall be adjusted against the payments to be made to the System Integrator in that quarter.

3) The total maximum quarterly deduction by way of penalty shall not exceed 25% of the quarterly payments (without penalties) to be made in that quarter.

Two consecutive quarterly deductions of 25% of the applicable fee on account of any reasons may be deemed to be an event of default and SCRB may terminate the contract as per Clause 8.2 of the MSA and the consequences as provided in Clause 8.3 of the MSA shall follow.

2.4.3 Severity Level

The severity level defines the conditions of categorizing any Problems/ Incidents/ Issues as High and Medium. Each category has an issue resolution time and a penalty attached to it in case of violation.

a. Classification of Priority level of assets:

SNo.	Priority 1 (P1)	Priority 2 (P2)
1	Desktop	Laser Printers

2	UPS & UPS Batteries	External HDD
3	Multi-Functional Printers	Electrical & Passive
4	Network Switch	Inverters
5	CCTNS 2.0 Application	

b. Resolution Time:

Description of Severity Levels	Resolution Time
Priority 1	8 Business Hours
Priority 2	16 Business Hours

c. Severity Level:

SNo.	Priority Level	Severity Level as per Contract
1	Priority 1	Medium
2	Priority 2	Low

d. Violations and associated Penalty:

The primary intent of penalties is to ensure that the system performs in accordance with the defined service levels. Penalties are not meant to be punitive or, conversely a vehicle for additional fees.

Penalty Calculations

The framework for penalties, as a result of not meeting the Service Level targets are as follows:

a. The performance will be measured for each of the defined service level metric against the minimum/ target service level requirements and the violations will be calculated accordingly.

b. The number of violations in the reporting period for each level of severity will be totaled and used for calculation of penalties applicable for each of the high, medium or low severity violations are mentioned below.

SNo.	Severity of Violation	Penalty per Violation (as % of respective payment period)
1	High – SDC/ DRC	1%
2	Medium – Client side Infra	0.5%
3	Low – Client side Infra	0.25%

2.4.4 Compliance to Timelines- Measured at completion of milestone Live

1) Any delay in the delivery of the project deliverables (solely attributable to the System Integrator) shall attract a penalty.

2) If the cumulative penalty reaches 10% of the total contract value, SCRB may invoke termination clause.

3) The penalty for default shall be deducted from the payment to be made for the respective milestone.

2.4.5 Security Breach SLA

Security of implemented system and the data contained therein is paramount for the success of this Project. Hence, the selected System Integrator shall take adequate security measures to ensure confidentiality, integrity and availability of the information. System Integrator is requested to note the following:

1) Failure to abide by any of the requirements during the Contract Period shall be interpreted as breach of security and breach of Contract.

2) In any circumstances, the selected System Integrator shall be fully held responsible for any security breach that may occur in the system during the period of Contract. The selected

System Integrator shall be required to perform a detailed root-cause analysis for the security breach and make necessary amends to ensure that no such incidents are repeated.

Note: - For any instance of security breach reported and proved during the duration of the contract, stringent measures will be taken by SCRB against the System Integrator, which may include both severe penalty and termination of contract.

2.4.6 Detailed Service Level

2.4.6.1 Hardware SLA

1. Station Hardware: Implementation Phase

The detailed service levels are mentioned below;

SNo.	SLA Description	Target Performance	Non-Compliance to SLA
1	Delay in supply of hardware to individual locations	Within 4 months, 2 months and 3 months respectively for the 3 Phases from the date of issuance of work order.	No Penalty
		For a delay of every one week from the stipulated time from the date of issuance of work order	1 % of the respective work order value capped to a maximum of 10 %
2	Delay in commissioning of equipment across all locations	Within 5 months, 2 months and 4 months respectively for the 3 Phases from the date of issuance of work order.	No Penalty
		For a delay of every one week from the stipulated time from the date of issuance of work order	1 % of the respective work order value capped to a maximum of 10 %

3	Delay in submission of the site commissioning report	Within 6 months,2 months and 5 months respectively for the 3 Phases from the date of issuance of work order	No Penalty
		For a delay of every one week from the stipulated time from the date of issuance of work order	1 % of the respective work order value capped to a maximum of 10 %
4	Delay in replacement of any device or other peripheral which was found to be defective by SCRB	Within 24 hours from the time of reporting /Commissioning of H/W	No Penalty
		Beyond 24 hours	5% of the value of the defective hardware or Rs. 1000/- whichever is lesser per day will be deducted.

2. Station Hardware: O & M Phase

SNo.	SLA Description	Measurement	Severity Level
1	Client Site – Support Performance	All incident that has an immediate impact on CCTNS 2.0 project at each site should be resolved within 8 business hours from the time call is received / logged whichever is earlier. This service level will be measured on a monthly basis for each implementation site. If resolution time exceeds 8 business hours, one additional instance would be considered	Medium

		for every 8 hours delay.		
		Number of instances per month per site	Violation for calculation of Penalty per month	
		>0 & <=4	1	
		>4 & <=8	2	
		>8 & <=12	3	
		>12	4	
		All incident that has an impact, while it is less critical, but can cause service to degrade should be resolved within 16 business hours from the time a call is received / logged whichever is earlier. This service level will be measured on a monthly basis for each implementation sites. If resolution time exceeds 16 business hours, one additional instance would be considered for every 16 hours delay.		Medium
		Number of instances per month per site	Violation for calculation of Penalty per month	
		>0 & <=4	1	

		>4 & <=8	2	
		>8 & <=12	3	
		>12	4	

Note: This SLA shall be calculated every month for all stations and number of instances per month per site is calculated and the corresponding number of violations for penalty is arrived. The penalty for the quarter will be the sum of penalties incurred in all three months in the respective quarter.

3. Data Center/ Data Recovery Center

The detailed service levels are mentioned below:

It is to be noted that:

The SLA parameters shall be monitored on a monthly basis as per the individual SLA parameter requirements. For SLA no. 1a & 1b below, if the infrastructure availability requirement is not met for consecutive weeks, penalty calculations shall be performed on weekly basis till the end of that quarter. For instance, if availability for week 3 in Quarter 1 falls below 99% & it continues to be the same in week 4, then violations will then be calculated on a weekly basis starting week 3 till the end of the quarter.

SNo.	SLA Parameter	Metric	Violations for calculation of penalty	Severity Level	Interpretation of Service Levels

1	**Infrastructure Availability**				
a	Production Systems (99% Min) The Complete SDC/DRC infrastructure - Any failure or disruption has a direct impact on the services in PS/HO, critical back office functions or direct impact on the organization. Availability up time in % (Scheduled operation time - System	< 99% & >= 98.5%	1	High	Production systems: All the CCTNS servers at the SDC and the CCTNS servers at the DRC will be treated as core application production systems. The downtime of the above servers will be added during the SLA period of three months and the % uptime will be calculated to decide the number of violation.
		< 98.5% & >= 98%	2		
		< 98%	3		

	down time) / (Scheduled Operation time) * 100 Scheduled operation time = Total operation time - Planned downtime Total operation time = 24x7x365	if the Availability in any month in the three - month period falls below 98%	one (1) additional violation will be added for each such month to the overall violations for this service level.		Downtime - If the services in the PS/HO are affected due to the failure of any hardware/ software, DB etc. that are supplied & commissioned by SI only. SLA applicable hours: 24x7x365
b	Non Production Systems & Non CCTNS Systems in Production (97% Min.) The Complete SDC/DRC infrastructure - Any failure or disruption has no direct impact on	< 97% & >= 96.5%	1	Medium	Non Production CCTNS Systems : Any back up servers at SDC/DRC will be treated as Non Production systems. The downtime of the above servers will be added during the SLA
		< 96.5% & >= 96%	2		
		< 96%	3		

	the services in PS/HO or critical back office functions. Availability up time in % (Scheduled operation time - System down time) / (Scheduled Operation time) * 100 Scheduled operation time = Total operation time - Planned downtime Total operation time = 24x7x365	if the Availability in any month in the three- month period falls below 96%	one (1) additional violation will be added for each such month to the overall violations for this service level.		period of three months and the % uptime will be calculated to decide the number of violation. Downtime - If the services in the PS/HO are affected due to the failure of the backup hardware/software , DB etc. that are supplied & commissioned by SI. SLA applicable hours: 24x7x365
2	**Infrastructure Performance**				
a	**Server CPU Utilization**	Peak CPU utilization crossing 70%, shall be less than 30 minutes (Except Batch Processing)		High	The SLA to be enforced based on the actual cause and impact on the services at PS/HO.
		Number of instances crossing 30 minutes over three-month Period			To be treated on case to case basis, if it is only due to the malfunctioning/failure of the

		instances >0 & <=3	1		hardware/software, DB etc. that are supplied & commissioned by SI. SLA applicable hours: 24x7x365
		instances > 3	2		
		if the number of instances in any month in the three-month period exceeds 3	one (1) additional violation will be added for each such month		
		In case of peak CPU utilization exceed 30 minutes, one instances will be considered for every 30 minutes (1 hour will be considered as 2 instances)			
b	**Server I/O Utilization**	Peak I/O utilization crossing 70%, shall be less than 30 minutes (Except Batch Processing)		High	The SLA to be enforced based on the actual cause and impact on the services at PS/HO. To be treated on case to case basis, if it is only due to the malfunctioning/failure of the
		Number of instances crossing 30 minutes over three-month Period			

		instances >0 & <=3	1		hardware/software, DB etc. that are supplied & commissioned by SI. SLA applicable hours: 24x7x365
		instances > 3	2		
		if the number of instances in any month in the three-month period exceeds 3	one (1) additional violation will be added for each such month		
		In case of peak I/O utilization exceed 30 minutes, one instances will be considered for every 30 minutes (1 hour will be considered as 2 instances)			
c	**Peak memory utilization**	Peak Memory utilization crossing 70%, shall be less than 30 minutes (Except Batch Processing)		High	The SLA to be enforced based on the actual cause and impact on the services at PS/HO. To be treated as case to case basis, if it is only due to the
		if the number of instances in any month in the three-month			

		period exceeds 3			malfunctioning/failure of the backup hardware/software, DB etc. that are supplied & commissioned by SI. SLA applicable hours: 24x7x365
		Instances >0 & <=3	1		
		Instances > 3	2		
		if the number of instances in any month in the three-month period exceeds 3	one (1) additional violation will be added for each such month		
		In case of peak memory utilization exceed 30 minutes, one instances will be considered for every 30 minutes (1 hour will be considered as 2 instances)			
3	**Datacenter -Support Performance**	Replacement of hardware equipment shall be done within 72 hours of notification by the State. These equipment's would have failed on four or	Each instance of non-meeting this service level will be	High	1. Notification will be issued to SI for replacement of the hardware if there is any violation in this parameter.

		more occasions in a period of less than three months or six times in a period of less than twelve months	treated as one (1) violation.		2. The replacement of hardware to be done within 72 hours after issue of notification.
		Up to date of the documentation of the design, modifications, enhancements, and fixes.	Each instance of non-meeting this service level will be treated as one (1) violation.	Medium	1. The documents to be submitted along with quarterly/half yearly SLA reports.
4	**Reporting - Availability & Performance Report**	Submission of monthly SLA compliance reports & MIS reports by fifth of the following month. Any non-compliance will be treated as one instance.	Each instance of non-meeting this service level will be treated as one (1) violation.	Medium	1. Monthly SLA report & MIS reports - fifth of every following month. 2. Quarterly SLA report & MIS reports -fifth of following month, on completion quarterly & half yearly operation.

2.4.6.2 Software SLA

The detailed service levels are mentioned below:

Please note that:

1. For SLAs, wherever slabs are mentioned, penalty will be cumulated over the different slabs.
2. For the purpose of calculation of uptime and issue resolution time, following times to be noted for SLAs:
   a. Police stations: 24 hours
   b. All other locations (Special units, Training centers) and Higher offices: 6AM-10PM
3. System Uptime, Application and Query response time SLAs shall be applicable for services delivered through any end user infrastructure
4. For SLAs in Web Application O&M phase and Change Control Note, SLA penalty shall be calculated on the basis of % of Software OPEX applicable to the particular period (every quarter i.e Total Software OPEX/ (5years x 4 quarters)
5. The critical defects in software as referred in SLA below shall refer to any defect which restricts significant number of users from accessing any particular feature of the application. The non-critical defects refer to defects which doesn't restrict majority of the users from accessing any feature of the application. The severity of defects shall be mutually decided by SI and SCRB

SNo.	Parameter	Formula	Baseline	Penalty	Measurement

1 Web Application: Implementation Phase

1	Delay in SRS completion		0.5 month	1 Week delay = 0.1% of Software CAPEX on a pro rata basis >1 week = 0.05% of Software CAPEX for every week of delay on a pro rata basis	Delay would be calculated as per timelines proposed in this RFP.
2	Delay in completing UAT		4 months		
3	Delay in Go-live in the state		6.5 months		
4	Implementation of Audit recommendations	-	Signed off timelines as agreed with SCRB (Only for defects or non-compliance identified during audits conducted by SCRB or its nominated agencies post the Go-live of the	0.1% of Software CAPEX on a pro rata basis for drop in service level by every 25%	Delay will be calculated against signed off timelines. Audit recommendations will be considered 'implemented' when accepted and approved by SCRB or its nominated agency

			solution) For any 'changes' as defined in the MSA, SLAs for Software Change Management will apply		

2 Web Application- O&M Phase:

SNo.	Parameter	Formula	Baseline	Penalty	Measurement
1	Average System Uptime including availability of infrastructure, all functionalities in the application, API/ Web Services etc. Time period for which the specified application, portal and other IT	System Uptime = {1-{[(A)/(B-C)]*100}} Where A = Time for which system is down B = Total Time C = Scheduled downtime	>99%	No Penalty	This includes Servers, storage, Backup, OS, Application, Portal, any other IT and non-IT infrastructure, their sub-components etc. that are deployed by the SI (either procured afresh by the SI or existing infrastructure of the Board being reused) as part of this project at the locations in question Excludes

	components are available to the internal and external users of the system averaged for all project locations	Total time will be calculated based on hours as mentioned in Point (2) above in this section	99% to 98%	0.1% of Software OPEX (respective quarter)	a) Scheduled downtime for planned maintenance as approved by SCRB b) Downtime of components that are to be provided under the SDC / DRC The SI will be required to schedule planned maintenance time with prior approval of SCRB. This will be planned outside working time. In exceptional circumstances, SCRB may allow the SI to plan scheduled downtime in the working hours. In any case this should not exceed 0.5% of the total time. System downtime for all components and sub-components will be calculated
			98% to 97%	0.2% of Software OPEX	

			Below 97%	For every 1 % drop in system availability below 97%, 0.1 % of Software OPEX shall be deducted on a pro rata basis over and above the penalty changes mentioned above.	by the EMS tool provided by the SI.
2	Application Response Time Average time taken to open any application page or submit forms or data by users including submission of any scanned documents (e.g., Submission of field visit reports, approval /	Sum of response time for all requests (or) Total number of requests in the period Response time = taken from pressing the 'submit' button and generation of acknowledgment of successful or	4 seconds At least 80 % of requests should be responded within 4 seconds	0.1% of Software OPEX for every 10% drop in service level on a pro rata basis 0.1% of Software OPEX for every 10% drop in service level on a pro rata basis	MIS reports generated from the system deployed, maintained and operated by the SI. Script based checking. SI to develop the scripts to aid measurement of this SLA. Random checks done by SCRB from various locations.

	rejection of requests, etc.)	unsuccessful submission by the system			
7	Query / Report Response Time Average Time the system takes to throw the results of a query / report after the user clicks on 'Submit' button	Sum of Time taken to throw results of all queries / reports in the period (or) Total number of queries / reports generated in the period Query (or) report response time = Time the system takes to throw the results of a query after the user clicks on 'Submit' button.	Simple reports: 10 seconds Medium complexity reports: 15 seconds High complexity reports: 20 seconds	0.1% of Software OPEX for every 10% drop in service level on a pro rata basis	Script based checking. SI to develop the scripts to aid measurement of this SLA. Random checks done by SCRB from various locations For ad-hoc reports, SCRB shall decide parameters for categorization of reports as simple, medium and complex during the implementation stage
3	Average Issue Resolution Time for Critical Defects	Sum of Resolution time of all call / Number of calls	2 working hours	0.1% Software OPEX for every 1 hour drop in service level on a prorata	Calculation of resolution time would be based on records / monitoring done at Helpdesk

	Resolution time is time from generation of ticket number as reported in Helpdesk			basis	
4	Average Issue Resolution Time for non-critical defects Resolution time is done from generation of ticket number to time of closure of call as reported in the Helpdesk	Sum of resolution time of all call / Number of calls	4 working hours On a case to case basis as agreed with SCRB at the time of implementation	0.1% Software OPEX for every 1 hour drop in service level on a pro rata basis 5% of Software Change Request value for drop in service level by every 25% on a pro rata basis	Calculation of resolution time would be based on records / monitoring done at Helpdesk
1	Delay in submission of Change Control Note				Delay will be calculated against signed off timelines

3 Web Application-Change Control Note:

				rata basis	
2	Delay in implementation of Change Request from signed off timelines in Change Control Note	-	Signed off timelines as agreed in Change Control Note	5% of Software Change request value for drop in service level by 25% on a pro rata basis	Delay will be calculated against signed off timelines

Non-Disclosure Agreement

THIS AGREEMENT is made on this the <***> day of <***> 20... at <***>, India.

BETWEEN

State Crime Records Bureau (SCRB) represented by ……. State Crime Records Bureau (SCRB) having its office at the ……. India hereinafter referred to as '**SCRB**', which expression shall, unless the context otherwise requires, include its permitted successors and assigns) of the one part;

AND

<***>**,** a Company incorporated under the *Companies Act, 1956/2013*, having its registered office at <***> represented by…… (hereinafter referred to as '***the System Integrator'*** which expression shall, unless the context otherwise requires, include its permitted successors and assigns) of the other part;

Whereas in order to pursue the mutual business purpose of this particular Project as (SCRB and M/s---------- recognize that there is a need to disclose to M/s---------- certain information, as defined in Para 1 below, of SCRB to be used only for the business purpose and to protect such Confidential Information from unauthorized use and disclosure.

In consideration of the other party's disclosure of such information, M/s---------- agrees as follows:

1. This Agreement will apply to all confidential and Proprietary Information disclosed by SCRB to the System Integrator, and other information which the disclosing party identifies in writing or otherwise as confidential within thirty days after disclosure to the System Integrator ("Confidential Information"). Information consists of certain specifications, documents, software, prototypes and/or technical information, and all copies and derivatives

containing such Information, that may be disclosed to the System Integrator for and during the purpose, which a party considers proprietary or confidential ("Information").

Information may be in any form or medium, tangible or intangible, and may be communicated/disclosed in writing, orally, or through visual observation or by any other means to the System Integrator by SCRB. Information shall be subject to this Agreement, if it is in tangible form, only if clearly marked as proprietary or confidential as the case may be, when disclosed to the System Integrator or, if not in tangible form, its proprietary nature must first be announced, and it must be reduced to writing and furnished to the System Integrator within thirty (30) days of the initial disclosure.

2. M/s_____ and SCRB hereby agreed that:

(a) The System Integrator shall use information only for the purpose, shall hold information in confidence using the same degree of care as it normally exercises to protect its own Proprietary Information, but not less than reasonable care, taking into account the nature of the information, and shall grant access to information only to its employees who have a need to know, but only to the extent necessary to carry out the business purpose of this Project, shall cause its employees to comply with the provisions of this Agreement applicable to the System Integrator, shall reproduce Information only to the extent essential to fulfilling the purpose, and shall prevent disclosure of Information to third parties. The System Integrator may, however, disclose the Information to its contractors with a need to know; provided that by doing so, the System Integrator agrees to bind those consultants and contractors to terms at least as restrictive as those stated herein, advise them of their obligations, and indemnify SCRB for any breach of those obligations.

(b) Upon the disclosing party's request, the System Integrator shall either return to the disclosing party all Information or shall certify to the disclosing party that all media containing information have been destroyed. Provided, however, that an archival copy of the Information may be retained in the files of the System Integrator's counsel, solely for the purpose of proving the contents of the Information.

3. The foregoing restrictions on each party's use or disclosure of information shall not apply to information that the System Integrator can demonstrate:

(a) was independently developed by or for the System Integrator without reference to the information, or was received without restrictions; or

(b) has become generally available to the public without breach of confidentiality obligations of the System Integrator; or

(c) was in the System Integrator's possession without restriction or was known by the System Integrator without restriction at the time of disclosure; or

(d) is the subject of a subpoena or other legal or administrative demand for disclosure; provided, however, that the System Integrator has given the disclosing party prompt notice of such demand for disclosure and the System Integrator reasonably cooperates with the disclosing party's efforts to secure an appropriate protective order; or

(e) is disclosed with the prior consent of the disclosing party; or

(f) was in its possession or known to it by being in its use or being recorded in its files or computers or other recording media prior to receipt from the disclosing party and was not previously acquired by the System Integrator from the disclosing party under an obligation of confidence; or

(g) the System Integrator obtains or has available from a source other than the disclosing party without breach by the System Integrator or such source of any obligation of confidentiality or non-use towards the disclosing party.

4. The System Integrator agrees not to remove any of the other party’s confidential information from the premises of SCRB without SCRB’s prior written approval. The System Integrator agrees to exercise extreme care in protecting the confidentiality of any confidential information which is removed, only with SCRB’s prior written approval, from SCRB’s premises. System Integrator agrees to comply with any and all terms and conditions SCRB may impose upon any such approved removal, such as conditions that the removed confidential information and all copies must be returned by a certain date, and that no copies are to be made of the same off the premises.

5. Upon SCRB's request, the System Integrator will promptly return to SCRB all tangible items containing or consisting of SCRB's confidential information all copies thereof.
6. System Integrator recognizes and agrees that all of SCRB's confidential information is owned solely by SCRB (or its licensors) and that the unauthorized disclosure or use of such confidential information would cause irreparable harm and significant injury, the degree of which may be difficult to ascertain. Accordingly, the System Integrator agrees that SCRB will have the right to obtain an immediate injunction enjoining any breach of this Agreement, as well as the right to pursue any and all other rights and remedies available at law or in equity for such a breach.
7. Access to information hereunder shall not preclude an individual who has seen such Information for the purposes of this Agreement from working on future Projects for SCRB which relate to similar subject matters, provided that such individual does not make reference to the information and does not copy the substance of the information during the confidentiality period. Furthermore, nothing contained herein shall be construed as imposing any restriction on the System Integrator's disclosure or use of any general learning, skills or know-how developed by the System Integrator's staff under this Agreement, if such disclosure and use would be regarded by a person of ordinary skill in the relevant area as not constituting a disclosure or use of the information.
8. As between the parties, all information shall remain the property of SCRB. By disclosing information or executing this Agreement, SCRB does not grant any license, explicitly or implicitly, under any trademark, patent, copyright, mask work protection right, trade secret or any other intellectual property right. SCRB disclaims all warranties regarding the information, including all warranties with respect to infringement of intellectual property rights and all warranties as to the accuracy or utility of such information. Execution of this Agreement and the disclosure of information pursuant to this Agreement do not constitute or imply any commitment, promise, or inducement by either party to make any purchase or sale, or to enter into any additional Agreement of any kind.
9. SCRB's failure to enforce any provision, right or remedy under this Agreement shall not constitute a waiver of such provision, right or remedy.

10. This Agreement will be construed in, interpreted and applied in accordance with the laws of India.

11. That in case of any dispute or differences, breach & violation relating to the terms of the Agreement, the said matter or dispute, difference shall be handled as per the dispute resolution clause defined in the MSA.

12. This Agreement constitutes the entire Agreement of the parties with respect to the parties' respective obligations in connection with information disclosed hereunder and supersedes all prior oral and written Agreements and discussions with respect thereto. The parties can amend or modify this Agreement only by writing, duly executed by their respective authorized representatives.

13. This Agreement will survive the expiry or earlier termination of the MSA and / or SLA and shall remain in effect perpetually.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement by their duly authorized officers or representatives and set their respective hands and seals on the date first above written in the presence of;

M/S……...	State Crime Records Bureau
Signature……..	Signature…….
Printed Name……..	Printed Name…….....
Title…….	Title…….
Signature of the System Integrator	Signature of Additional Director General of Police

Witness:

Schedules

1. Change Control Schedule

1.1 Change Control Procedure

This Schedule describes the procedure to be followed in the event of any proposed change to the Master Services Agreement (MSA) or Service Level Agreement (SLA), or scope of work. Such change shall include, but shall not be limited to, changes in the scope of Services provided by the System Integrator.

SCRB and the System Integrator recognize that frequent change is an inevitable part of delivering Services and that a significant element of this change can be accomplished by re-organizing processes and responsibilities without a material effect on the cost. The System Integrator will endeavor, wherever reasonably practicable, to effect change without an increase in the payment as stated in the Terms of Payment Schedule and SCRB will work with the System Integrator to ensure that all changes are discussed and managed in a constructive manner.

This Change Control Schedule sets out the provisions which will apply the changes to;

(a) the Master Services Agreement

(b) Service Level Agreement

(c) Scope of work

1.2 Change Control Note ("CCN")

SCRB at any time shall give written change order to the System Integrator to make changes within the general scope of work of the Contract. Such changes may constitute an increase or decrease in the scope of work of the Contract.

The following are to be noted:

(i) A change shall be considered so, only when such change is beyond the scope of Services including ancillary and concomitant Services required as detailed in Volume I, II and III of the RFP.

(ii) The System Integrator will be required to carry out any change proposed by SCRB.

(iii) The following shall not constitute a change:

(a) Any enhancements / upgradations to infrastructure (IT / non-IT) that may need to be done by the System Integrator to meet the SLAs or any other requirements of the RFP at the time of Acceptance of the solution or at any time during the Contract Period. These will have to be provided by the System Integrator without any additional time or cost effect to SCRB.

(b) Any revisions and / or additions consequent to errors, ambiguities, discrepancies in the quantities, specifications, drawings, etc. of the RFP documents which were not brought to the notice of SCRB by the System Integrator before the award of work and not accounted for in his Proposal. Such upward revisions and / or additions shall be carried out by the System Integrator without any additional time or cost effect to SCRB.

(iv) Request for revisions to the requirements of the MSA, SLA, or scope of work will emanate from the parties' respective Principal contact or the Principal Contact's nominated representative. The Party requesting the change will complete part A of the Change Control Note (CCN) attached below (Section 1.7 of this Volume of the RFP) hereto. The CCN will be presented to the other Party who will acknowledge receipt by signature of the CCN.

(v) Both parties will mutually agree as to whether the request corresponds to a 'Change' or not. Please note that any such request initiated by the System Integrator before being accepted as 'Change' will have to be approved by SCRB.

(vi) Once both parties agree that the request corresponds to a 'Change', the System Integrator will study the 'Change' and its implementation time and cost implications.

(vii) The impact of the Change on the Total Contract Value (referred to as "Value of Change") will be calculated as under:

a. Value of the Change as stated in herein will be calculated using the unit rates provided by the System Integrator for various components in his detailed Commercial Proposal

or as agreed with the System Integrator during negotiations before the award of Contract.

b. For any items for which the unit rates are not available from (a) above, SCRB may use GoTN empanelment rates available or issue an open tender for procurement. Any costs involved in this process will be borne by SCRB.

(viii) The System Integrator will submit the results of the time and cost implication study to SCRB along with relevant supporting documents to allow SCRB to take a final decision on whether the System Integrator should proceed with implementing the Change or not. The estimated cost and time impact indicated by System Integrator shall be considered as a ceiling limit and shall be reviewed by SCRB for taking a decision on implementation of the change. The time and cost impact applicable to the Contract shall be mutually agreed, on the basis of the detailed calculations supported with all relevant back up documents. In case System Integrator fails to submit all necessary substantiation/calculations and back up documents, the decision of SCRB regarding time and cost impact of the Change shall be final and binding on the System Integrator.

(ix) Based on the estimated 'Value of Change', the following will be done:

(a) If the Value of Change is less than 25% of Total Contract Value, the Total Contract value will be revised (increased / decreased) by an amount equal to the Value of Change and the System Integrator will be required to implement the Change within the same Contract subject to the approval of Additional Director General of Police (ADGP), State Crime Records Bureau. Any adjustment to System Integrator's subsequent payments arising due to such a change in Total Contract Value will be mutually agreed with SCRB.

(b) If the Value of Change is more than 25% of Total Contract Value and the Change arises from a decrease in scope of work, the Total Contract value will be decreased by an amount equal to the Value of Change and the System Integrator will be required to implement the Change within the same Contract subject to the approval of Additional Director General of Police (ADGP), State Crime Records Bureau. Any adjustment to

System Integrator's subsequent payments arising due to such a change in Total Contract Value will be mutually agreed with SCRB.

(c) If the Value of Change is more than 25% of Total Contract Value and the Change arises from an increase in scope of work, implementation of this Change will not be done as part of same Contract and will be considered as the subject matter for a separate Bid process subject to the approval of Additional Director General of Police (ADGP), State Crime Records Bureau.

(x) Based on the above, if SCRB approves the implementation of the Change, then System Integrator shall proceed with the enforcement of the Change.

(xi) The provisions of the Contract shall apply to revised work / change order as if the revised work/ change order has been included in the original scope of work. The System Integrator's obligations with respect to such revised work / change order shall remain in accordance with the Contract.

1.3 Quotation

The System Integrator shall assess the CCN and complete part B of the CCN as mentioned in Section 1.7 below. The System Integrator shall consider the materiality of the proposed Change in the context of the Agreement, the Project implementation, operation and management SLA affected by the Change and the total effect that may arise from implementation of the Change. In completing part B of the CCN the System Integrator shall provide as a minimum:

a. A description of the change;

b. A list of Deliverables required for implementing the change;

c. A timetable for implementation;

d. An estimate of cost implication of implementing any proposed change;

e. Any relevant acceptance criteria;

f. Material evidence to prove that the proposed change is not already covered within the scope of Work, SLAs, or MSA.

1.4 Costs

Each party shall be responsible for its own costs incurred in the quotation, preparation of CCNs and in the completion of its obligations described in this process above. In the event the System Integrator is unable to meet the obligations as defined in the CCN then the cost borne by SCRB for getting it done through any third party will be borne by the System Integrator.

1.5 Reporting/ Review

The status on the progress of the change requests and CCNs will be reported by System Integrator to SCRB during the Project review meetings that will be held on a weekly basis till 6 months after Go-live and on a fortnightly basis after this period.

1.6 Obligations

The System Integrator shall be obliged to implement any proposed Changes once approved from SCRB in accordance with this Change Control Schedule, within a time period agreed with SCRB in the CCN and with effect from the date agreed for implementation in the CCN.

1.7 Format of the Change Control Note (CCN)

Change Control Note	**CCN Number:**
Part A: Initiation	
Title:	
Originator:	
Sponsor:	
Date of Initiation:	
Details of Proposed Change	
(To include reason for change and appropriate details/specifications. Identify any attachments as A1, A2, and A3 etc.)	
Authorized by SCRB	Date:
Name:	
Signature:	Date:

Change Control Note	**CCN Number:**
Received by	
Name:	
Signature:	
Part B: Evaluation	
Change Control Note	
(Identify any attachments as B1, B2, and B3 etc.) Changes to Services, Solution architecture, Hardware & Software, Network connectivity, Implementation timelines, Payment Schedule, Documentation, Training, Service levels, component working arrangements and any other Contractual issue.	
Brief Description of solution:	
Impact:	
Deliverables:	
Timetable:	
Future Impact of not implementing proposed change	
Services unavailable during the Change request activity	
Post Implementation risk and risk probability	
Description of Post Implementation risk (other requirement effected) and potential mitigation plan	
Charges for implementation:	
Details of manpower to be provided (Provide CVs of manpower to be deployed in proforma as in Section C of CCN)	
Other Relevant Information: (including value-added and acceptance criteria)	
Authorized by the	**Date:**

Change Control Note	CCN Number:
System Integrator	
Name:	
Signature:	
Part C: Authority to proceed	
Change Control Note	**CCN Number:**
Implementation of this CCN as submitted in part A, in accordance with part B is: (tick as appropriate)	
Approved Rejected Requires Further Information (as follows, or as Attachment 1 etc.)	
For SCRB	**For the System Integrator**
Signature	Signature
Name	Name
Title	Title
Date	Date

2. Exit Management Schedule

2.1 Purpose

1. This Schedule sets out the provisions, which will apply on expiry or termination of the Contract Period and/ or earlier termination of the MSA, and/ or the SLA for any reasons whatsoever.

2. In the case of termination of the Project implementation and/or SLA due to illegality, the parties shall agree at that time whether, and if so during what period, the provisions of this Schedule shall apply.
3. The parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Schedule.
4. The Exit Management Period starts, in case of expiry of Contract, 6 months before the Contract comes to an end or in case of earlier termination of Contract, on the date of service of termination orders to the System Integrator. The Exit Management Period ends on the date agreed upon by SCRB or six months after the beginning of the Exit Management Period, whichever is earlier.
5. During the Exit Management Period, the System Integrator shall use its best efforts to deliver the Services. Payments during the Exit Management Period shall be made in accordance with the Terms of Payment Schedule.

2.2 Transfer of Project Assets

1. Before the expiry of the Exit Management Period, all Project Assets including the hardware, software, system software documentation and any other infrastructure shall have been renewed and cured of all defects and deficiencies as necessary so that the Project is compliant with the specifications and standards set forth in the Agreement, RFP, and any other amendments made during the Contract Period;
2. Before the expiry of the exit management period, the System Integrator will deliver relevant records and reports pertaining to the Project and/or SCRB and its design, implementation, operation, and maintenance including all operation and maintenance records and manuals pertaining thereto and complete as on the divestment date;
3. The System Integrator will provide SCRB with a complete and up to date list of the Assets to be transferred to SCRB within 30 days of start of Exit Management Period.
4. All Assets procured and supplied in the existing contract will be transferred to SCRB on the last day of the Exit Management Period at a book value of Rs. 1 in case of expiry of Contract

and at a book value calculated on that date (40% W.D.V depreciation per annum) in case of earlier termination of Contract.

5. Even during the Exit Management period, the System Integrator's team and/or all third parties appointed by the System Integrator shall continue to perform all their obligations and responsibilities as stipulated under this MSA, and as may be proper and necessary to execute the scope of work under the MSA in terms of this MSA, the RFP and System Integrator's Bid, in order to execute an effective transition and to maintain business continuity.
6. The System Integrator complies with all other requirements as may be prescribed under applicable laws to complete the divestment and assignment of all the rights, title and interest of the System Integrator in this Project free from all encumbrances absolutely and free of any charge or tax to SCRB or its nominated agencies or the replacement System Integrator as the case may be.

2.3 Payments during Exit Management Period

(a) Payment to the outgoing System Integrator shall be made to the tune of last set of rendered Services / Deliverables (including parts thereof) as stated in the terms of Payment Schedule, subject to SLA requirements. Without prejudice to any other rights, SCRB may retain such amounts from the payment due and payable by SCRB to the System Integrator as may be required to offset any losses, damages or costs incurred by SCRB as a result of the termination of System Integrator or due to any act/omissions of the System Integrator or default on the part of System Integrator in performing any of its obligations with regard to this MSA.

(b) Nothing herein the Exit Management Schedule shall restrict the right of SCRB to invoke the Bank Guarantee and other Guarantees furnished hereunder, enforce the Deed of Indemnity and pursue such other rights and/or remedies that may be available to SCRB under law.

2.4 Knowledge Transfer

During the Exit Management period:

(a) The selected System Integrator will be required to provide necessary handholding and transition support to SCRB's staff or its nominated agency or replacement System Integrator.

The handholding support will include but not be limited to, conducting detailed walkthrough and demonstrations for the IT Infrastructure, handing over all relevant documentation, addressing the queries/clarifications of the new agency with respect to the working / performance levels of the infrastructure, conducting training sessions etc.

(b) The System Integrator shall permit SCRB and/or any replacement System Integrator to have reasonable access to its employees and facilities as reasonably required by SCRB to understand the methods of delivery of the Services employed by the System Integrator and to assist appropriate knowledge transfer.

2.5 Transfer of Confidential Information and Data

1. The System Integrator will promptly on the commencement of and during the exit management period supply to SCRB the following:

   (a) Information relating to the current services rendered and customer satisfaction surveys and performance data relating to the Services;

   (b) Documentation relating to SCRB's Intellectual Property Rights;

   (c) SCRB data and Confidential Information;

   (d) All current and updated Project data as is reasonably required for purposes of SCRB transitioning the Services to its replacement System Integrator in a readily available format nominated by SCRB;

   (e) All other information (including but not limited to documents, records and Agreements) held or controlled by the System Integrator which they have prepared or maintained in accordance with the Master Services Agreement, the Project implementation, and the SLA relating to any material aspect of the Services (whether provided by the System Integrator) or as is reasonably necessary to effect a seamless handover of the Project to SCRB or its replacement System Integrator.

2. Before the expiry of the exit management period, the System Integrator shall deliver to SCRB all new or up-dated materials from the categories set out above and shall not retain any copies thereof.

3. For the purposes of this Schedule, anything in the possession or control of System Integrator or its associated entity is deemed to be in the possession or control of the System Integrator. Before the expiry of the exit management period, unless otherwise provided under the Agreement, SCRB shall deliver to the System Integrator all forms of System Integrator Confidential Information, which is in the possession or control of SCRB or its users.

2.6 Employees

1. Promptly on reasonable request at any time during the Exit Management Period, the System Integrator shall, subject to applicable laws, restraints and regulations (including in particular those relating to privacy) provide to SCRB a list of all employees (with job titles) of the System Integrator dedicated to providing the Services at the commencement of the exit management period;
2. Where any national, regional law or regulation relating to the mandatory or automatic transfer of the Contracts of employment from the System Integrator to SCRB or its nominees, or a replacement System Integrator ("Transfer Regulation") applies to any or all of the employees of the System Integrator, then the parties shall comply with their respective obligations under such Transfer Regulations.
3. To the extent that any Transfer Regulation does not apply to any employee of the System Integrator, SCRB, or its replacement System Integrator may make an offer of employment or Contract for services to such employee of the System Integrator and the System Integrator shall not enforce or impose any contractual provision that would prevent any such employee from being hired by SCRB or any replacement System Integrator.
4. Promptly on reasonable request at any time during the Exit Management Period, the System Integrator shall, facilitate training and knowledge transfer for SCRB and/or any replacement System Integrator as reasonably required for understanding the methods of delivery of the Services employed by the System Integrator.

2.7 Transfer of Certain Agreements

On request by SCRB, the System Integrator shall effect such assignments, transfers, licenses and sub-licenses as SCRB may require in favour of SCRB, or its replacement System Integrator in

relation to any equipment lease, maintenance or service provision agreement between System Integrator and third party lessors, vendors, and which are related to the Services and reasonably necessary for the carrying out of replacement services by SCRB or its replacement System Integrator.

2.8 Right of Access of Premises

1. At any time during the Exit Management Period, where Assets are located at the System Integrator's premises, the System Integrator will be obliged to give reasonable rights of access to (or, in the case of Assets located on a third party's premises, procure reasonable rights of access to) SCRB, and/or any replacement System Integrator in order to make an inventory of the Assets.
2. The System Integrator shall also give SCRB or its nominated agencies, or any replacement System Integrator right of reasonable access to the System Integrator's premises and shall procure SCRB or its nominated agencies and any replacement System Integrator rights of access to relevant third party premises during the exit management period and for such period of time following termination or expiry of the Agreement as is reasonably necessary to migrate the services to SCRB or its nominated agencies, or a replacement System Integrator.

2.9 Exit Management Plan

1. The System Integrator shall provide SCRB with a recommended exit management plan ("Exit Management Plan") which shall deal with at least the following aspects of exit management in relation to the Agreement as a whole and in relation to the Project implementation, and the SLAs.
    (a) A detailed program of the transfer process that could be used in conjunction with a replacement System Integrator including details of the means to be used to ensure continued 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;

(b) Plans for the communication with such of the System Integrator's staff and any related third party as are necessary to avoid any material detrimental impact on SCRB's operations as a result of undertaking the transfer;

(c) (if applicable) Propose arrangements for the segregation of the System Integrator's networks from the networks employed by SCRB in specific and / or Govt. of Tamil Nadu in general and identification of specific security tasks necessary at termination;

(d) Plans for provision of contingent support to SCRB and replacement System Integrator for a reasonable period after transfer.

2. The System Integrator shall re-draft the Exit management plan annually thereafter to ensure that it is kept relevant and up to date after obtaining required approval from SCRB or its nominated agencies.
3. The terms of payment as stated in the Terms of Payment Schedule include the costs of the System Integrator complying with its obligations under this Schedule.
4. This Exit management plan shall be furnished in writing to SCRB or its nominated agencies within 90 days from the date of signing of the Agreement.

Note: For details regarding the Exit Management Plan, Process and Milestones, SI to refer to Exit Management described in Section 8.25 of Volume 2 of this RFP.

2.10 Transfer Cost

The System Integrator shall pay all costs (transfer costs, stamp duty etc.) as applicable to meet the requirements of this Exit Management Schedule.

3. Terms of Payment Schedule

3.1 Payment Terms

(a) This Project is planned to be implemented as a service complete with all the components and infrastructure required for delivery of the envisaged activities of the Project. The System Integrator will sign SLA with SCRB covering all the Services required and it will be compensated for such Services, subject to the performance of the system as reflected by the

SLA metrics defined in the Agreement and/or the RFP between the System Integrator and SCRB.

(b) The entire cost for establishing, operating and maintaining the project during the Contract Period will be borne by the System Integrator and factored in his Commercial Proposal submitted in response to the RFP.

(c) The Total Bid Price shall be inclusive of

1. Capital expenditure for Application Development.
2. Capital expenditure for Hardware Items in all three phases.
3. Operations & Maintenance expenses for developed application
4. Operations & Maintenance expenses for supplied hardware
5. Operations & Maintenance expenses for already existing hardware (UPS Units, UPS Batteries & Servers)
6. Item-wise unit cost for Site Infrastructure.
7. Unit Price for Anti-virus, HIPS, API, Web service development & Person Man month.

(d) The System Integrator will be solely responsible to bear the cost of any items that are not quoted or are under quoted in this Proposal but are required to meet the SLAs or any other requirements as stated in the RFP. No additional payment for these components would be made to the System Integrator.

(e) The System Integrator would be paid as per the milestones given in the Terms of Payment Schedule.

(f) For payments, the System Integrator will be required to raise invoice along with detailed report. SCRB will make payment, after the verification of invoice amount and adjusting for penalties, to the System Integrator within 30 days of submission of the correct and valid invoice.

1) The System Integrator shall bear all the statutory levies like customs, insurance, freight, etc. applicable on the goods during their shipment from respective manufacturing/ shipment site of the OEM to the port of landing.

2) All charges including transportation charges that may be applicable till the hardware items are delivered at the respective site of installation shall also be borne by the System Integrator.

3.2 Additional Costs

(a) SCRB shall make payments to the System Integrator at the times and in the manner set out in the Terms of Payment Schedule subject always to the fulfillment by the System Integrator of the obligations herein.

(b) All payments shall be made after adjustments required for any SLA based penalties.

(c) No invoice for extra work/change order on account of change order will be submitted by the System Integrator unless the said extra work /change order has been authorized/ approved by SCRB in writing in accordance with Change Control Schedule of the MSA.

(d) SCRB shall make payments after withholding tax deductible at source (TDS) as appropriate.

3.3 Taxes and Statutory Payments

(a) All payments agreed to be made by SCRB to the System Integrator in accordance with the RFP shall be inclusive of all statutory taxes and other charges whenever levied/applicable.

(b) The System Integrator shall bear all personal/income taxes levied or imposed on its staff, vendor etc. on account of payment received under this Contract. The System Integrator shall bear all income/corporate taxes, levied or imposed on the System Integrator on account of payments received by it from SCRB for the work done under this Contract.

(c) If any change in GST, the same shall be agreed and adjusted accordingly.

3.4 Payment Schedule

The below table comprises of the details of payment schedule against deliverables:

3.4.1 Hardware Payment Schedule

1. Payment Schedule and Milestone for Implementation Phase:

#	Payment Milestone for the Implementation Phase	Phase 1		Phase 2		Phase 3	
		Timelin	Paymen	Timelin	Paymen	Timelin	Paymen

		es	t (as a % of Work Order Value)	es	t (as a % of Work Order Value)	es	t (as a % of Work Order Value)
1	Issuance of Work Order	T	-	T1	-	T2	-
2	Supply of hardware to individual locations and submission of sealed and signed delivery challans	T + 4 months	40%	T1 + 2 month	-	T2 + 3 months	40%
3	Commissioning of equipment and submission of equipment inspection report • Fixing of Asset Tags and computer cover at all locations • Configuration of EMS (existing CA EMS or new EMS) and mapping details of each hardware to asset ids, location and employee	T + 5 months	30%	T1 + 2 month	-	T2 + 4 months	30%
4	Submission of site commissioning report	T + 6 months	30%	T1 + 2 month	100%	T2 + 5 months	30%

2. Payment Schedule and Milestone for O & M Phase:

SNo.	Payment Milestone for the Implementation Phase	Timelines	Payment
1	Submission of SLA report	Quarterly (from date of completion of equipment commissioning)	25% of annual O & M payment of that year payment after deduction of SLA penalties paid every quarter

Note:

- T, T1 & T2 = Issuance of the Work Order for Phase – 1, Phase – 2 & Phase – 3 respectively.

3.4.2 Software Payment Schedule

1. Payment Schedule and Milestone for Implementation Phase:

SNo.	Key Milestones	Timelines (in Months)	% Payment (of Software Capex Value)
1	Signing of Agreement	T	Nil
2	Acceptance of Architecture & System Requirement Study (SRS)	T + 0.5 Month	-
3	Completion of Application Development & Testing by System Integrator	T + 3.5 Months	5%
4	Completion of User Acceptance Testing (UAT) by SCRB	T + 4 Months	15%
5	SI to make software compliant as per security audit as per the VAPT clause (Section 8.14.1 in Volume 2 of RFP)	T + 4.5 Months	-
6	Hosting of Application Software in TNSDC servers by SI	T + 5 Months	-
7	Completion of Pilot Rollout & Training for users in Pilot locations	T + 5 Months	-
8	Application Stabilization & Acceptance of Pilot Rollout by SCRB	T + 5.5 Months	25%
9	Complete Training for all Users	T + 6 Months	-
10	SI to make software compliant as per independent TPA audit as per TPA clause (Section 8.14.2 in Volume 2 of RFP)	T + 6 Months	-
11	State-wide Rollout of Application by SI	T + 6.5 Months	-
12	Acceptance of Go-Live by SCRB	T + 7 Months	30%

2. Payment Schedule and Milestone for Implementation Phase:

SNo.	Key Milestones	Timelines (in Months)	% Payment
1	Application Operations & Maintenance (O&M)	T + 8 Months to T + 68 Months	25% of annual O & M payment of that year payment post Go – Live after deduction of SLA penalties paid every quarter

Note:

1. 'T'- Signing of agreement
2. **75 % of Software Capex Value will be paid during implementation phase and the remaining 25% of Software Capex Value will be paid equally during the O&M phase at 5% per year.**
3. SCRB reserves the right to release the part payment for completed work against the milestone payment.
4. All Payments shall be made in Indian Rupees Only.
5. Definition of Go-Live - SCRB will accept the commissioning and project Go-Live only after successfully passed SDLC review process and also satisfying all the following parameters across all sites
   a. UAT sign-off from SCRB.
   b. Security, Performance, Testing, & VAPT signoff.
   c. SI shall ensure that the TPA audit is completed and the modifications as per the audit observations are completed and SI shall furnish the Third-party auditor certification to SCRB.
   d. Successful completion capacity building to all intended audience before the end of stabilization period.

Based on the above four parameters Go-Live sign off will be issued by SCRB.

4. Deliverables and Timelines Schedule

Following table details the key Project milestones and the Deliverables to be submitted by the System Integrator at each milestone.

Project Stage	Indicative Deliverables

Project Stage	Indicative Deliverables
Contract Stage	• Performance Bank Guarantee (5 % of Total Contract Value).
Study & Design Stage	• Detailed Project Plan. • Risk Management and Mitigation Plan. • Manpower Deployment Plan. • Gap analysis report on existing infrastructure, network and hardware recommendations. • Site Inspection Report on the reusability of existing site infrastructure • Part wise hardware procurement & Software deployment plan separately for pilot and full-scale rollout. • Make & model of OEM proposed. • IT Infrastructure Security plan. • IT Infrastructure deployment plan. • IT Infrastructure Management Policy and related SOPs in line with the ITIL (Information Technology Infrastructure Library) standards. • Storage management policy. • Helpdesk / Technical support plan. • Business Continuity and Disaster Recovery plan including backup plan. • Information Systems Security Policy and related procedures in line with the ISO27001 standard. • Data migration plan. • Manpower deployment plan.

Project Stage	Indicative Deliverables
	• Exit Management Plan including plan for Knowledge Transfer.
Application Design & Development and Customization	• Technical Architecture Document (Application, Network, and Security). • Database Architecture Report. • Software Implementation Plan Document. • Detailed Design Plan. • Developed and customized application including web-portal for UAT. • Application Test plan, Test cases, Test assumptions, Test coverage and boundaries. • Test documents. • Test reports until zero defects. • Application User manual and deployment document. • Web APIs. • Software installation guide. • Application Technical manual, drivers, installable etc. • System maintenance manuals. • Application Source code.
Helpdesk, Business Continuity, Disaster Recovery, Database	• Detailed plan on Helpdesk, Business continuity, Disaster recovery, Data Migration, Integration with in-house and Third party system.

Project Stage	Indicative Deliverables
Migration, Third Party Integration, SMS, Email and Payment gateway Integration	• Capacity Building and Change Management plan. • Completion report on o Database migration and validation of Oracle databases. o Integration with SCRB and other department portals, Third party systems. o Report exchange of data and communication with in-house, external and other Third-party system in scope. o Maintain integration log for all Third party integration, in house legacy databases and portals. o Helpdesk operations & maintenance.
Hardware & Software License Procurement & Commissioning- Pilot	• SCRB approved Pilot sites. • Final BoM (Bill of Material). • Configuration files of the infrastructure. • PAT Report on IT Infrastructure (DC, DR, Pilot Locations). • Documentation on IT Infrastructure and Software license procured and deployed. • Infrastructure Deployment / Commissioning Report for Police Stations, SCRB Offices, Acceptance report form SCRB. • Readiness of DC, DR before pilot deployment. • Completion report on EMS & Remote Device Management setup. • Readiness report for IT infra monitoring. • Knowledge repository readiness report. • Business Continuity plan and Disaster Recovery plan. • Information security management procedures.

Project Stage	Indicative Deliverables
Training Plan Preparation	Detailed Training plan comprising • SCRB approved location wise participant name and count for pilot training. • Training Materials, User Manual. • IT Infrastructure System Operation Manual. • IT Infrastructure Maintenance and Troubleshooting Manual. • End User Manual for SCRB Applications – Final. • Sign off from SCRB on identified Training locations, Training assessment approach.
UAT	• Application Test plans, Test cases, Test assumptions, Test coverage and boundaries. • Application User manual & standard operating procedures. • Software installation guide. • System maintenance manuals. • UAT report. • UAT Signoff report • Completion report on Site preparation & Application.
Training- Pilot Users	• Change Management workshop completion Report. • Training Completion Report. • Training Assessment Results. • Training Feedback and plan for implementation of changes.
Deployment Phase- Pilot	• System change over strategy for and transition to new system from existing system.

Project Stage	Indicative Deliverables
	• Pilot deployment plan. • Pilot rollout report including. o Site preparation and infrastructure deployment / commissioning report for pilot sites. o Data Migration report for pilot. o Helpdesk operationalization report. o Performance Assessment report for Pilot site. o Pilot deployment completion report.
Audit- Pilot Rollout	• Documents required by TPA for audit purpose.
Application Stabilization & Pilot Rollout Acceptance	• Report on amendments / enhancements / modifications made based on inputs of Department's / Third Party's Acceptance Testing for pilot rollout. • Application Stabilization report. • Report on completion of changes in the software. • Obtain Pilot Acceptance report from Department.
Hardware & Software License Procurement & Commissioning- Full Scale	• Final BoM • Documentation on IT Infrastructure and Software license procured and deployed. • Infrastructure Deployment / Commissioning Report - Acceptance report from SCRB. • Factory Acceptance Test (FAT) Report on IT Infrastructure • Warranty Certificate. • Site Delivery Plan showing exact coordinates of the hardware.

Project Stage	Indicative Deliverables
Training Plan Preparation for Full Scale	• Training plan and schedule. • SCRB approved location wise participant name and count for full-scale training. • Approval of Training location and Facility. • Revised training content as per Pilot feedback (if applicable).
Training- Full Scale	• Change Management workshop completion Report. • Training Completion Report. • Overview Training Completion report. • Training material. • Training Materials, System User Manual. • IT Infrastructure System Operation Manual. • IT Infrastructure Maintenance and Troubleshooting Manual. • End User Manual for complete system – Final.
Audit	• Documents required by TPA for audit purpose.
Full Scale Rollout	• Rollout across State ready for acceptance by Department. • Report on amendments / enhancements / modifications made based on inputs of Department's Pilot Acceptance Testing. • Site preparation and infrastructure deployment report across all locations. • Manpower deployment report. • Data Migration report for pilot. • Data Migration report including Test plans and Test results for Data Migration.

Project Stage	Indicative Deliverables
	• Helpdesk operationalization report. • Training Delivery report. • Performance Assessment report for State-wide-rollout.
Acceptance of State-wide Rollout and Go-live	• Report on rollout for full scale. • Report on amendments / enhancements / modifications made based on inputs of Department's / Third Party's Acceptance Testing for full scale rollout. • Final acceptance of System. • Obtain Go-live Acceptance Report from Department. • Training Completion Report. • Final Report on the Access rights and control structure. • Application Configuration/ customization report –Final. • Manpower Deployment Report. • Final Report on the Access rights and control structure. • IT Infrastructure Integration & Connectivity Report. • Performance Assessment report for Data Centre, DR Site and all department office locations. • Business Continuity and Disaster Recovery report.
Operations & Maintenance Phase	• Detailed plan for monitoring of SLAs and performance of the overall system. • Fortnightly Progress Report on Project including SLA Monitoring Report and Exception Report. • Details on all the issues logged.

Project Stage	Indicative Deliverables
Project Closure	• Project Closure report. • Project documents and other artefacts. • Document of design standard operating procedures to manage system. • Provide the Source Code (all version) related to the Application development / Integration as per the license Agreement. • Handover configuration information & System documentation • Hardware related documents. • SDK for all major software languages such as Android/ Java, .Net, C/C+. SDK shall be compatible with all major OS such as windows, android, Linux etc.

In case the Contract period with the System Integrator is extended beyond 5 years after Go-Live, the Deliverables of the "Monitor and Review" Phase would continue for the extended period.

Timelines Schedule:

1. Hardware Infrastructure Implementation and O & M Schedule

Legends:

M = Month

0.5 = 0.5 Month

1 = 1 Month

T, T1 & T2 = Issuance of the Work Order for Phase – 1, Phase – 2 & Phase – 3 respectively.

Phase 1:

Key Milestones	Months		M0	M1	M2	M3	M4	M5	M6
Issuance of Work Order	**T**	**0**							

Supply of hardware/ server to individual locations and Submission of sealed and signed delivery challans	**T + 4**	**4**							
Commissioning of equipment and Submission of equipment inspection report	**T + 5**	**1**							
Configuration of Monitoring Tool (existing CA EMS or new EMS) and mapping details of each hardware to asset ids and locations									
Submission of Site Commissioning Report	**T +6**	**1**							

Phase 2:

Key Milestones	Months		M0	M1	M2
Issuance of Work Order	**T1**	**0**			
Supply of hardware/ server to individual locations and Submission of sealed and signed delivery challans	**T1 + 2**	**2**			
Commissioning of equipment and Submission of equipment inspection report					
Configuration of Monitoring Tool (existing CA EMS or new EMS) and mapping details of each hardware to asset ids and locations					
Submission of Site Commissioning Report					

Phase 3:

Key Milestones	Months		M0	M1	M2	M3	M4	M5
Issuance of Work Order	**T2**	**0**						
Supply of hardware/ server to individual locations and Submission of sealed and signed delivery challans	**T2 + 3**	**3**						
Commissioning of equipment and Submission of equipment inspection report	**T2 + 4**	**1**						

Configuration of Monitoring Tool (existing CA EMS or new EMS) and mapping details of each hardware to asset ids and locations	**T2 + 4**	**0**						
Submission of Site Commissioning Report	**T2 +5**	**1**						

2. Software Implementation and O & M Schedule

Key Milestone	Month(s)	Duration	M0	M0.5	M1	M1.5	M2	M2.5	M3	M3.5	M4	M4.5	M5	M5.5	M6	M6.5	M7	M9–M68
Signing of Agreement and Issuance of Work Order	T	0																
Acceptance of Architecture & System Requirement Study (SRS)	T+0.5	0.5																
Completion of Application Development & Testing by System Integrator	T+3.5	3																
Completion of User Acceptance Testing (UAT) by SCRB	T+4	0.5																
SI to make software compliant as per security audit as per the VAPT clause (Section 8.14.1 in Vol 2 of RFP)	T+4.5	0.5																
Hosting of Application Software in TNSDC servers by SI	T+5	0.5																
Completion of Pilot Rollout & Training for users in Pilot locations	T+5	0																
Application Stabilization & Acceptance of Pilot Rollout by SCRB	T+5.5	0.5																
Complete Training for all Users	T+6	0.5																
SI to make software compliant as per	T+6	0																

independent TPA audit as per TPA clause (Section 8.14.2 in Vol 2 of RFP)																		
State-wide Rollout of Application by SI	**T+6.5**	**0.5**																
Acceptance of Go-Live by SCRB	**T+7**	**0.5**																
Application Operations & Maintenance (O&M)	**T+8 to T+68**	**60**																

5. Audit, Access and Reporting Schedule

The Parties shall comply with the Audit, Access and Reporting Schedule. The System Integrator shall, on request, allow access to SCRB to all information which is in the possession or control of the System Integrator, which relates to the provision of the Services as set out in the MSA and the RFP and is reasonably required to comply with the terms of the Audit, Access and Reporting Schedule.

5.1 Purpose

This Schedule details the audit, access and reporting rights and obligations of SCRB and the System Integrator under the Master Services Agreement, and/or SLA and any other agreements that are entered into simultaneously with this Agreement or subsequently.

5.2 Audit Notice and Timing

1. As soon as reasonably practicable after the Effective Date, the Parties shall use their best endeavors to agree to a timetable for routine audits prior to the Go-Live of the Solution and post Go-Live. Once a timetable for routine audits has been agreed, SCRB shall conduct audits in accordance with such agreed timetable and shall not be required to give the System Integrator any further notice of carrying out such audits.
2. SCRB may conduct non-timetabled audits at their own discretion if it reasonably believes that such non-timetabled audits are necessary as a result of an act of fraud by the System Integrator, a security violation, or breach of confidentiality obligations by the System Integrator, provided that the requirement for such an audit is notified in writing to the System Integrator, a reasonable time period prior to the audit (taking into account the circumstances giving rise to the reasonable belief) stating in a reasonable level of detail the reasons for the requirement and the alleged facts on which the requirement is based.
3. SCRB shall endeavor to conduct such audits to minimize inconvenience and disturbance to the System Integrator.
4. In addition to the above, there will be audits conducted by statutory bodies as and when they are required to do it. Notwithstanding any condition given in the MSA, System Integrator

will have to provide these statutory bodies access to all the facilities, infrastructure, documents and artifacts of the Project as required by them and approved by SCRB, in writing.

5. During any such audits conducted by SCRB, if any unlawful, fraudulent activities are identified, SCRB may subject the contract for termination at its discretion.

5.3 Access

The System Integrator shall provide to SCRB reasonable access to employees, third party facilities, including leased premises used for any activity of "Implementation of CCTNS 2.0 project of SCRB" as detailed in Volume I, II & III of the RFP, documents, records and systems reasonably required for audit and shall provide all such persons with routine assistance in connection with the audits and inspections. SCRB shall have the right to copy and retain copies of any relevant records. The System Integrator shall make every reasonable effort to co-operate with them.

5.4 Audit Rights

1. SCRB shall have the right to audit, third party facilities, including leased premises used for the Implementation of the Project which may include but not limited to Helpdesk, documents, records, procedures and systems relating to the provision of the services, but only to the extent that they relate to the provision of the services, as shall be reasonably necessary to verify:

   (a) the security, integrity and availability of all SCRB data processed, held or conveyed by the System Integrator on behalf of SCRB and documentation related thereto;

   (b) that the actual level of performance of the services is the same as specified in the SLAs;

   (c) that the System Integrator has complied with the relevant technical standards, and has adequate internal controls in place; and

   (d) the compliance of the System Integrator with any other obligation under the Master Services Agreement and SLAs.

2. For the avoidance of doubt the audit rights under this Schedule shall not include access to the System Integrator's profit margins or overheads associated with any obligation under the Master Services Agreement.

5.5 Action and Review

Any discrepancies identified by any audit pursuant to this Schedule shall be immediately notified to SCRB and the System Integrator's Project Manager in the form of an Audit report. The System Integrator shall address any identified gaps and issues identified during the Audit process to the satisfaction of SCRB and the auditing agency within thirty (30) days from the date of notification of the said Audit report.

5.6 Records and Information

For the purposes of audit in accordance with this Schedule, the System Integrator shall maintain true and accurate records in connection with the provision of the Services and the System Integrator shall handover all the relevant records and documents upon the termination or expiry of the Contract.

6. Pricing Schedule

6.1 Pricing Summary

The pricing summary presented by the System Integrator in his Commercial Proposal as mentioned in Annexure 5 of Volume - I of the RFP would be a part of the MSA.

6.2 Detailed Component-Wise Pricing Formats

The detailed component-wise pricing formats presented by the System Integrator in his Commercial Proposal as mentioned in Annexure 5 (2) of Volume - I of the RFP would be a part of the MSA.