E-GOVERNANCE
MISSION MODE PROJECT (MMP)

CRIME & CRIMINAL TRACKING NETWORK AND SYSTEMS
(CCTNS)

REQUEST FOR PROPOSAL FOR SELECTION OF SYSTEM INTEGRATOR FOR IMPLEMENTING, COMMISSIONING AND MAINTAINING CCTNS IN HARYANA POLICE

VOLUME-III: MASTER SERVICE AGREEMENT

RELEASED BY:

HARYANA POLICE

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ADGP	Additional Director General of Police
AFIS	Automated Fingerprint Identification System
AIG	Assistant Inspector General of Police
AT	Acceptance Testing
BOM	Bill of Material
BPR	Business Process Reengineering
BSNL	Bharat Sanchar Nigam Limited
CAD	Computer Aided Dispatch
CAS	Core Application Software
CBI	Central Bureau of Investigation
CCIS	Crime and Criminals Information System
CCTNS	Crime & Criminal Tracking Network and Systems
CID	Criminal Investigation Department
CIPA	Common Integrated Police Application
CPMU	Central Program Management Unit
CrPC	Criminal Procedure Code
DCRB	District Crime Record Bureau
DG	Director General
DG Set	Diesel Generator Set
DGP	Director General of Police
DIG	Deputy Inspector General of Police
DIT	Department of Information Technology
DRC	Disaster Recovery Centre
DSP	Deputy Superintendent of Police
EMD	Earnest Money Deposit
EMS	Enterprise Management System
FIR	First Information Report
FRS	Functional Requirement Specifications
GIS	Geographical Information System
GO	Gazetted Officer
GOI	Government of India
GPS	Global Positioning System
GRP	Government Railway Police
HLD	High Level Design
HQ	Headquarters
ICT	Information & Communication Technology
IGP	Inspector General of Police
IIF	Integrated Investigation Forms
IO	Investigation Officer

IPC	Indian Penal Code
IT	Information Technology
LAN	Local Area Network
LIMS	Lawful Interception Monitoring System
LLD	Low Level Design
MHA	Ministry of Home Affairs
MIS	Management Information System
MMP	Mission Mode Project
MPLS	Multiprotocol Label Switching
NCR	Non-Cognizable Report
NCRB	National Crime Record Bureau
NeGP	National eGovernance Plan
NGO	Non-Gazetted Officer
NIC	National Informatics Centre
NOC	No Objection Certificate
PCR	Police Control Room
PHQ	Police Headquarters
RFP	Request for Proposal
RTI	Right To Information
SAN	Storage Area Network
SCRB	State Crime Record Bureau
SDA	Software Development Agency
SDC	State Data Centre
SDPO	Sub-Division Police Office
SHO	Station House Officer
SI	System Integrator
SLA	Service Level Agreement
SOA	Service Oriented Architecture
SP	Superintendent of Police
SPMC	State Project Management Consultants
SPMU	State Program Management Unit
SRS	Software Requirement Specifications
SWAN	State Wide Area Network
SyRS	System Requirement Specifications
UT	Union Territory
VPN	Virtual Private Network
XML	Extensible Markup Language

GLOSSARY OF TERMS

The definitions of various terms that have been used in this RFP are as follows:

- **"Request for Proposal (RFP)"** means all three Volumes and its annexure and any other documents provided along with this RFP or issued during the course of the selection of bidder, seeking a set of solution(s), services(s), materials and/or any combination of them.

- **"Contract / Agreement / Contract Agreement/ Master Service Agreement"** means the Agreement to be signed between the successful bidder and Haryana Police, including all attachments, appendices, all documents incorporated by reference thereto together with any subsequent modifications, the RFP, the bid offer, the acceptance and all related correspondences, clarifications, presentations.

- **"Bidder"** means any firm offering the solution(s), service(s) and /or materials as required in the RFP. The word Bidder when used in the pre-award period shall be synonymous with parties bidding against this RFP, and when used after award of the Contract shall mean the successful party with whom Haryana Police signs the agreement for rendering of services for implementation of this project.

- **"Proposal / Bid"** means the Pre-Qualification, Technical and Commercial bids submitted for this project against this RFP.

- **"Requirements"** shall mean and include all the reports prepared by Haryana Police SPMC, schedules, details, description, statements of technical data, performance characteristics and standards (Indian & International) as applicable and specified in the RFP.

- **"Successful Implementation / Go-Live"** will mean:
    - Successful deployment, commissioning and UAT of the CCTNS application modules implemented during the phase
    - Site Preparation including civil works, creation of LAN, electrical works, etc. during that phase after verification and approval by Haryana Police or its constituted committees or representatives
    - Successful Data digitization / migration after verification and approval by Haryana Police or its constituted committees or representatives
    - Training and Certification of all the trainees, trained on the CCTNS application modules of that Phase
    - Procurement, deployment and commissioning of the hardware at PHQ, Data Center, DR Site and other locations required to support the functioning of modules of that Phase
    - Procurement, deployment and commissioning of the networking equipments and provisioning of desired connectivity required to support the functioning of modules of that Phase
    - Achievement of the Service Levels as expected during that Phase

- Acceptance / Sign off from Haryana Police or its constituted committees or representatives

1 REQUEST FOR PROPOSAL DATASHEET

S. No	Information	Details
1.	RFP reference No and Date	
2	Non Refundable Tender Cost	Rs. 10,000/-
3	Sale of RFP Document	24th January 2011
4	Earnest Money Deposit (EMD/ Bid Security)	Rs. 2,00,00,000/-
5.	Last date and Time for submission of written queries[1] for clarifications	1st February 2011 by 12:00 p.m.
	Date, Time and Venue of pre-proposal conference	1st February 2011 at 3:00 p.m. at Gazetted Officers Mess. Police Complex, Moginand, Panchkula
6.	Release of response to clarifications on	5th February 2011
7.	Last date, Time (deadline) and Venue for receipt of proposals in response to RFP notice	1st March 2011 till 2:00 p.m. at the Office of IGP Telecommunication, Haryana Police Headquarter, Sector-6, Panchkula
8.	Date, Time and Venue of opening of Technical proposals received in response to the RFP notice	1st March 2011, 3:00 p.m. at Gazetted Officers Mess. Police Complex, Moginand, Panchkula
9.	Place, Time and Date of Technical Presentations by the bidders	To be intimated Later
10.	Place, Time and Date of opening of Financial proposals received in response to the RFP notice	To be intimated Later
11.	Contact Person for queries	Sh. Jagdish Chand DSP/IT, Haryana Police Headquarters, Sector -6, Panchkula dsp.itphq-hry@nic.in Ph: 0172 2587900 to 906, Extn. 199 or 151
12.	Addressee and Address at which proposal in response to RFP notice is to be submitted:	Director General of Police, Haryana Haryana Police Headquarters, Sector-6, Panchkula

Table 1: RFP Datasheet

[1] Queries submitted in written to Haryana Police would only be accepted for further consideration

Address for Communications for the purpose of this RFP

Mr. Jagdish Chand
Deputy Superintendent of Police, Haryana Police
IT Cell, Police Headquarter, Sector-6, Panchkula, Haryana,
Ph: 0172 2587900 to 906, Extn. 199 or 151
Email: dsp.itphq-hry@nic.in

2 MASTER SERVICES AGREEMENT

THIS AGREEMENT is made on this the <***> day of <***> 2011 at <***>, India.

BETWEEN

Governor of Haryana acting through Director General of Police, Haryana, Haryana Police Headquarters, Panchkula, India (hereinafter referred to as '***Client*****,** which expression shall, unless excluded by or repugnant to the context, include his successor in office and assignees and delegates) on the one part,

AND

<***>**,** a Company registered under the *Companies Act, 1956*, having its registered office at <***> acting through <***>, authorized through Power of Attorney dated <***> to sign the document (hereinafter referred to as '***System Integrator/ SI'*** which expression shall, unless excluded by or repugnant to the context, include his successors/ administrators/ assignees) on the second part.

Each of the parties mentioned above are collectively referred to as the '***Parties***' and individually as a '***Party***'.

WHEREAS:

1. Client is desirous to implement the Mission Mode Project Crime & Criminal Tracking Network and Systems, an initiative of National Crime Record Bureau under Ministry of Home Affairs in Haryana Police for creating a comprehensive and integrated system for enhancing the efficiency and effectiveness of policing at all levels and especially at the Police Station level through adoption of principles of e-Governance.

2. In furtherance of the same, Client 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 <***> .

3. The successful bidder has been selected as the System Integrator on the basis of the Bid Details set out as Annexure D of this Agreement, to undertake the Project of the development and implementation of the solution, its roll out and sustained operations.

NOW THEREFORE, in consideration of the mutual covenants, promises, assurances, representations and provisions set forth herein, the Parties hereto agree as follows:

2.1 Definitions and Interpretations

2.1.1 Definitions

Terms and expressions used in this Agreement (including the Introduction) shall have the meanings set out in Schedule I.

2.1.2 Interpretation

In this Agreement, unless otherwise specified:

(a) references to Clauses, Sub-Clauses, Paragraphs, Schedules and Annexure are to clauses, sub-clauses, paragraphs, schedules and annexure to this Agreement;

(b) use of any gender includes the other genders;

(c) references to a '**company**' shall be construed so as to include any company, corporation or other body corporate, wherever and however incorporated or established;

(d) references to a '**person**' shall be construed so as to include any individual, firm, company, government, state or agency of a state, local or municipal authority or government body or any joint venture, association or partnership (whether or not having separate legal personality);

(e) a 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;

(f) any reference to a '**day**' (including within the phrase 'business day') shall mean a period of 24 hours running from midnight to midnight;

(g) references to a **'business day'** shall be construed as a reference to a day (other than a Sunday) on which Government offices in the State of Haryana are generally open for business;

(h) references to times are to Indian Standard Time;

(i) a reference to any other document referred to in this Agreement is a reference to that other document as amended, varied, notated or supplemented at any time; and

(j) all headings and titles are inserted for convenience only. They are to be ignored in the interpretation of this Agreement.

(k) System integrator (SI) has been used for the same entity i.e. bidder selected for the project.

2.2 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 INR.

2.3 Ambiguities within Agreement

In case of ambiguities or discrepancies within this Agreement, the following principles shall apply:

(a) 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;

(b) 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

(c) as between any value written in numerals and that in words, the value in words shall prevail.

2.4 Priority of documents

This Agreement, 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 Agreement 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) This Agreement along with the SLA agreement, NDA agreement, Schedules and Annexure;

(b) Request for Proposal and Addendum/ Corrigendum to the Request for Proposal (if any).

For the avoidance of doubt, it is expressly clarified that in the event of a conflict between this Agreement, Annexure/ Schedules or the contents of the RFP, the terms of this Agreement shall prevail over the Annexure/ Schedules and Annexure/ Schedules shall prevail over the contents and specifications of the RFP.

2.5 Scope of the Project

The System Integrator shall be required to follow the scope of work as defined in section 6, of Volume I of this RFP. In addition to the scope of work, SI will also be required to adhere to the project timelines and submit the required deliverables as defined in section 7, of Volume I of this RFP.

2.5.1 Terms & Duration of the Project

The Client intends to grant to the System Integrator the right to undertake and implement the Project on the terms and conditions set forth below:

i. Successful implementation / Go-Live of the project in two Phases (as defined in RFP Volume 1) within the defined period from the date of signing of contract. The Successful implementation / Go-Live of a Phase will include:

- Successful deployment, commissioning and UAT for the modules in the concerned phases
- Successful Data digitization / migration along with verification from the CLIENT,
- Successful training of the staff members on the modules
- Procurement, deployment and commissioning of the hardware required for the concerned phase at PHQ, Data Center and other Police locations,
- Procurement, deployment and commissioning of the networking equipments and connectivity required for that Phase
- Acceptance / Sign off from the Client for reaching the stage of successful Go-Live at each phase

ii. Operations and Maintenance of the system for a period of five years from the Successful Implementation / Go-Live of the Complete CCTNS Solution.

iii. Hence, the Overall "Term" for the Project will be at least 50 weeks[2] and 5 years.

iv. This Agreement shall come into effect on <***> 2011 (hereinafter the '***Effective Date***') and shall continue till operation and maintenance completion date which shall be the date of the completion of the operation and maintenance to the satisfaction of Client or its nominated agencies.

2.6 Conditions Precedent & Effective Date

2.6.1 Provisions to take effect upon fulfillment of Conditions Precedent

Subject to express terms to the contrary, the rights and obligations under this Agreement shall take effect only upon fulfillment of all the Conditions Precedent set out below. However, Client or its nominated agencies may at any time at its sole discretion waive fully or partially any of the Conditions Precedent for the System Integrator.

2.6.2 Conditions Precedent of the System Integrator

The System Integrator shall be required to fulfill the Conditions Precedent in which is as follows:

(a) to provide a Performance Security/Guarantee and other guarantees/ payments as and when required to the Client or its nominated agencies; and

(b) to provide the Client or its nominated agencies certified true copies of its constitutional documents and board resolutions authorizing the execution, delivery and performance of this Agreement by the System Integrator

For the avoidance of doubt, it is expressly clarified that the obligations of the Parties except the financial obligations of Client or its nominated agencies under this Agreement shall commence from the fulfillment of the Conditions Precedent as set forth above.

[2] This is subject to the receipt of CAS (State) from NCRB, MHA, Government of India

2.6.3 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 Agreement.

(b) For the avoidance of doubt, it is expressly clarified that any such extension of time shall be subject to imposition of penalties on the System Integrator linked to the delay in fulfilling the Conditions Precedent.

2.6.4 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 days of signing of this Agreement and the same have not been waived fully or partially by Client or its nominated agencies, this Agreement shall cease to exist;

(b) In the event that the Agreement fails to come into effect on account of non fulfillment of the System Integrator's Conditions Precedent, the Client or its nominated agencies shall not be liable in any manner whatsoever to the System Integrator and the Client shall forthwith forfeit the Performance Guarantee.

(c) In the event that possession of any of the Client or its nominated agencies facilities has been delivered to the System Integrator prior to the fulfillment of the Conditions Precedent, upon the termination of this Agreement such shall immediately revert to Client or its nominated agencies, free and clear from any encumbrances or claims.

2.7 Obligations under the SLA

2.7.1 The SLA shall be a separate contract in respect of this Agreement and shall be entered into concurrently with this Agreement between Client and System Integrator;

2.7.2 In relation to any future SLA entered into between the Parties; each of the Parties shall observe and perform the obligations set out herein.

2.7.3 Change of Control

(a) In the event of a change of control of the System Integrator during the Term, the SI shall promptly notify Client and/or its nominated agencies of the same in the format set out as Annexure A of this Agreement.

(b) In the event that the net worth of the surviving entity is less than that of System Integrator prior to the change of control, the Client or its nominated agencies may within 30 days of becoming aware of such change in control, require a replacement of existing Performance Guarantee furnished by the SI from a guarantor acceptable to the Client or its nominated agencies (which shall not be System Integrator or any of its associated entities).

(c) If such a guarantee is not furnished within 30 days of the Client or its nominated agencies requiring the replacement, the Client may exercise its right to terminate the SLA and/ or this Agreement 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 2.16.2 of

this Agreement 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.

2.7.4 Final testing and certification

The Project shall be governed by the mechanism of final acceptance testing and certification to be put into place by the Client, guided by the following principles:

(a) Client reserves the right to nominate a technically competent agency ("***Final Testing and Certification Agency***") for conducting final acceptance testing and certification;

(b) Such Final Testing and Certification 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 requirements of the RFP and this Agreement;

(c) The Final Testing and Certification Agency will be involved with Project from the development stage to ensure that the guidelines are being followed and to avoid large scale modifications pursuant to testing done after the application is fully developed;

(d) The Final Testing and Certification Agency may engage professional organizations for conducting specific tests on the software, hardware, networking, security and all other aspects;

(e) The Final Testing and Certification Agency will establish appropriate processes for notifying the System Integrator of any deviations from the norms, standards or guidelines at the earliest instance after taking cognizance of the same to enable the System Integrator to take corrective action;

(f) Such an involvement of and guidance by the Final Testing and Certification Agency shall not, however, absolve the System Integrator of the fundamental responsibility of designing, customizing/ developing, installing, testing and commissioning the various components of the Project to deliver the services in perfect conformity with this Agreement

2.7.5 The Parties shall each ensure that the range of the Services under the SLA shall not be varied, reduced or increased except with the prior written agreement between the Client and System Integrator in accordance with the Change Control Schedule set out in Schedule II of this Agreement. Save for the express terms of the Terms of Payment Schedule set out as Schedule VI of this Agreement, Client or its nominated agencies and its users may purchase any particular category of Services that may become necessary

as per the Change Control Schedule set out in Schedule II of this Agreement, without the need to go for a separate procurement process.

2.8 Representations and Warranties

2.8.1 Representations and warranties of the System Integrator

The System Integrator represents and warrants to the Client or its nominated agencies that:

(a) it is duly organized and validly existing under the laws of India, and has full power and authority to execute and perform its obligations under this Agreement and other agreements and to carry out the transactions contemplated hereby;

(b) it is a competent provider of a variety of information technology and business process management services;

(c) it has taken all necessary corporate and other actions under Applicable Laws to authorize the execution and delivery of this Agreement and to validly exercise its rights and perform its obligations under this Agreement;

(d) from the Effective Date, it will have the financial standing and capacity to undertake the Project in accordance with the terms of this Agreement;

(e) in providing the Services, it shall use reasonable endeavours not to cause any unnecessary disruption to Client's normal business operations

(f) this Agreement has been duly executed by it and constitutes a legal, valid and binding obligation, enforceable against it in accordance with the terms hereof, and its obligations under this Agreement shall be legally valid, binding and enforceable against it in accordance with the terms hereof;

(g) the information furnished in the tender documents and as updated on or before the date of this Agreement is to the best of its knowledge and belief true and accurate in all material respects as at the date of this Agreement;

(h) the execution, delivery and performance of this Agreement shall not conflict with, result in the breach of, constitute a default by any of the terms of its Memorandum and Articles of Association or any Applicable Laws or any covenant, contract, agreement, arrangement, understanding, decree or order to which it is a party or by which it or any of its properties or assets is bound or affected;

(i) there are no actions, suits, proceedings, or investigations pending or, to its knowledge, threatened against it at law or in equity before any court or before any other judicial, quasi-judicial or other authority, the outcome of which may result in the breach of this Agreement or which individually or in the aggregate may result in any material impairment of its ability to perform any of its material obligations under this Agreement;

(j) it has no knowledge of any violation or default with respect to any order, writ, injunction or decree of any court or any legally binding order of any Government Instrumentality which may result in any Adverse Effect on its ability to perform its obligations under this Agreement and no fact or circumstance exists which may give rise to such proceedings that would adversely affect the performance of its

obligations under this Agreement;

(k) it has complied with Applicable Laws in all material respects and has not been subject to any fines, penalties, injunctive relief or any other civil or criminal liabilities which in the aggregate have or may have an Adverse Effect on its ability to perform its obligations under this Agreement;

(l) no representation or warranty by it contained herein or in any other document furnished by it to Client or its nominated agencies in relation to the Required Consents contains or shall contain any untrue or misleading statement of material fact or omits or shall omit to state a material fact necessary to make such representation or warranty not misleading; and

(m) no sums, in cash or kind, have been paid or shall be paid, by it or on its behalf, to any person by way of fees, commission or otherwise for entering into this Agreement or for influencing or attempting to influence any officer or employee of Client or its nominated agencies in connection therewith.

2.8.2 Representations and warranties of the CLIENT or its nominated agencies

CLIENT or its nominated agencies represent and warrant to the System Integrator that:

(a) it has full power and authority to execute, deliver and perform its obligations under this Agreement and to carry out the transactions contemplated herein and that it has taken all actions necessary to execute this Agreement, exercise its rights and perform its obligations, under this Agreement and carry out the transactions contemplated hereby;

(b) it has taken all necessary actions under Applicable Laws to authorize the execution, delivery and performance of this Agreement and to validly exercise its rights and perform its obligations under this Agreement;

(c) it has the financial standing and capacity to perform its obligations under the Agreement;

(d) it is subject to the laws of India, and hereby expressly and irrevocably waives any immunity in any jurisdiction in respect of this Agreement or matters arising thereunder including any obligation, liability or responsibility hereunder;

(e) this Agreement has been duly executed by it and constitutes a legal, valid and binding obligation enforceable against it in accordance with the terms hereof and its obligations under this Agreement shall be legally valid, binding and enforceable against it in accordance with the terms thereof;

(f) the execution, delivery and performance of this Agreement shall not conflict with, result in the breach of, constitute a default under, or accelerate performance required by any of the Applicable Laws or any covenant, contract, agreement, arrangement, understanding, decree or order to which it is a party or by which it or any of its properties or assets is bound or affected;

(g) there are no actions, suits or proceedings pending or, to its knowledge, threatened against it at law or in equity before any court or before any other judicial, quasi-judicial or other authority, the outcome of which may result in the

default or breach of this Agreement or which individually or in the aggregate may result in any material impairment of its ability to perform its material (including any payment) obligations under this Agreement;

(h) it has no knowledge of any violation or default with respect to any order, writ, injunction or any decree of any court or any legally binding order of any Government Instrumentality which may result in any Adverse Effect on the Client or its nominated agencies ability to perform its obligations under this Agreement and no fact or circumstance exists which may give rise to such proceedings that would adversely affect the performance of its obligations under this Agreement;

(i) it has complied with Applicable Laws in all material respects;

(j) all information provided by it in the RFP in connection with the Project is, to the best of its knowledge and belief, true and accurate in all material respects; and

(k) upon the System Integrator performing the covenants herein, it shall not at any time during the term hereof, interfere with peaceful exercise of the rights and discharge of the obligations by the System Integrator, in accordance with this Agreement.

2.9 Undertakings of the Client or its Nominated Agencies

Without prejudice to any other undertakings or obligations of the Client or its nominated agencies under this Agreement the Client or its nominated agencies shall undertake the following:

(l) To provide any support through personnel to test the system during the Term;

(m) To provide any support through personnel and/or test data during development, rollout, steady state operation, as well as, for any changes/enhancements in the system whenever required due to scope change that may arise due to business, delivery or statutory/regulatory reasons;

(n) Client shall provide the data (including in electronic form wherever available) to be digitized or migrated.

(o) To authorize the System Integrator to interact for implementation of the Project with external entities such as the Transport Department, Government Hospitals, Courts, Jails, etc. other entities mentioned for integration requirements in Volume I of the RFP.

2.10 Obligations of the System Integrator

(a) It shall provide to the Client or its nominated agencies, the Minimum Required Deliverables as set out in Annexure C of this Agreement.

(b) It shall keep abreast of the relevant technical, managerial and operational requirements applicable to the provision of the services and best practices in this area and shall share their knowledge with Client or its nominated agencies regarding matters which would assist Client or its nominated agencies in its use of the Services, provided that System Integrator shall not be obligated to share other client information or Confidential Information of System Integrator not

relevant to this Agreement;

(c) It shall perform the Services as set out in Section 2 of this Agreement and in a professional manner commensurate with industry and technical standards which are generally in effect for international projects and innovations pursuant thereon similar to those contemplated by this Agreement, and so as to comply with the applicable Service Levels set out with this Agreement.

(d) It shall ensure that the Services are being provided as per the Project Timelines set out as Annexure C to this Agreement.

2.11 Approvals and Required Consents

(a) The Parties shall cooperate to procure, maintain and observe all relevant and regulatory and governmental licenses, clearances and applicable approvals (hereinafter the "***Required Consents***") necessary for the System Integrator to provide the Services. The costs of such Approvals shall be borne by the Party normally responsible for such costs according to local custom and practice in the locations where the Services are to be provided.

(b) The Client or its nominated agencies shall use reasonable endeavours to assist System Integrator to obtain the Required Consents. In the event that any Required Consent is not obtained, the System Integrator and the Client or its nominated agencies will co-operate with each other in achieving a reasonable alternative arrangement as soon as reasonably practicable for the Client or its nominated agencies to continue to process its work with as minimal interruption to its business operations as is commercially reasonable until such Required Consent is obtained, provided that the System Integrator shall not be relieved of its obligations to provide the Services and to achieve the Service Levels until the Required Consents are obtained if and to the extent that the System Integrator's obligations are not dependent upon such Required Consents.

2.12 Use of Assets by the System Integrator

During the Term the System Integrator shall:

(a) take all reasonable and proper care of the entire hardware and software, network or any other information technology infrastructure components used for the Project and other facilities leased / owned / operated by the System Integrator exclusively in terms of ensuring their usability for the delivery of the Services as per this Agreement (hereinafter the "Assets") in proportion to their use and control of such Assets which will include all upgradation/enhancements and improvements to meet the current needs of the Project; and

(b) keep all the tangible Assets in as good and serviceable condition (reasonable wear and tear excepted) and/or the intangible Assets suitably upgraded subject to the relevant industry standards (including those stated in Volume I of the RFP) as at the date the System Integrator takes control of and/or first uses the Assets and during the entire Term of the Agreement. Pursuant to technological obsolescence, upgradation will be carried out by the System Integrator.

(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;

(d) take such steps as may be properly recommended by the manufacturer of the Assets and notified to the System Integrator or as may, in the reasonable opinion of the System Integrator, be necessary to use the Assets in a safe manner;

(e) ensure that the Assets that are under the control of the System Integrator, are kept suitably housed and in conformity with Applicable Law;

(f) procure permission from the Client or its nominated agencies and any persons duly authorized by them to enter any land or premises on which the Assets are for the time being sited so as to inspect the same, subject to any reasonable third party requirements;

(g) 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 Applicable Law; and

(h) be responsible for undertaking comprehensive insurance including liability insurance, system and facility insurance and any other insurance for the personnel, Assets, data, software, etc.

2.13 Access to the Client or its Nominated Agencies Locations

For so long as the System Integrator provides services to the Client or its nominated agencies location, as the case may be, on a non-permanent basis and to the extent necessary, the Client as the case may be or its nominated agencies shall, subject to compliance by the System Integrator with any safety and security guidelines which may be provided by the Client as the case may be or its nominated agencies and notified to the System Integrator in writing, provide the System Integrator with:

(a) reasonable access, in the same manner granted to the Client or its nominated agencies employees, to the Client as the case may be location twenty-four hours a day, seven days a week;

(b) reasonable work space, access to office equipment as mutually agreed and other related support services in such location and at such other the Client as the case may be location, if any, as may be reasonably necessary for the System Integrator to perform its obligations hereunder and under the SLA.

Access to locations, office equipments and services shall be made available to the System Integrator on an "as is, where is" basis by the Client as the case may be or its nominated agencies. The System Integrator agrees to ensure that its employees, agents and contractors shall not use the location, services and equipment referred to in RFP Volume 1 for the following purposes:

(a) for the transmission of any material which is defamatory, offensive or abusive or of an obscene or menacing character; or

(b) in a manner which constitutes a violation or infringement of the rights of any person, firm or company (including but not limited to rights of copyright or

confidentiality).

2.14 Management Phase

2.14.1 Governance

The review and management process of this Agreement shall be carried out in accordance with the Governance Schedule set out in Schedule V of this Agreement and shall cover all the management aspects of the Project.

2.14.2 Use of Services

(a) The Client as the case may be or its nominated agencies, will undertake and use the Services in accordance with any instructions or procedures as per the acceptance criteria as set out in the SLA or this Agreement or any agreement that may be entered into between the Parties from time to time;

(b) The Client as the case may be or its nominated agencies shall be responsible for the operation and use of the Deliverables resulting from the Services.

2.14.3 Changes

Unless expressly dealt with elsewhere in this Agreement, any changes under or to this Agreement or under or to the SLA shall be dealt with in accordance with the Change Control Schedule set out in Schedule II of this Agreement.

2.14.4 Security And Safety

(a) The System Integrator shall comply with the directions issued from time to time by the Client or its nominated agencies and follow the industry standards related to safety and security (including those as stated in the RFP Volume I), insofar as it applies to the provision of the Services.

(b) Each Party to the SLA/Agreement shall also comply with CLIENT or the Government of India, and the respective State's security standards and policies in force from time to time at each location of which CLIENT or its nominated agencies make the System Integrator aware in writing insofar as the same apply to the provision of the Services.

(c) The Parties to the SLA/Agreement shall use reasonable endeavours to report forthwith in writing to each other all identified attempts (whether successful or not) by unauthorized persons (including unauthorized persons who are employees of any Party) either to gain access to or interfere with the CLIENT as the case may be or any of their nominees data, facilities or Confidential Information.

(d) The System Integrator shall upon reasonable request by the CLIENT as the case may be or their nominee(s) participate in regular meetings when safety and information technology security matters are reviewed.

(e) As per the provisions of the SLA or this Agreement, the System Integrator shall promptly report in writing to the CLIENT or its nominated agencies, any act or

omission which they are aware that could have an adverse effect on the proper conduct of safety and information technology security at the facilities of CLIENT as the case may be.

2.14.5 Cooperation

Except as otherwise provided elsewhere in this Agreement or the SLA, each Party ("***System Integrator***") to this Agreement or to the SLA undertakes promptly to provide the other Party ("***Client***") with all such information and co-operation which the Client reasonably requests, provided that such information and co-operation:

(a) does not require material expenditure by the Providing Party to provide the same;

(b) is reasonably required by the Receiving Party in order for it to comply with its obligations under this Agreement or the SLA;

(c) cannot be construed to be Confidential Information; and

(d) is capable of being provided by the Providing Party.

Further, each Party agrees to co-operate with the contractors and subcontractors of the other Party as reasonably requested in order to accomplish the purposes of this Agreement.

2.15 Finances

2.15.1 Terms of Payment and Service Credits and Debits

(a) In consideration of the Services and subject to the provisions of this Agreement and of the SLA, the CLIENT shall pay the System Integrator for the Services rendered in pursuance of this agreement, in accordance with the Terms of Payment Schedule set out as Schedule VI of this Agreement.

(b) All payments are subject to the application of service credits and debits as may be provided for in the SLA. For the avoidance of doubt, it is expressly clarified that the CLIENT will pay the service credits as stated in accordance with the Schedule VI of this Agreement and the CLIENT may also calculate a financial sum and debit the same against the terms of payment as set out in Schedule VI of this Agreement as a result of the failure of the System Integrator to meet the Service Level as defined in SLA.

(c) Save and except as otherwise provided for herein or as agreed between the Parties in writing, the CLIENT shall not be required to make any payments in respect of the Services (or, without limitation to the foregoing, in respect of the System Integrator performance of any obligations under this Agreement or the SLA) other than those covered in Schedule VI of this Agreement. For the avoidance of doubt, it is expressly clarified that the payments shall be deemed to include all ancillary and incidental costs and charges arising in the course of delivery of the Services including consultancy charges, infrastructure costs, project costs, implementation and management charges and all other related costs including taxes which are addressed in this Clause.

2.15.2 Invoicing and Settlement

(a) Subject to the specific terms of the SLA, the System Integrator shall submit its invoices in accordance with the following principles:

i. The CLIENT shall be invoiced by the System Integrator for the Services. Generally and unless otherwise agreed in writing between the Parties or expressly set out in the SLA, the System Integrator shall raise an invoice along with necessary approvals as per Schedule VI of this Agreement on Half yearly basis; and

ii. Any invoice presented in accordance with this Article shall be in a form agreed with the CLIENT.

(b) The System Integrator alone shall invoice all payments after receiving due approval from the competent authority. Such invoices shall be accurate and all adjustments to or changes in the terms of payment as stated in Schedule VI of this Agreement. 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 change relating to such Service is authorized or incurred, whichever is later.

(c) Payment shall be made within 30 working days of the receipt of invoice along with supporting documents by the CLIENT subject to penalties. The penalties are imposed on the vendor as per the SLA criteria specified in the SLA.

(d) The CLIENT shall be entitled to delay or withhold payment of any invoice or part of it delivered by the System Integrator under Schedule VI of this Agreement where the CLIENT disputes/ withholds such invoice or part of it provided that such dispute is bona fide. The withheld amount shall be limited to that which is in dispute. The disputed / withheld amount shall be settled in accordance with the escalation procedure as set out in Schedule V of this Agreement. Any exercise by the CLIENT under this Clause shall not entitle the System Integrator to delay or withhold provision of the Services.

(e) The CLIENT shall be entitled to delay or withhold payment of any invoice or part of it delivered by the System Integrator under Schedule V of this Agreement where the disputes any previous invoice or part of it that it had not previously disputed provided that such dispute is bona fide. The withheld amount shall be limited to that which is the disputed amount. The disputed amount shall be referred to the escalation procedure as set out in Schedule V of this Agreement. Any exercise by the CLIENT under this Clause shall not entitle the System Integrator to delay or withhold provision of the Services.

(f) The System Integrator shall pay all its sub-contractors in a timely fashion in accordance with a mechanism, which will not prejudice the Project.

2.15.3 Tax

(a) The CLIENT or its nominated agencies 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 other taxes in connection with this

Agreement, SLA, scope of work and any other engagement required to be undertaken as a part of this Agreement, including, but not limited to, property, sales, use, excise, value-added, goods and services, consumption and other similar taxes or duties.

(b) The CLIENT or its nominated agencies shall provide System Integrator with the original tax receipt of any withholding taxes paid by CLIENT or its nominated agencies on payments under this Agreement. The System Integrator agrees to reimburse and hold the CLIENT or its nominated agencies harmless from any deficiency including penalties and interest relating to taxes that are its responsibility under this paragraph. For purposes of this Agreement, taxes shall include taxes incurred on transactions between and among the CLIENT or its nominated agencies, the System Integrator and third party subcontractors.

(c) In the event of any increase or decrease of the rate of taxes due to any statutory notification/s during the Term of the Agreement the consequential effect shall be to the account of the System Integrator.

(d) 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 the following:

i. any resale certificates;
ii. any relevant information regarding out-of-state or use of materials, equipment or services; and
iii. any direct pay permits, exemption certificates or information reasonably requested by the other Party.

2.16 Termination

2.16.1 Material Breach

(a) In the event that either Party believes that the other Party is in Material Breach of its obligations under this Agreement, such aggrieved Party may terminate this Agreement upon giving a one month's notice for curing the Material Breach to the other Party. In case the Material Breach continues, after the notice period, the CLIENT as the case may be will have the option to terminate the Agreement. Any notice served pursuant to this Clause shall give reasonable details of the Material Breach, which could include the following events and the termination will become effective:

i. If the System Integrator is not able to deliver the services as per the SLAs defined in Volume 1 of RFP which translates into Material Breach, then the CLIENT may serve a 7 days written notice for curing this Material Breach. In case the Material Breach continues, after the expiry of such notice period, the CLIENT will have the option to terminate this Agreement. Further, the CLIENT may after affording a reasonable opportunity to the System Integrator to explain the circumstances leading to such a delay.

ii. If there is a Material Breach by the CLIENT or its nominated agencies which results in not providing support for effecting data migration and / or

not providing the certification of User Acceptance, then the System Integrator will give a one month's notice for curing the Material Breach to the CLIENT. After the expiry of such notice period, the System Integrator will have the option to terminate the Agreement

(b) The CLIENT may by giving a one month's written notice, terminate this Agreement if a change of control of the System Integrator has taken place. For the purposes of this Clause, in the case of System Integrator, change of control shall mean the events stated in Clause 2.7.3, and such notice shall become effective at the end of the notice period as set out in Clause 2.7.3 (c).

(c) In the event that System Integrator undergoes such a change of control, CLIENT may, as an alternative to termination, require a full Performance Guarantee for the obligations of System Integrator by a guarantor acceptable to CLIENT or its nominated agencies. If such a guarantee is not furnished within 30 days of CLIENT's demand, the CLIENT may exercise its right to terminate this Agreement in accordance with this Clause by giving 15 days further written notice to the System Integrator.

(d) The termination provisions set out in this Clause shall apply mutatis mutandis to the SLA.

2.16.2 Effects of termination

(a) In the event that CLIENT 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 Guarantee furnished by System Integrator may be forfeited.

(b) Upon termination of this Agreement, the Parties will comply with the Exit Management Schedule set out as Schedule III of this Agreement.

(c) In the event that CLIENT or the System Integrator terminates this Agreement, the compensation will be decided in accordance with the Terms of Payment Schedule set out as Schedule VI of this Agreement.

(d) On termination of this Agreement for any reason, the CLIENT will decide the appropriate course of action.

2.16.3 Termination of this Agreement due to bankruptcy of System Integrator

The CLIENT may serve written notice on System Integrator at any time to terminate this Agreement with immediate effect in the event that:

(a) The System Integrator reporting an apprehension of bankruptcy to the CLIENT or its nominated agencies;

(b) CLIENT or its nominated agencies apprehending a similar event.

2.17 Indemnification

2.17.1 Subject to Clause 3.17.2 below, System Integrator (the "Indemnifying Party") undertakes to indemnify CLIENT (the "Indemnified Party") from and against all Losses on account of bodily injury, death or damage to tangible personal property arising in favour of any person, corporation or other entity (including the Indemnified Party) attributable to the Indemnifying Party's performance or non-performance under this Agreement or the SLA to the extent of the Indemnifying Party's comparative fault in causing such Losses.

2.17.2 The indemnities set out in Clause 3.17.1 shall be subject to the following conditions:

(a) the Indemnified Party as promptly as practicable informs the Indemnifying Party in writing of the claim or proceedings and provides all relevant evidence, documentary or otherwise;

(b) the Indemnified Party shall, at the cost of the Indemnifying Party, give the Indemnifying Party all reasonable assistance in the Defense of such claim including reasonable access to all relevant information, documentation and personnel provided that the Indemnified Party may, at its sole cost and expense, reasonably participate, through its attorneys or otherwise, in such Defense;

(c) if the Indemnifying Party does not assume full control over the Defense of a claim as provided in this Article, 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;

(d) the Indemnified Party shall not prejudice, pay or accept any proceedings or claim, or compromise any proceedings or claim, without the written consent of the Indemnifying Party;

(e) all settlements of claims subject to indemnification under this Article will:

i. 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

ii. include any appropriate confidentiality agreement prohibiting disclosure of the terms of such settlement;

(f) the Indemnified Party shall account to the Indemnifying Party for all awards, settlements, damages and costs (if any) finally awarded in favour of the Indemnified Party which are to be paid to it in connection with any such claim or proceedings;

(g) the Indemnified Party shall take steps that the Indemnifying Party may reasonably require to mitigate or reduce its loss as a result of such a claim or proceedings;

(h) in the event that the Indemnifying Party is obligated to indemnify an Indemnified Party pursuant to this Article, the Indemnifying Party will, upon payment of such indemnity in full, be subrogated to all rights and defenses of the Indemnified Party with respect to the claims to which such indemnification relates; and

(i) if a Party makes a claim under the indemnity set out under Clause 3.17.1 above

in respect of any particular Loss or Losses, then that Party shall not be entitled to make any further claim in respect of that Loss or Losses (including any claim for damages).

2.18 Force Majeure

2.18.1 Definition of Force Majeure

The System Integrator or the CLIENT as the case may be, shall be entitled to suspend or excuse performance of its respective obligations under this Agreement to the extent that such performance is impeded by an event of force majeure ('*Force Majeure*').

2.18.2 Force Majeure events

A Force Majeure event means any event or circumstance or a combination of events and circumstances referred to in this Clause, which:

(a) is beyond the reasonable control of the affected Party;

(b) such Party could not have prevented or reasonably overcome with the exercise of reasonable skill and care;

(c) does not result from the negligence of such Party or the failure of such Party to perform its obligations under this Agreement;

(d) is of an incapacitating nature and prevents or causes a delay or impediment in performance; and

(e) may be classified as all or any of the following events:

Such events include:

Non-Political Events

(a) act of God, including earthquake, flood, inundation, landslide, exceptionally adverse weather conditions, storm, tempest, hurricane, cyclone, lightning, thunder, volcanic eruption, fire or other extreme atmospheric conditions;

(b) radioactive contamination or ionizing radiation or biological contamination except as may be attributable to the System Integrator's use of radiation or radio-activity or biologically contaminating material;

(c) strikes, lockouts, boycotts, labour disruptions or any other industrial disturbances as the case may be not arising on account of the acts or omissions of the System Integrator and which affect the timely implementation and continued operation of the Project; or

(d) any event or circumstances of a nature analogous to any of the foregoing.

Political Events

(a) Change in Law, other than any Change in Law for which relief is provided under

this Agreement;

(b) expropriation or compulsory acquisition by the CLIENT or any of their nominated agencies of any material assets or rights of the Implementing Partner;

(c) unlawful or unauthorised revocation of, or refusal by CLIENT or any of their nominated agencies, GoI or any of its agencies to renew or grant any clearance or Required Consents required by the System Integrator to perform its obligations without valid cause, provided that such delay, modification, denial, refusal or revocation did not result from the System Integrator's inability or failure to comply with any condition relating to grant, maintenance or renewal of such Required Consents applied on a non-discriminatory basis;

(d) any judgment or order of any court of competent jurisdiction or statutory authority in India made against the System Integrator in any proceedings for reasons other than failure of the System Integrator to comply with Applicable Laws or Required Consents or on account of breach thereof, or of any contract, or enforcement of this Agreement or exercise of any of its rights under this Agreement;

(e) expropriation or compulsory acquisition by the CLIENT or any of their nominated agencies of any material assets or rights of the System Integrator;

(f) unlawful or unauthorized revocation of, or refusal by any authority other than the CLIENT or any of their nominated agencies to renew or grant any Required Consents required by the System Integrator to perform its obligations without valid cause, provided that such delay, modification, denial, refusal or revocation did not result from the System Integrator's inability or failure to comply with any condition relating to grant, maintenance or renewal of such Required Consents applied on a non-discriminatory basis;

(g) any requisition of the Project by any other authority; or

(h) any requisition of the Project by the CLIENT or any of their nominated agencies.

(i) For the avoidance of doubt, suspension of the Project in accordance with the provisions of this Agreement shall not be considered a requisition for the purposes of Force Majeure event.

Other Events

(a) an act of war (whether declared or undeclared), hostilities, invasion, armed conflict or act of foreign enemy, blockade, embargo, prolonged riot, insurrection, terrorist or military action, civil commotion or politically motivated sabotage, for a continuous period exceeding seven (7) days.

For the avoidance of doubt, it is expressly clarified that the failure on the part of the System Integrator under this Agreement or the SLA to implement any disaster contingency planning and back-up and other data safeguards in accordance with the terms of this Agreement or the SLA against natural disaster, fire, sabotage or other similar occurrence shall not be deemed to be a Force Majeure event.

2.18.3 Notification procedure for Force Majeure

(a) The affected Party shall notify the other Party of a Force Majeure event within seven (7) days of occurrence of such event. If the other Party disputes the claim for relief under Force Majeure it shall give the claiming Party written notice of such dispute within thirty (30) days of such notice. Such dispute shall be dealt with in accordance with the dispute resolution mechanism in accordance with Clause

(b) Upon cessation of the situation which led the Party claiming Force Majeure, the claiming Party shall within seven (7) days hereof notify the other Party in writing of the cessation and the Parties shall as soon as practicable thereafter continue performance of all obligations under this Agreement.

2.18.4 Allocation of costs arising out of Force Majeure

(a) Upon the occurrence of any Force Majeure Event prior to the Effective Date, the Parties shall bear their respective costs and no Party shall be required to pay to the other Party any costs thereof.

(b) Upon occurrence of a Force Majeure Event after the Effective Date, the costs incurred and attributable to such event and directly relating to the Project ('Force Majeure Costs') shall be allocated and paid as follows:

- upon occurrence of a Non-Political Event, the Parties shall bear their respective Force Majeure Costs and neither Party shall be required to pay to the other Party any costs thereof.
- upon occurrence of an Other Event of Force Majeure, all Force Majeure Costs attributable to such Other Event, and not exceeding the Insurance Cover for such Other Event, shall be borne by the Implementing Partner and to the extent Force Majeure costs exceed such Insurance Cover, one half of such excess amount shall be reimbursed by CLIENT to the Implementing Partner.
- upon occurrence of a Political Event, all Force Majeure Costs attributable to such Political Event shall be reimbursed by CLIENT to the Implementing Partner.
- For the avoidance of doubt, Force Majeure Costs may include interest payments on debt, operation and maintenance expenses, any increase in the cost of the Services on account of inflation and all other costs directly attributable to the Force Majeure Event.
- Save and except as expressly provided in this Clause, neither Party shall be liable in any manner whatsoever to the other Party in respect of any loss, damage, costs, expense, claims, demands and proceedings relating to or arising out of occurrence or existence of any Force Majeure Event or exercise of any right pursuant hereof.

2.18.5 Consultation and duty to mitigate

(a) Except as otherwise provided in this Clause, the affected Party shall, at its own cost, take all steps reasonably required to remedy and mitigate the effects of the

Force Majeure event and restore its ability to perform its obligations under this Agreement as soon as reasonably practicable. The Parties shall consult with each other to determine the reasonable measures to be implemented to minimize the losses of each Party resulting from the Force Majeure event. The affected Party shall keep the other Parties informed of its efforts to remedy the effect of the Force Majeure event and shall make reasonable efforts to mitigate such event on a continuous basis and shall provide written notice of the resumption of performance hereunder.

2.19 Confidentiality

(a) The CLIENT or its nominated agencies shall allow the System Integrator to review and utilize highly confidential public records and the System Integrator shall maintain the highest level of secrecy, confidentiality and privacy with regard thereto.

(b) Additionally, the System Integrator shall keep confidential all the details and information with regard to the Project, including systems, facilities, operations, management and maintenance of the systems/facilities.

(c) The CLIENT or its nominated agencies 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 System Integrator shall ensure that all its employees, agents and sub-contractors execute individual non disclosure agreements, which have been duly approved by the CLIENT with respect to this Project.

(e) For the avoidance of doubt, it is expressly clarified that the aforesaid provisions shall not apply to the following information:

- information already available in the public domain;
- information which has been developed independently by the System Integrator;
- information which has been received from a third party who had the right to disclose the aforesaid information;
- information which has been disclosed to the public pursuant to a court order.

2.20 Audit, Access and Reporting

The System Integrator shall allow access to the CLIENT or its nominated agencies to all information which is in the possession or control of the System Integrator and which relates to the provision of the Services as set out in the Audit, Access and Reporting Schedule and which is reasonably required by the CLIENT to comply with the terms of the Audit, Access and Reporting Schedule set out as Schedule IV of this Agreement.

2.21 Intellectual Property Rights

2.21.1 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 in the name of CLIENT. Bidder would be responsible for arranging any licenses associated with products. "**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 CLIENT for license which is published by product owner or its affiliates, or a third party. "**Fixes**" means product fixes that are either released generally (such as commercial product service packs) or that are provided to you when performing services (such as workarounds, patches, bug fixes, beta fixes and beta builds) and any derivatives of the foregoing.

2.21.2 Customized CAS (State)

SI shall neither hold nor shall claim to have any type of right(s) for the customization made in the Core Application Software (State) or on the additionally developed modules/ applications/ utilities/ APIs including source code and material (including upgrade/ updates/ fixes/ patches/etc.), as done during the implementation of the project and shall always lie with the CLIENT.

2.21.3 Bespoke development:

The IPR rights for any bespoke development done during the implementation of the project will lie with CLIENT.

2.21.4 Pre-existing work:

All IPR including the source code and materials (other than products or fixes) developed or otherwise obtained independently of the efforts of a party under this agreement ("**pre-existing work**") shall remain the sole property of that party. During the performance of the services for this agreement, each party grants to the other party (and their sub-contractors as necessary) a non-exclusive license to use, reproduce and modify any of its pre-existing work provided to the other party solely for the performance of such services. Except as may be otherwise explicitly agreed to in a statement of services, upon payment in full, the bidder should grant CLIENT a non-exclusive, perpetual, full use, fully paid-up enterprise edition license(s) to use, reproduce and modify (if applicable) the pre-existing work in the form delivered to CLIENT as part of the service deliverables only for its internal business operations. Under such license either of parties will have no right to sell the pre-existing work of the other party to a Third Party.

CLIENT's license to pre-existing work is conditioned upon its compliance with the terms of this agreement and the perpetual license applies solely to the pre-existing work that bidder leaves with CLIENT at the conclusion of performance of the services.

2.22 Miscellaneous

2.22.1 Personnel

(a) The personnel assigned by System Integrator to perform the Services shall be employees of System Integrator, and under no circumstances shall such personnel be considered employees of CLIENT or its nominated agencies. The System Integrator shall have the sole responsibility for the supervision and control of its personnel and for payment of such personnel's compensation, including salary, withholding of income taxes and social security taxes, worker's compensation, employee and disability benefits and the like and shall be responsible for all obligations of an employer subject to Applicable Law.

(b) The System Integrator shall use its best efforts to ensure that sufficient System Integrator personnel are assigned to perform the Services and that such personnel have appropriate qualifications to perform the Services. After discussion with System Integrator, CLIENT or its nominated agencies shall have the right to require the removal or replacement of any System Integrator personnel performing work under this Agreement. In the event that CLIENT or its nominated agencies requests that any System Integrator personnel be replaced, the substitution of such personnel shall be accomplished pursuant to a mutually agreed upon schedule.

(c) The System Integrator shall also be responsible to train certain employees of CLIENT, or its nominated agencies with regard to the Services being provided by the System Integrator as and when required by the CLIENT or its nominated agencies during the Term of this Project. The parameters of the training required for these employees of CLIENT or its nominated agencies shall be communicated by CLIENT or its nominated agencies to the System Integrator periodically and shall be in accordance with the latest procedures and processes available in the relevant areas of work.

(d) In the event that the CLIENT or its nominated agencies identifies any personnel of System Integrator as "Key Personnel", then neither the System Integrator shall remove such personnel from the CLIENT or its nominated agencies engagement without the prior written consent of CLIENT or its nominated agencies unless such removal is the result of an unavoidable circumstance including but not limited to resignation, termination, medical leave, etc.

(e) Except as stated in this Clause, nothing in this Agreement or the SLA will limit the ability of System Integrator to freely assign or reassign its employees; provided that System Integrator shall be responsible, at its expense, for transferring all appropriate knowledge from personnel being replaced to their replacements. CLIENT or its nominated agencies shall have the right to review and approve System Integrator's plan for any such knowledge transfer. System Integrator shall maintain the same or higher standards for skills and professionalism among replacement personnel as in personnel being replaced.

(f) Each Party shall be responsible for the performance of all its obligations under this Agreement or the SLA as the case may be and shall be liable for the acts and omissions of its employees and agents in connection therewith.

(g) Neither Party will solicit for employment or knowingly hire an employee of the other Party with whom such Party has contact pursuant to project engagements under this Agreement. This restriction shall not apply to employees of either Party responding to advertisements in job fairs or news media circulated to the general public.

2.22.2 Independent Contractor

Nothing in this Agreement or the SLA shall be construed as establishing or implying any partnership or joint venture between the Parties to this Agreement or the SLA and, except as expressly stated in this Agreement or the SLA, nothing in this Agreement or the SLA shall be deemed to constitute any Parties as the agent of any other Party or authorizes either Party to:

(a) incur any expenses on behalf of the other Party;

(b) enter into any engagement or make any representation or warranty on behalf of the other Party;

(c) pledge the credit of or otherwise bind or oblige the other Party; or

(d) commit the other Party in any way whatsoever without in each case obtaining the other Party's prior written consent.

2.22.3 Sub-contractors

System Integrator shall not subcontract any work related to the data recovery centre, data centre, security, etc. other Core activities to be performed under this Agreement without CLIENT's prior written consent. However the System Integrator shall provide the list of all the other services planned to be sub contracted with the Technical proposal. It is clarified that the System Integrator shall be the principal employer for all claims arising from the liabilities statutory or otherwise, concerning the sub-contractors. The System Integrator undertakes to indemnify the CLIENT or its nominated agencies from any claims on the grounds stated hereinabove.

2.22.4 Assignment

(a) All terms and provisions of this Agreement shall be binding on and shall inure to the benefit of the CLIENT and their respective successors and permitted assigns.

(b) Subject to Clause 2.7.3 above, the System Integrator shall not be permitted to assign its rights and obligations under this Agreement to any third party.

(c) The CLIENT may assign or novate all or any part of this Agreement and Schedules/Annexure, and the System Integrator shall be a party to such novation, to any third party contracted to provide outsourced services to CLIENT or any of its nominees.

2.22.5 Trademarks, Publicity

Neither Party may use the trademarks of the other Party without the prior written consent of the other Party. Except as required by law or the rules and regulations of each stock exchange upon

which the securities of one of the Parties is listed, neither Party shall publish or permit to be published either along or in conjunction with any other person any press release, information, article, photograph, illustration or any other material of whatever kind relating to this Agreement, the SLA or the business of the Parties without prior reference to and approval in writing from the other Party, such approval not to be unreasonably withheld or delayed provided however that System Integrator may include CLIENT or its client lists for reference to third parties subject to the prior written consent of CLIENT not to be unreasonably withheld or delayed. Such approval shall apply to each specific reference and relate only to that reference.

2.22.6 Notices

(a) Any notice or other document which may be given by either Party under this Agreement or under the SLA shall be given in writing in person or by pre-paid recorded delivery post, email or by facsimile transmission.

(b) In relation to a notice given under this Agreement, any such notice or other document shall be addressed to the other Party's principal or registered office address as set out below:

Director General of Police, Haryana

Police Headquarters, Sector -6, Panchkula

Haryana

Tel:

Fax:

Email:

Contact:

With a copy to:

System Integrator

Tel:

Fax:

Email:

Contact:

(c) In relation to a notice given under the MSA / SLA, a Party shall specify the Parties' address for service of notices, any such notice to be copied to the Parties at the addresses set out in this Clause.

(d) Any such notice or other document shall be deemed to have been given to the other Party (or, if relevant, its relevant associated company) when delivered (if delivered in person) if delivered between the hours of 9.00 am and 5.00 pm at the address of the other Party set forth above or if sent by fax, provided the copy

fax is accompanied by a confirmation of transmission, or on the next working day thereafter if delivered outside such hours, and 7 days from the date of posting (if by letter).

(e) Either Party to this Agreement or to the SLA may change its address, telephone number, facsimile number and nominated contact for notification purposes by giving the other reasonable prior written notice of the new information and its effective date.

2.22.7 Variations and Further Assurance

(a) No amendment, variation or other change to this Agreement or the SLA shall be valid unless authorised in accordance with the change control procedure as set out in the Change Control Schedule set out in Schedule II of this Agreement. Such amendment shall be made in writing and signed by the duly authorised representatives of the Parties to this Agreement or the SLA.

(b) Each Party to this Agreement or the SLA agrees to enter into or execute, without limitation, whatever other agreement, document, consent and waiver and to do all other things which shall or may be reasonably required to complete and deliver the obligations set out in this Agreement or the SLA.

2.22.8 Severability and Waiver

(a) If any provision of this Agreement or the SLA, 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 Agreement or the SLA 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.

(b) No failure to exercise or enforce and no delay in exercising or enforcing on the part of either Party to this Agreement or the SLA of any right, remedy or provision of this Agreement or the SLA shall 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.

2.22.9 Compliance with Applicable Law

Each Party to this Agreement and the SLA accepts that its individual conduct shall (to the extent applicable to it) at all times comply with all laws, rules and regulations of government and other bodies having jurisdiction over the area in which the Services are undertaken provided that changes in such laws, rules and regulations which result in a change to the Services shall be

dealt with in accordance with the Change Control Schedule set out in Schedule II of this Agreement. For the avoidance of doubt the obligations of the Parties to this Agreement and the SLA are subject to their respective compliance with all local, state, national, supra-national, foreign and international laws and regulations.

2.22.10 Professional Fees

All expenses incurred by or on behalf of each Party to this Agreement and the SLA, including all fees of agents, legal advisors, accountants and actuaries employed by either of the Parties in connection with the negotiation, preparation and execution of this Agreement or the SLA shall be borne solely by the respective Party which incurred them.

2.22.11 Ethics

The System Integrator represents, warrants and covenants that it has given no commitments, payments, gifts, kickbacks, lavish or expensive entertainment, or other things of value to any employee or agent of CLIENT or its nominated agencies in connection with this agreement and acknowledges that the giving of any such payment, gifts, entertainment, or other things of value is strictly in violation of CLIENT standard policies and may result in cancellation of this Agreement, or the SLA.

2.22.12 Entire Agreement

This Agreement and the SLA with all schedules & annexure appended thereto and the contents and specifications of the Volumes I and II of the RFP constitute the entire agreement between the Parties with respect to their subject matter, and as to all other representations, understandings or agreements which are not fully expressed herein, provided that nothing in this Clause shall be interpreted so as to exclude any liability in respect of fraudulent misrepresentation.

2.22.13 Amendment

Any amendment to this Agreement shall be made in accordance with the Change Control Schedule set out in Schedule II of this Agreement by mutual written consent of all the Parties.

2.23 Dispute Resolution

(a) Any dispute arising out of or in connection with this Agreement or the SLA shall in the first instance be dealt with in accordance with the escalation procedure as set out in the Governance Schedule set out as Schedule V of this Agreement.

(b) Any dispute or difference whatsoever arising between the parties to this Contract out of or relating to the construction, meaning, scope, operation or effect of this Contract or the validity of the breach thereof shall be referred to a sole Arbitrator to be appointed by Client only. If the System Integrator cannot agree on the appointment of the Arbitrator within a period of one month from the notification by one party to the other of existence of such dispute, then the ultimate Arbitrator shall be Financial Commissioner & Principal Secretary to Government of Haryana, Home Department, Haryana. The provisions of the Arbitration and Conciliation Act, 1996 will be applicable and the award made there under shall

be final and binding upon the parties hereto, subject to legal remedies available under the law. Such differences shall be deemed to be a submission to arbitration under the Indian Arbitration and Conciliation Act, 1996, or of any modifications, Rules or re-enactments thereof. The Arbitration proceedings will be held at Chandigarh, India. Any legal dispute will come under Haryana State jurisdiction.

IN WITNESS WHEREOF THE PARTIES HERETO HAVE HERE UNTO SET THEIR RESPECTIVE HANDS THE DAY AND THE YEAR FIRST ABOVE WRITTEN.

WITNESSES:-

1. Signature _____
Name _____
Designation _____
Date _____

Signature _____
Name _____
Designation _____
Date _____

2. Signature _____
Name _____
Designation _____
Date _____

For and on behalf of Governor of Haryana

WITNESSES:-

1. Signature _____
Name _____
Designation _____
Date _____

Signature _____
Name _____
Designation _____
Address _____
Date _____

2. Signature _____
Name _____
Designation _____
Date _____

For and on behalf of the System Integrator

3 SCHEDULES

3.1 Schedule - I: Definitions

Adverse Effect	means material adverse effect on (a) the ability of the System Integrator to exercise any of its rights or perform/discharge any of its duties/obligations under and in accordance with the provisions of this Agreement and/or (b) the legal validity, binding nature or enforceability of this Agreement;
Agreement	means this Master Services Agreement, Service Level Agreement and Non-Disclosure Agreement together with all Articles, Annexure, Schedules and the contents and specifications of the Volumes I and II of the RFP;
Applicable Law(s)	means any statute, law, ordinance, notification, rule, regulation, judgment, order, decree, bye-law, approval, directive, guideline, policy, requirement or other governmental restriction or any similar form of decision of, or determination by, or any interpretation or administration of the Client as may be in effect on the date of the execution of this Agreement and during the subsistence thereof, applicable to the Project;
Assets	shall have the same meaning ascribed to it in Clause 2.12 (a)
Software	means the software (including CAS (State)) designed, developed / customized, tested and deployed by the System Integrator for the purposes of the Project and includes the source code (in case of Bespoke development) along with associated documentation, which is the work product of the development efforts involved in the Project and the improvements and enhancements effected during the term of the Project, but does not include the proprietary software components and tools deployed by the System Integrator;
Business Hours	shall mean the working time for Haryana Police IT Cell personnel which is 9:00 AM to 7:00 PM. Again for Servers and other components which enable successful usage of CCTNS solution the working time should be considered as 24 hours for all the days of the week. It is desired that IT maintenance, other batch processes (like backup) etc. should be planned so that such backend activities have minimum effect on the performance;
Certificate(s) of Compliance	shall have the same meaning ascribed to it in Clause 2.7.4.;
Confidential Information	means all information including Haryana Police Data (whether in written, oral, electronic or other format) which relates to the technical, financial and business affairs, which is disclosed to or otherwise learned by the System Integrator in the course of or in connection with this Agreement (including

	without limitation such information received during negotiations, location visits and meetings in connection with this Agreement);
Control	means, in relation to any business entity, the power of a person to secure (i) by means of the holding of shares or the possession of voting power in or in relation to that or any other business entity, or (ii) by virtue of any powers conferred by the articles of association or other document regulating that or any other business entity, that the affairs of the first mentioned business entity are conducted in accordance with that person's wishes and in relation to a partnership, means the right to a share of more than one half of the assets, or of more than one half of the income, of the partnership;
CCTNS Solution	Shall comprise of software, hardware and networking components used for implementation of CCTNS project in Haryana Police
Deliverables	means the products, infrastructure and services agreed to be delivered by the System Integrator in pursuance of the agreement as defined more elaborately in Volume I and Volume II of the RFP, Implementation and the Maintenance phases and includes all documents related to the user manual, technical manual, design, process and operating manuals, service mechanisms, policies and guidelines (such as security related, data migration related), inter alia payment and/or process related etc., source code and all its modifications;
Proprietary Information	shall have the same meaning ascribed to it in Clause 2.21.1
Effective Date	shall have the same meaning ascribed to it in Clause 2.5.1 (iv)
Haryana Police Data	means all proprietary data of the department or its nominated agencies generated out of operations and transactions, documents all taxpayers data and related information including but not restricted to user data which the System Integrator obtains, possesses or processes in the context of providing the Services to the users pursuant to this Agreement;
Final Acceptance Test	shall be conducted on completion of the following: 1) CCTS Solution deployed and Operational at State Data Center 2) Deployment & operational hardware and networking at requisite locations, 3) UAT of the overall integrated solution and portal.
Final Testing and Certification Agency	shall have the same meaning ascribed to it in Clause 2.7.4
Force Majeure	shall have the same meaning ascribed to it in Clause 2.18.1

Force Majeure Costs	shall have the same meaning ascribed to it in Clause 2.18.4
GoI	means the Government of India;
Indemnifying Party	shall have the same meaning ascribed to it in Clause 2.17
Indemnified Party	shall have the same meaning ascribed to it in Clause 2.17
Intellectual Property Rights	means all rights in written designs and copyrights, moral rights, rights in databases and Bespoke Software/ CAS (State)/ Pre-existing work including its up-gradation systems and compilation rights (whether or not any of these are registered and including application for registration);
Insurance Cover	means the aggregate of the maximum sums insured under the insurances taken out by the System Integrator and when used in the context of any act or event, it shall mean the aggregate of the maximum sums insured and payable in relation to such act or event;
Material Breach	means a breach by either Party (Client or System Integrator) of any of its obligations under this Agreement which has or is likely to have an Adverse Effect on the Project which such Party shall have failed to cure;
Minimum Required Deliverables	shall have the same meaning ascribed to it in Annexure C of this Agreement;
Parties	means Client and System Integrator for the purposes of this Agreement and "***Party***" shall be interpreted accordingly;
Performance Guarantee	Means the guarantee of 10% of value of the contract in the form of a Bank Guarantee as per the format provided in this RFP from Indian Public Sector Banks or Private Sector Banks authorized by the Government to conduct Government transaction. At present HDFC Bank, ICICI Bank and AXIS Bank are the only three private sector banks authorized by the Government. Details of the bank are to be furnished in the commercial offer.
Planned Application Downtime	means the unavailability of the application services due to maintenance activities such as configuration changes, upgradation or changes to any supporting infrastructure wherein prior intimation (at least two working days in advance) of such planned outage shall be given and approval sought from the Client as applicable;
Planned network outage	means the unavailability of the network services due to infrastructure maintenance activities such as configuration changes, upgradation or changes to any supporting infrastructure. Prior intimation of such planned outage shall be given and approval sought from the Client as applicable

	and shall be notified at least two working days;
Project	means Pilot, Project Implementation (roll out) and Maintenance in terms of the Agreement;
Project Implementation	means Project Implementation as per the testing standards and acceptance criteria prescribed by Client or its nominated agencies;
Project Implementation Phase	shall be from the Effective Date of the Agreement to the date of final acceptance testing & certification as set out in Clause 2.7.4 of this Agreement;
State Project Monitoring Unit (SPMU)	shall be constituted by each state to monitor the activities, deliverables and progress of the Project. SPMU may comprise of the staff members of the Client or may be a team of external experts (as defined in the RFP Volume 1);
Project Timelines	shall have the same meaning ascribed to in Annexure C;
Providing Party	shall have the same meaning ascribed to it in Clause 2.14.5
Receiving Party	shall have the same meaning ascribed to it in Clause 2.14.5
Replacement System Integrator	means any third party that Client or its nominated agencies appoint to replace System Integrator upon expiry of the Term or termination of this Agreement to undertake the Services or part thereof;
Required Consents	means the consents, waivers, clearances and licenses to use Client's Intellectual Property Rights, rights and other authorizations as may be required to be obtained for the software and other items that Client or their nominated agencies are required to make available to System Integrator pursuant to this Agreement;
Services	means the services delivered to the Stakeholders of Client or its nominated agencies, employees of Client or its nominated agencies, and to professionals, using the tangible and intangible assets created, procured, installed, managed and operated by the System Integrator including the tools of information and communications technology and includes but is not limited to the list of services specified in Annexure B;
Service Level	means the level of service and other performance criteria which will apply to the Services delivered by the System Integrator
SLA	means the Performance and Maintenance SLA executed as part of this Master Service Agreement;
Stakeholders	Term stakeholders shall cover Citizens/ Citizens groups, MHA/NCRB/Others, State Police department, CID, CBI, External Departments of the State such as Jails, Courts, Passport Office, Transport

	Department and Hospitals etc., Non-Government/Private sector organizations
Term	shall have the same meaning ascribed to it in Clause 2.5.1
Third Party Systems	means systems (or any part thereof) in which the Intellectual Property Rights are not owned by the Client or System Integrator and to which System Integrator has been granted a license to use and which are used in the provision of Services;
Unplanned Application Downtime	means the total time for all the instances where services in the software requirement specification document prepared by the System Integrator are not available for more than 5 consecutive minutes;
Network	in Client users refers to all the IT assets installed or maintained by the System Integrator as part of the Project for networking;
Unplanned network outage	means the total time for all the instances where services in the software requirement specification document prepared by the System Integrator are not available for more than 5 consecutive minutes;
Application	means the software application developed as a part of scope of work set out in Clause 2.5
Application Downtime	means the time for which user/s is not able to access the application. However, in calculating downtime, scheduled downtime (for example, backup time, batch processing time, routine maintenance time) would not be considered;
Network Uptime	Shall mean as defined in Service Level Agreement
Warranty / AMC Period	shall be counted five years from the date of successful completion of Successful implementation / Go-Live

3.2 Schedule – II: Change Control Schedule

This Schedule describes the procedure to be followed in the event of any proposed change to the Master Service Agreement ("**MSA**"), Project Implementation Phase, SLA and Scope of Work and Functional Requirement Specifications. Such change shall include, but shall not be limited to, changes in the scope of services provided by the System Integrator and changes to the terms of payment as stated in the Terms of Payment Schedule. Changes proposed for amendments/ modifications in the CCTNS application shall be eligible under this schedule only after completion of one year handholding support post Go-Live of the complete CCTNS solution in the State.

The CLIENT and SI 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 SI will endeavour, wherever reasonably practicable, to effect change without an increase in the terms of payment as stated

in the Terms of Payment Schedule and CLIENT or its nominated agencies 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 to all the changes to this agreement and other documents except for the changes in SLAs for which a separate process has been laid out.

This Change Control Schedule sets out the provisions which will apply to changes to the MSA.

3.2.1 Change Management Process

(a) Change Control Note ("CCN")

i. Change requests in respect of the MSA, the Project Implementation, the operation, the SLA or Scope of work and Functional Requirement specifications will emanate from the Parties' respective Project Manager who will be responsible for obtaining approval for the change and who will act as its sponsor throughout the Change Control Process and will complete Part A of the CCN attached as Annexure A hereto. CCNs will be presented to the other Party's Project Manager who will acknowledge receipt by signature of the CCN.

ii. The SI and the CLIENT or its nominated agencies, during the Project Implementation Phase and the CLIENT or its nominated agencies during the Operations and Management Phase and while preparing the CCN, shall consider the change in the context of the following parameter, namely whether the change is beyond the scope of Services including ancillary and concomitant services required and as detailed in Volume I of the RFP and is suggested and applicable only after the testing, commissioning and certification of the Pilot Phase and the Project Implementation Phase as set out in this Agreement.

iii. It is hereby also clarified here that any change of control suggested beyond 15 % of the value of this Project will be beyond the scope of the change control process and will be considered as the subject matter for a separate bid process and a separate contract. It is hereby clarified that the 15% of the value of the Project as stated in herein above is calculated on the basis of bid value submitted by the System Integrator and accepted by the CLIENT or its nominated agencies or as decided and approved by CLIENT or it Nominated Agencies. For arriving at the cost / rate for change upto 15% of the project value, the payment terms and relevant rates as specified in Annexure D shall apply.

(b) Quotation

The SI shall assess the CCN and complete Part B of the CCN, in completing the Part B of the CCN the SI shall provide as a minimum:

1. a description of the change
2. a list of deliverables required for implementing the change;
3. a time table for implementation;
4. an estimate of any proposed change

5. any relevant acceptance criteria

6. an assessment of the value of the proposed change;

7. Material evidence to prove that the proposed change is not already covered within the Agreement and the scope of work.

i. Prior to submission of the completed CCN to the CLIENT, or its nominated agencies, the Service Provider will undertake its own internal review of the proposal and obtain all necessary internal approvals. As a part of this internal review process, the SI shall consider the materiality of the proposed change in the context of the MSA and the Project Implementation affected by the change and the total effect that may arise from implementation of the change.

(c) 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 provided the SI meets the obligations as set in the CCN. In the event the SI is unable to meet the obligations as defined in the CCN then the cost of getting it done by third party will be borne by the SI.

(d) Obligations

The SI shall be obliged to implement any proposed changes once approval in accordance with above provisions has been given, with effect from the date agreed for implementation and within an agreed timeframe.

3.3 Schedule – III: Exit Management Schedule

3.3.1 Purpose

(a) This Schedule sets out the provisions, which will apply on expiry or termination of the MSA, the Project Implementation, Operation and Management SLA.

(b) In the case of termination of the Project Implementation and/or Operation and Management, the Parties shall agree at that time whether, and if so during what period, the provisions of this Schedule shall apply.

(c) The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Schedule.

3.3.2 Transfer of Assets

(a) CLIENT shall be entitled to serve notice in writing on the SI at any time during the exit management period as detailed hereinabove requiring the SI and/or its sub contractors to provide the CLIENT with a complete and up to date list of the Assets within 30 days of such notice. CLIENT shall then be entitled to serve notice in writing on the SI at any time prior to the date that is 30 days prior to the end of the exit management period requiring the SI to sell the Assets, if any, to be transferred to CLIENT or its nominated agencies at book value as determined as of the date of such notice in accordance with the provisions of relevant laws.

(b) In case of contract being terminated by CLIENT, CLIENT reserves the right to ask SI to continue running the project operations for a period of 6 months after termination orders are issued.

(c) Upon service of a notice under this Article the following provisions shall apply:

i. in the event, if the Assets to be transferred are mortgaged to any financial institutions by the SI, the SI shall ensure that all such liens and liabilities have been cleared beyond doubt, prior to such transfer. All documents regarding the discharge of such lien and liabilities shall be furnished to the CLIENT.

ii. All risk in and title to the Assets to be transferred / to be purchased by the CLIENT pursuant to this Article shall be transferred to CLIENT, on the last day of the exit management period.

iii. CLIENT shall pay to the SI on the last day of the exit management period such sum representing the Net Block (procurement price less depreciation as per provisions of Companies Act) of the Assets to be transferred as stated in the Terms of Payment Schedule.

iv. Payment to the outgoing SI shall be made to the tune of last set of completed services / deliverables, subject to SLA requirements.

v. The outgoing SI will pass on to CLIENT and/or to the Replacement SI, the subsisting rights in any leased properties/ licensed products on terms not less favorable to CLIENT/ Replacement SI, than that enjoyed by the outgoing SI.

3.3.3 Cooperation and Provision of Information

During the exit management period:

(a) The System Integrator will allow the CLIENT or its nominated agency access to information reasonably required to define the then current mode of operation associated with the provision of the services to enable the CLIENT to assess the existing services being delivered;

(b) promptly on reasonable request by the CLIENT, the SI shall provide access to and copies of all information held or controlled by them which they have prepared or maintained in accordance with this agreement relating to any material aspect of the services (whether provided by the System Integrator or sub contractors appointed by the System Integrator). The CLIENT shall be entitled to copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. The System Integrator shall permit the CLIENT or its nominated agencies to have reasonable access to its employees and facilities as reasonably required to understand the methods of delivery of the services employed by the System Integrator and to assist appropriate knowledge transfer.

3.3.4 Confidential Information, Security and Data

(a) The System Integrator will promptly on the commencement of the exit management period supply to the CLIENT or its nominated agency the following:

i. information relating to the current services rendered and customer and performance data relating to the performance of sub contractors in relation to the services;

ii. documentation relating to Project's Intellectual Property Rights;

iii. documentation relating to sub-contractors;

iv. all current and updated data as is reasonably required for purposes of CLIENT or its nominated agencies transitioning the services to its Replacement System Integrator in a readily available format nominated by the CLIENT, or its nominated agency;

v. all other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable CLIENT or its nominated agencies, or its Replacement System Integrator to carry out due diligence in order to transition the provision of the Services to CLIENT or its nominated agencies, or its Replacement System Integrator (as the case may be).

(b) Before the expiry of the exit management period, the System Integrator shall deliver to the CLIENT or its nominated agency all new or up-dated materials from the categories set out in Schedule above and shall not retain any copies thereof, except that the System Integrator shall be permitted to retain one copy of such materials for archival purposes only.

(c) Before the expiry of the exit management period, unless otherwise provided under the MSA, the CLIENT or its nominated agency shall deliver to the System Integrator all forms of System Integrator confidential information, which is in the possession or control of Client or its nominated agency.

3.3.5 Employees

(a) 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 the CLIENT or its nominated agency 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.

(b) Where any national, regional law or regulation relating to the mandatory or automatic transfer of the contracts of employment from the System Integrator to the CLIENT or its nominated agency, 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.

(c) To the extent that any Transfer Regulation does not apply to any employee of the System Integrator, department, 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 the SPMU or any Replacement System Integrator.

3.3.6 Transfer of Certain Agreements

On request by the CLIENT or its nominated agency the System Integrator shall effect such assignments, transfers, licenses and sub-licenses as the Director General of Police may require the same in the name of Director General of Police, Haryana or its Replacement System Integrator in relation to any equipment lease, maintenance or service provision agreement between System Integrator and third party licensor, vendors, and which are related to the services and reasonably necessary for the carrying out of replacement services by the CLIENT or its nominated agency or its Replacement System Integrator.

3.3.7 Rights of Access to Premises

(a) 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) the CLIENT or its nominated agency and/or any Replacement System Integrator in order to make an inventory of the Assets.

(b) The System Integrator shall also give the CLIENT or its nominated agency or its nominated agencies, or any Replacement System Integrator right of reasonable

access to the System Integrator's premises and shall procure the CLIENT or its nominated agency 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 MSA as is reasonably necessary to migrate the services to the CLIENT or its nominated agency, or a Replacement System Integrator.

3.3.8 General Obligations of the System Integrator

(a) The System Integrator shall provide all such information as may reasonably be necessary to effect as seamless a handover as practicable in the circumstances to the CLIENT or its nominated agency or its Replacement System Integrator and which the System Integrator has in its possession or control at any time during the exit management period.

(b) For the purposes of this Schedule, anything in the possession or control of any System Integrator, associated entity, or sub contractor is deemed to be in the possession or control of the System Integrator.

(c) The System Integrator shall commit adequate resources to comply with its obligations under this Exit Management Schedule.

3.3.9 Exit Management Plan

(a) The System Integrator shall provide the CLIENT or its nominated agency 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 MSA as a whole and in relation to the Project Implementation, and the Operation and Management SLA.

i. 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 continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;

ii. plans for the communication with such of the System Integrator's sub contractors, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on the CLIENT's operations as a result of undertaking the transfer;

iii. (if applicable) proposed arrangements for the segregation of the System Integrator's networks from the networks employed by CLIENT and identification of specific security tasks necessary at termination;

iv. Plans for provision of contingent support to CLIENT, and Replacement System Integrator for a reasonable period after transfer.

(b) The System Integrator shall re-draft the Exit Management Plan annually thereafter to ensure that it is kept relevant and up to date.

(c) Each Exit Management Plan shall be presented by the System Integrator to and

approved by the CLIENT or its nominated agencies.

(d) The terms of payment as stated in the Terms of Payment Schedule includes the costs of the System Integrator complying with its obligations under this Schedule.

(e) In the event of termination or expiry of MSA, and Project Implementation, each Party shall comply with the Exit Management Plan.

(f) During the exit management period, the System Integrator shall use its best efforts to deliver the services.

(g) Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.

(h) This Exit Management plan shall be furnished in writing to the CLIENT or its nominated agencies within 90 days from the Effective Date of this Agreement.

3.4 Schedule – IV: Audit, Access And Reporting

3.4.1 Purpose

This Schedule details the audit, access and reporting rights and obligations of the CLIENT or its nominated agency and the System Integrator.

3.4.2 Audit Notice and Timing

(a) As soon as reasonably practicable after the Effective Date, the Parties shall use their best endeavours to agree to a timetable for routine audits during the Project Implementation Phase and the Operation and Management Phase. Such timetable during the Implementation Phase, the CLIENT or its nominated agency and thereafter during the operation Phase, the CLIENT or its nominated agency shall conduct routine 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.

(b) The CLIENT or its nominated agency may conduct non-timetabled audits at his/ her own discretion if they 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 period time 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. If the System Integrator considers that the non-timetabled audit was not appropriate, the matter shall be referred to the escalation procedure as set out in the Governance Schedule.

(c) The frequency of audits shall be half yearly, provided always that the CLIENT or its nominated agency shall endeavour to conduct such audits with the lowest levels of inconvenience and disturbance practicable being caused to the System Integrator.

3.4.3 Access

The System Integrator shall provide to the CLIENT or its nominated agency reasonable access to employees, subcontractors, suppliers, agents and third party facilities as detailed in Volume I & II 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. The SPMU/ Client or its nominated agency 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.

3.4.4 Audit Rights

(a) The CLIENT or its nominated agency shall have the right to audit and inspect suppliers, agents and third party facilities (as detailed in Volume I of the RFP), data centres, 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:

i. The security, integrity and availability of all data processed, held or conveyed by the Partner on behalf of CLIENT and documentation related thereto;

ii. That the actual level of performance of the services is the same as specified in the SLA;

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 SLA.

v. Security audit and implementation audit of the system shall be done once each year, the cost of which shall be borne by the System Integrator.

vi. 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 MSA.

3.4.5 Audit Rights of Sub-Contractors, Suppliers And Agents

(a) The System Integrator shall use reasonable endeavours to achieve the same audit and access provisions as defined in this Schedule with sub-contractors, suppliers and agents who supply labour, services, equipment or materials in respect of the services. The System Integrator shall inform the CLIENT or its nominated agency prior to concluding any sub-contract or supply agreement of any failure to achieve the same rights of audit or access.

(b) REPORTING: The System Integrator will provide quarterly reports to the Client or its nominated agency regarding any specific aspects of the Project and in context of the audit and access information as required by the CLIENT or its nominated agency.

3.4.6 Action and Review

(a) Any change or amendment to the systems and procedures of the System Integrator, or sub-contractors, where applicable arising from the audit report shall be agreed within thirty (30) calendar days from the submission of the said report.

(b) Any discrepancies identified by any audit pursuant to this Schedule shall be immediately notified to the CLIENT or its nominated agency and the System Integrator's Project Manager in consultation with Client, shall determine what action should be taken in respect of such discrepancies in accordance with the terms of the MSA.

3.4.7 Terms of Payment

The System Integrator shall bear all the cost of any audits and inspections. The terms of payment are inclusive of any costs of the System Integrator and the sub-contractor, for all reasonable

assistance and information provided under the MSA, the Project Implementation, Operation and Management SLA by the System Integrator pursuant to this Schedule.

3.4.8 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 MSA.

3.5 Schedule – V: Governance Schedule

3.5.1 Purpose

The purpose of this Schedule is to:

(i) establish and maintain the formal and informal processes for managing the relationship between the CLIENT and the System Integrator (including the outputs from other Schedules to this Agreement;

(ii) define the principles that both Parties wish to follow to ensure the delivery of the Services;

(iii) ensure the continued alignment of the interests of the Parties;

(iv) ensure that the relationship is maintained at the correct level within each Party;

(v) create the flexibility to revise and maintain the relationship and this Agreement during the Term;

(vi) set out the procedure for escalating disagreements; and

(vii) enable contract administration and performance management.

3.5.2 Governance Structure

(a) Project Managers: The relationship under this Agreement will be managed by the Project Managers appointed by each Party, who will provide the interface between the executive management of the respective Parties.

(b) Project Implementation Unit (PIU): In addition the Governance Structure defined in the RFP Volume I, Within 7 days following the Effective Date, CLIENT or its nominated agencies and the System Integrator shall form a joint Project Implementation Unit comprising of members from each party, and each party shall appoint a Project Manager. In the event that either Party wishes to substitute its Project Manager it will do so in manner in which the original appointment is made and notify the other Party of such substitution as soon as reasonably practicable but at the latest within 7 days of the substitution.

(c) The Project Managers shall have responsibility for maintaining the interface and communication between the Parties.

(d) The PIU will meet formally on a fortnightly / monthly / quarterly, as required, basis

at a time and location to be agreed between them. These meetings will cover, as a minimum, the following agenda items: (i) consideration of Quarterly Performance Reports; (ii) consideration of matters arising out of the Change Control Schedule; (iii) issues escalated in accordance with the escalation procedure as set out in the Governance Schedule; (iv) matters to be brought before the PIU in accordance with the MSA and the Schedules; (v) any matter brought before the PIU by the System Integrator under this Article; and (vi) any other issue which either Party wishes to add to the agenda.

(e) In the event that there is any material factor which affects the delivery of the Services or the terms of payment as stated in the Terms of Payment Schedule, the Parties agree to discuss in the PIU any appropriate amendment to the Agreement or any Service Level Agreements or Statement of Works including any variation to the terms of payment as stated in the Terms of Payment Schedule. Any variation so agreed shall be implemented through the change control procedure as set out in the Change Control Schedule.

3.5.3 Governance Procedures

(a) The System Integrator shall document the agreed structures in a procedures manual.

(b) The agenda for each meeting of the PIU shall be set to reflect the discussion items referred to above and extraordinary items may be added either with the agreement of the Parties or at the request of either Party. Copies of the agenda for meetings of the PIU, along with relevant pre-reading material, shall be distributed at least one week in advance of the relevant meeting.

(c) All meetings and proceedings will be documented such documents to be distributed to the Parties and copies shall be kept as a record. All actions, responsibilities and accountabilities arising out of any meeting shall be tracked and managed.

(d) The Parties shall ensure as far as reasonably practicable that the PIU shall resolve the issues and resolve the objectives placed before them and that members representing that Party are empowered to make relevant decisions or have easy access to empowered individuals for decisions to be made to achieve this.

(e) In order formally to submit a Disputed Matter to the aforesaid for a, one Party ("Claimant") shall give a written notice ("Dispute Notice") to the other Party. The Dispute Notice shall be accompanied by (a) a statement by the Claimant describing the Disputed Matter in reasonable detail and (b) documentation, if any, supporting the Claimant's position on the Disputed Matter.

(f) The other Party ("Respondent") shall have the right to respond to the Dispute Notice within 7 days after receipt of the Dispute Notice. In the event that the parties are unable to resolve the Disputed Matter within a further period of 7 days, it shall refer the Disputed Matter to next level of the dispute resolution for action as per the process mentioned in article 9.1

(g) All negotiations, statements and / or documentation pursuant to these Articles

shall be without prejudice and confidential (unless mutually agreed otherwise).

(h) If the Disputed Matter is having a material effect on the operation of the Services (or any of them or part of them) the Parties will use all their respective reasonable endeavours to reduce the elapsed time in reaching a resolution of the Disputed Matter.

3.5.4 The payment under the various cost heads is given as under:

(a) For the payment purposes the pro rata reduction has been done on the cost items and sub items. The financial implications for both the states have been mentioned separately. Breakup of the overall project cost for all the phases of the project have been given in the Schedule below.

3.6 Schedule – VI: Payment Schedule

The payment schedule and milestones are divided into two phases:

A) Implementation Phase

B) Operations and Maintenance Phase

S. No.	Payment Milestones for the Implementation phase	% Payment
A. Implementation Phase		**35%**
1.	M1: Advance against submission of Bank Guarantee	5%
2.	M2: Pre – Go Live Readiness[1] of the Pilot Districts	5%
3.	M3: Go-Live[2] of the Pilot Districts	5%
4.	M4: Pre – Go Live Readiness[1] for Phase II	5%
5.	M6: Successful integration with external agencies with successful transfer of the data for three months in succession	5%
6.	M5: Go-Live[2] of the Phase II	10%
B. Operations and Maintenance Phase[3]		**65%**
7.	Ten half-yearly installments over Five years from the "Go-Live" date, each installment being a maximum of 6.5% of total contract value depending upon the quarterly performance level assessed on the basis of SLAs defined in this RFP	65%

Note: All payments to the System Integrator shall be made upon submission of invoices along with relevant sign-offs from Haryana Police.

1. Pre – Go Live Readiness of Districts under Phase requires Completion and Acceptance of the following activities in at least 85% of the Police Stations / Higher Offices in each of the Districts targeted under the Phase

- SRS, design documents, test cases and test plan
- Data Migration / Digitization
- Capacity Building Program covering the targeted personnel
- Change Management Initiatives covering the targeted personnel
- Site Preparation
- Delivery and Commissioning of Client Side Infrastructure
- Networking

2. Go-Live in the Phase requires Completion and Acceptance of the following activities all 100% of the Police Stations / Higher Offices in each of the Districts targeted under the Phase

- SRS, design documents, test cases and test plan
- Data Migration / Digitization
- Capacity Building Program covering the targeted personnel
- Change Management Initiatives covering the targeted personnel
- Site Preparation
- Delivery and Commissioning of Client Side Infrastructure
- Networking
- Commission of the Configured, Customized, and Extended CAS (State)
- The PS / HO have completely migrated to the new application and the police station and the higher offices' personnel are successfully conducting the intended functions through the application
- User Acceptance Testing
- Successful operations of system as desired by the Haryana Police

Please note:

- The above payments are subject to meeting of SLA's failing which the appropriate deductions as mentioned in the SLA section of Vol. 1 of this RFP
- All the hardware proposed under this project should be along with an AMC for 5 years post Successful Go-Live of the project
- The successful bidder will also be responsible to maintain the AMC for the existing hardware that bidder will use during the implementation of this project.
- The payment against the hardware will be made on the basis of the actual quantity of the items procured. CLIENT will have the right for reduction / addition in the quantity proposed. Any payments will be done on the basis of the unit rates quoted by the bidder in the Commercial bid.
- The cost for the manpower will also be done on the actual basis i.e. category of the manpower deployed and the period of deployment.

- For the payment purposes, price reduction shall be applied on pro rata basis on all head, sub heads and items of the commercial bid.
- Any fluctuation in prices due to inflation, tax regulations, will be borne by the bidder and not be passed on to CLIENT
- Whenever the penalty is levied on System Integrator for failing to meet the required SLA, the half year installment shall be paid and the penalty (if any) will be adjusted in the subsequent half yearly installment (s)
- Any delay on account of CLIENT officials (and not attributable to the SI) shall not be taken into account while computing adherence to service levels for the SI. While CLIENT will ensure that any Sign off / Comments are provided within a period of 15 working days from the submission of deliverables by the SI.
- Any monetary figure in decimal shall be rounded off to the nearest INR

4 SERVICE LEVEL AGREEMENT

1. This document describes the service levels to be established for the Services offered by the SI to the Haryana Police. The SI shall monitor and maintain the stated service levels to provide quality service to the Haryana Police.

2. Definitions.

(a) **"Scheduled Maintenance Time"** shall mean the time that the System is not in service due to a scheduled activity as defined in this SLA. The scheduled maintenance time would not be during 16X6 timeframe. Further, scheduled maintenance time is planned downtime with the prior permission of the Haryana Police.

(b) **"Scheduled operation time"** means the scheduled operating hours of the System for the month. All scheduled maintenance time on the system would be deducted from the total operation time for the month to give the scheduled operation time. The total operation time for the systems and applications within the Primary DC, DRC and critical client site infrastructure will be 24X7X365. The total operation time for the client site systems shall be 18 hours.

(c) **"System or Application downtime"** means accumulated time during which the System is totally inoperable within the Scheduled Operation Time but outside the scheduled maintenance time and measured from the time the Haryana Police and/or its employees log a call with the SI team of the failure or the failure is known to the SI from the availability measurement tools to the time when the System is returned to proper operation.

(d) **"Availability"** means the time for which the services and facilities are available for conducting operations on the Haryana Police system including application and associated infrastructure. Availability is defined as:

{(Scheduled Operation Time – System Downtime) / (Scheduled Operation Time)} * 100%

(e) **"Helpdesk Support"** shall mean the 16x6 basis support centre which shall handle Fault reporting, Trouble Ticketing and related enquiries during this contract.

(f) "**Incident**" refers to any event / abnormalities in the functioning of the Data Centre Equipment / Services that may lead to disruption in normal operations of the Data Centre, System or Application services.

(g) **" Error"** in data digitization or data migration exercise, refers to the mistakes made intentional/ unintentional by SI which may or may not change the actual meaning of the subject.

3. Interpretations.

(a) The business hours are 8:30AM to 4:30PM on all working days (Mon-Sat) excluding Public Holidays or any other Holidays observed by the Haryana Police. The SI however recognizes the fact that the Haryana Police offices will require to work beyond the business hours on need basis.

(b) "Non-Business Hours" shall mean hours excluding "Business Hours".

(c) 18X7 shall mean hours between 06:00AM -12.00 midnight on all days of the week.

(d) If the operations at Primary DC are not switched to DRC within the stipulated timeframe (Recovery Time Objective), it will be added to the system downtime.

(e) The availability for a cluster will be the average of availability computed across all the servers in a cluster, rather than on individual servers. However, non compliance with performance parameters for infrastructure and system / service degradation will be considered for downtime calculation.

(f) The SLA parameters shall be monitored on a monthly basis as per the individual SLA parameter requirements. However, if the performance of the system/services is degraded significantly at any given point in time during the contract and if the immediate measures are not implemented and issues are not rectified to the complete satisfaction of the Haryana Police or an agency designated by them, then the Haryana Police will have the right to take appropriate disciplinary actions including termination of the contract.

(g) A Service Level violation will occur if the SI fails to meet Minimum Service Levels, as measured on a half yearly basis, for a particular Service Level. Overall Availability and Performance Measurements will be on a monthly basis for the purpose of Service Level reporting. An "Availability and Performance Report" will be provided by the SI on monthly basis in the Haryana Police suggested format and a review shall be conducted based on this report. A monthly Availability and Performance Report shall be provided to the Haryana Police at the end of every month containing the summary of all incidents reported and associated SI performance measurement for that period. The monthly Availability and Performance Report will be deemed to be accepted by the Haryana Police upon review and signoff by both SI and the Haryana Police. Where required, some of the Service Levels will be assessed through audits or reports e.g. utilization reports, measurements reports, etc., as appropriate to be provided by the SI on a monthly basis, in the formats as required by

the Haryana Police The tools to perform the audit will need to be provided by the SI. Audits will normally be done on regular basis or as required by the Haryana Police and will be performed by the Haryana Police or the Haryana Police appointed third party agencies.

(h) EMS system as specified in this RFP shall play a critical role in monitoring the SLA compliance and hence will have to be customized accordingly. The 3rd party testing and audit of the system shall put sufficient emphasis on ensuring the capability of EMS system to capture SLA compliance correctly and as specified in this RFP. The selected System Integrator (SI) must deploy EMS tool and develop additional scripts (if required) for capturing the required data for SLA report generation in automated way. This tool should generate the SLA Monitoring report in the end of every month which is to be shared with the Haryana Police on a monthly basis. The tool should also be capable of generating SLA reports for a half-year. the Haryana Police will audit the tool and the scripts on a regular basis. SPMC shall assess the EMS requirements and include the same in the RFP.

(j) The Post Implementation SLAs will prevail from the start of the Operations and Maintenance Phase. However, SLAs will be subject to being redefined, to the extent necessitated by field experience at the police stations / higher offices and the developments of technology practices globally. The SLAs may be reviewed on an annual/bi-annual basis as the Haryana Police decides after taking the advice of the SI and other agencies. All the changes would be made by the Haryana Police in consultation with the SI.

(k) The SI is expected to provide the following service levels. In case these service levels cannot be achieved at service levels defined in the tables below, it shall result in a breach of contract and invoke the penalty clause. Payments to the SI are linked to the compliance with the SLA metrics laid down in the tables below. The penalties will be computed and calculated as per the computation explained in this Annexure. During the contract period, it is envisaged that there could be changes to the SLA, in terms of addition, alteration or deletion of certain parameters, based on mutual consent of both the parties i.e. the Haryana Police and SI.

(l) Following tables outlines the key service level requirements for the system, which needs be ensured by the SI during the operations and maintenance period. These requirements shall be strictly imposed and either the Haryana Police or a third party audit/certification agency shall be deployed for certifying the performance of the SI against the target performance metrics as outlined in the tables below.

Implementation Phase SLAs

1. <u>Capacity Building</u>

Service Level Description	Measurement
Capacity Building	All the trainees within each of the training program should pass the training exam with more than 80% or more marks conducted after their training Severity of Violation: High This service level will be monitored and measured on a per District basis through online examination of each trainee and their result If the training quality in the program falls below the minimum service level, it will be treated as one (1) violation. The total number of violations for the payment period will be the cumulative number of violations across all the programs across all Districts in the payment period.

2. Data Migration / Digitization

Service Level Description	Measurement
Data Migration/ Digitization	Errors having "High" impact would amount from mistakes in section of offence/ FIR details/ Name of accused or complainant/ particulars of accused such as address, contact details, Ids (DL No., passport No. etc.). High impacting errors shall have direct implications to penalties. Errors having "Low" impact would amount from other mistakes. 3 or less low impacting errors per case file will not be subjected for penalties, however mistakes would be corrected by SI at the time of such incident is reported. Severity of Violation: High This service level will be measured on a monthly basis for each Police Station / Higher Office.

Service Level Description	**Measurement**
	If the data migration / digitization service level in a police station / higher office falls below the minimum service level, it will be treated as one (1) violation. The total number of violations for the payment period will be the cumulative number of violations across all the police stations / higher offices in the payment period.

Delivery Related Service Level Agreement (SLA) Criteria								
Explanation: The deduction mentioned in this table shall be made from the next due payment to the vendor for services provided on Statewide basis.								
S. No.	**Service Metrics Parameters**	**Baseline**	**Lower Performance**		**Violation of Service level agreement**		**Basis of Measurement**	**Remarks**
		Metric	**Metric**	**Deduction**	**Metric**	**Deduction**		
1	Delivery of the reports/ deliverables due for this section	As per the dates as mentioned in the contract	One week after the due date	Rs. 10,000	>1 week after the due date	Rs. 20,000 for every week of delay	Dates for delivery of reports as mentioned in the contract	
2	Development, deployment and testing of CAS (State) application	5.0 months from date of signing of contract	5-7 months	100,000 Rupees	More than 7 months	Rs. 1,00,000 per month of delay	Months taken after beginning of the assignment to develop and test the application at the Data center by the Operator, not including the software audit by TPA	The centralized application should be tested for desired functionalities, security, and completeness as well as compliance with SLA, within the period

Delivery Related Service Level Agreement (SLA) Criteria								
Explanation: The deduction mentioned in this table shall be made from the next due payment to the vendor for services provided on Statewide basis.								
S. No.	**Service Metrics Parameters**	**Baseline**	**Lower Performance**		**Violation of Service level agreement**		**Basis of Measurement**	**Remarks**
		Metric	**Metric**	**Deduction**	**Metric**	**Deduction**		
	Supply, installation and Commissioning of hardware at offices	3 months	3-4 months	For non-compliance at each point of deployment: Rs. 30,000	> 4 months	For non-compliance at each point of deployment: Rs. 45,000	Months after taking over of the office site for project	The deduction shall be made per site basis, where criterion is not satisfied
	Supply, installation and Commissioning of the Data Center Equipment	6 months from the date of signing of contract	6-7 months	Rs. 100,000	More than 7 months	Rs. 100,000 for every month of delay	Months taken after beginning of the assignment	Haryana Police may conduct independent audit to verify that the data center is as per the specifications.
	Capacity building	All the trainees should pass the online training	Less than 80% and more than 60% marks	Rs. 1500 / trainee/ training program	Less than 60% marks	Rs. 3000 per trainee/ training program	Results from Online examination test post training course	The feedback of the attendees must be taken after every training session/

Delivery Related Service Level Agreement (SLA) Criteria								
Explanation: The deduction mentioned in this table shall be made from the next due payment to the vendor for services provided on Statewide basis.								
S. No.	**Service Metrics Parameters**	**Baseline**	**Lower Performance**		**Violation of Service level agreement**		**Basis of Measurement**	**Remarks**
		Metric	**Metric**	**Deduction**	**Metric**	**Deduction**		
		exam with more than 80% marks						program and this feedback should be leveraged for improving the capacity building program
	Data Digitization	Zero tolerance for High Impacting errors and less than 3 low impacting errors per case file	No high impacting error and 1-2 low impacting errors	Rs. 50 / error	1 or more high impacting error (s) or less than 3 low impacting errors or more than 3 low impacting	Rs. 100 / error and entire case to be re-done	Error per case file during verification	Error rate is measured by percentage of the records with corrections marked by designated officials

Delivery Related Service Level Agreement (SLA) Criteria								
Explanation: The deduction mentioned in this table shall be made from the next due payment to the vendor for services provided on Statewide basis.								
S. No.	**Service Metrics Parameters**	**Baseline**	**Lower Performance**		**Violation of Service level agreement**		**Basis of Measurement**	**Remarks**
		Metric	**Metric**	**Deduction**	**Metric**	**Deduction**		
					errors			
	Maintenance phase	All the issues reported regarding hardware, software etc. should be resolved within 24 hours (within 1 working day)	Resolution of issues within 2 working days of reporting	Rs. 500	Resolution of the issue after 2 working days	Rs. 1000 for every day delay over and above beyond	Time and date of reporting of the issue	
	The above list of Service levels is indicative. The Haryana Police should add more service levels / modify the above service levels as per their requirements							

3. Violations and Associated Penalties

(a) 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.

(b) **Penalty Calculations.** The framework for Penalties, as a result of not meeting the Service Level Targets are as follows:

(i) 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.

(ii) The number of violations in the reporting period for each level of severity will be totaled and used for the calculation of Penalties.

(iii) Penalties applicable for each of the high severity violations are 0.1% of respective payment-period payment to the SI.

(iv) Penalties applicable for each of the medium severity violations are 0.05% of respective payment-period payment to the SI.

Post Implementation Phase SLAs

1. Primary DC/DRC Site Infrastructure Systems and Application Availability and Performance

(a) **Production CAS Systems**. The failure or disruption has a direct impact on the Haryana Police's ability to service its police stations / higher offices, ability to perform critical back-office functions or a direct impact on the organization. This includes but not limited to:-

(i) Storage and related switches at Primary DC and DRC.

(ii) Web, Application, Database, and Backup Servers at Primary DC and DRC.

(iii) Primary DC to DRC connectivity.

(iv) Primary DC and DRC network infrastructure.

(v) Primary DC and DRC security infrastructure.

(b) **Non-CAS Systems in Production and Non Production Systems (Development, QA, and Training)**. The failure or disruption has no direct impact on the Haryana Police's ability to serve its police stations / higher offices, or perform critical back-office functions.

(i) Production Non CAS Servers.

(ii) Test, QA and Training Servers.

(iii) Helpdesk infrastructure & applications.

(iv) EMS Infrastructure.

(c) **CAS Solution Components**. The failure or disruption has a direct impact on the Haryana Police's ability to service its police stations / higher offices, ability to perform critical back-office functions or a direct impact on the organization.

(d) **Non ERP Solution Components**. The failure or disruption has no direct impact on the Haryana Police's ability to serve its police stations / higher offices, or perform critical back-office functions.

(e) These service levels will be monitored on a monthly basis.

(f) The below tables gives details on the Service Levels the SI should maintain.

Service Level Description	Measurement

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td>Infrastructure Availability</td><td>Availability of production CAS systems shall be at least 99%

Severity of Violation: High

<table><tr><td>Availability over the six-month period</td><td>Violations for calculation of penalty</td></tr><tr><td>< 99% & >= 98.5%</td><td>1</td></tr><tr><td>< 98.5% & >= 98%</td><td>2</td></tr><tr><td>< 98%</td><td>3</td></tr></table>
In addition to the above, if the service level in any month in the six-month period falls below 98%, one (1) additional violation will be added for each % drop for each such month to the overall violations for this service level.</td></tr>
<tr><td>Infrastructure Availability</td><td>Availability of non-CAS systems in production and non-production systems shall be at least 97%.

Severity of Violation: Medium

<table><tr><td>Availability over the six-month period</td><td>Violations for calculation of penalty</td></tr><tr><td>< 97% & >= 96.5%</td><td>1</td></tr><tr><td>< 96.5% & >= 96%</td><td>2</td></tr><tr><td>< 96%</td><td>3</td></tr></table>
In addition to the above, if the service level in any month in the six-month period falls below 96%, one (1) additional violation will be added for each % drop for each such month to the overall violations for this service level.</td></tr>
<tr><td>Infrastructure Availability</td><td>RTO shall be less than or equal to six (6) hours.

Severity of Violation: High</td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>Each instance of non-meeting this service level will be treated as one (1) violation.</td></tr>
<tr><td>Infrastructure Availability</td><td>RPO (zero data loss in case of failure of Primary DC) should be zero minutes

Severity of Violation: High

Each instance of non-meeting this service level will be treated as two (2) violations.</td></tr>
<tr><td>Infrastructure Performance</td><td>Sustained period of peak CPU utilization of any server crossing 70% (with the exception of batch processing) shall be less than or equal to 30 minutes.

Severity of Violation: High

Each occurrence where the peak CPU utilization of any server crosses 70% (with the exception of batch processing) and stays above 70% for time more than 30 minutes will be treated as one (1) instance.

<table><tr><td>Number of instances over the six month period</td><td>Violations for calculation of penalty</td></tr><tr><td>>0 & <=3</td><td>1</td></tr><tr><td>> 3</td><td>2</td></tr></table>
In addition to the above, if the number of instances in any month in the six-month period exceeds 3, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Infrastructure Performance</td><td>Sustained period of peak I/O utilization of any server crossing 70% (with the exception of batch processing) shall be less than or equal to 30 minutes.

Severity of Violation: High

Each occurrence where the peak I/O utilization of any server crosses</td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>70% (with the exception of batch processing) and stays above 70% for time more than 30 minutes will be treated as one (1) instance.

<table><tr><td>Number of instances over the six month period</td><td>Violations for calculation of penalty</td></tr><tr><td>>0 & <=3</td><td>1</td></tr><tr><td>> 3</td><td>2</td></tr></table>
In addition to the above, if the number of instances in any month in the six-month period exceeds 3, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Infrastructure Performance</td><td>Sustained period of peak memory utilization of any server crossing 70% (with the exception of batch processing) shall be less than or equal to 30 minutes.

Severity of Violation: High

Each occurrence where the peak memory utilization of any server crosses 70% (with the exception of batch processing) and stays above 70% for time more than 30 minutes will be treated as one (1) instance.

<table><tr><td>Number of instances over the six month period</td><td>Violations for calculation of penalty</td></tr><tr><td>>0 & <=3</td><td>1</td></tr><tr><td>> 3</td><td>2</td></tr></table>
In addition to the above, if the number of instances in any month in the six-month period exceeds 3, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Application Availability</td><td>Availability of CAS solution components measured within the Data Center shall be at least 98%</td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>Severity of Violation: High

This service level will be monitored on a monthly basis.

<table><tr><td>Availability over the six-month period</td><td>Violations for calculation of penalty</td></tr><tr><td>< 98% & >= 96%</td><td>1</td></tr><tr><td>< 96% & >= 94%</td><td>2</td></tr><tr><td>< 94%</td><td>3</td></tr></table>
In addition to the above, if the service level in any month in the six-month period falls below 99%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Application Availability</td><td>Availability of non-CAS solution components measured within the Data Center shall be at least 97%

Severity of Violation: Medium

This service level will be monitored on a monthly basis.

<table><tr><td>Availability over the six-month period</td><td>Violations for calculation of penalty</td></tr><tr><td>< 97% & >= 96%</td><td>1</td></tr><tr><td>< 96%</td><td>2</td></tr></table>
In addition to the above, if the service level in any month in the six-month period falls below 96%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Application Performance</td><td>Average application response time during peak usage hours as measured from a client terminal within the Data Center shall not exceed 4 seconds.</td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>Severity of Violation: High

The list of critical business functions and peak usage hours will be identified by the Haryana Police during the Supply and System Integration Phase.

This service level will be monitored on a monthly basis.

<table>
<tr><td>Average application response time over the six-month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>> 4s & <= 5s</td><td>2</td></tr>
<tr><td>> 5s & <= 6s</td><td>4</td></tr>
<tr><td>> 6s</td><td>5</td></tr>
</table>

In addition to the above, if the average turnaround time in any month in the six-month period goes beyond 6s, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
</table>

2. Client Site Infrastructure Systems

(a) **Critical Client Site Systems**. The failure or disruption results in inability of the police station / higher offices to service its dependent offices or perform critical back-office functions. Critical client site infrastructure means the IT infrastructure at client site which are shared by multiple users i.e., Core Switch, Core Routers, etc.

(b) This service level will be measured on a monthly basis for each implementation site.

(c) The below tables gives details on the Service Levels the SI should maintain.

Service Level Description	Measurement
Client Site Systems Availability	Availability of the critical client site infrastructure components at all the implementation sites shall be at least 99% Severity of Violation: High This service level will be measured on a monthly basis for each implementation site. If the availability in a month for an implementation site falls below the minimum service level, it will be treated as one (1) violation. The total number of violations for the six-month period will be the cumulative number of violations across all the months across all sites in the six-month period.

3. Handholding Support: Client Site Support

(a) **Level 1 Incidents**. The incident has an immediate impact on the Haryana Police's ability to service its police stations / higher offices, to perform critical back-office functions or has a direct impact on the organization.

(b) **Level 2 Incidents.** The incident has an impact on the Haryana Police's ability to service its police stations / higher offices that while not immediate, can cause service to degrade if not resolved within reasonable time frames

(c) The severity of the individual incidents will be mutually determined by the Haryana Police and SI.

(d) The scheduled operation time for the client site systems shall be the business hours of the Haryana Police.

(e) This service level will be measured on a monthly basis for each implementation site.

(f) The tables on the following page give details of the Service Levels the SI is required to maintain.

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td>Client Site Support Performance</td><td>80% of the Level 1 Incidents at each site should be resolved within 2 business hours from the time call is received / logged which ever is earlier. The maximum resolution time for any incident of this nature shall not exceed 8 business hours.

Severity of Violation: Medium

This service level will be measured on a monthly basis for each implementation site.

If the performance in a month for an implementation site falls below the minimum service level, it will be treated as one (1) instance. The total number of instances for the six-month period will be the cumulative number of instances across all the months across all sites in the six-month period.

Average number of instances per month = (Total number of instances for the six-month period) / 6

<table><tr><td>Average number of instances per month</td><td>Violations for calculation of penalty</td></tr><tr><td>>0 & <=4</td><td>1</td></tr><tr><td>>4 & <=8</td><td>2</td></tr><tr><td>>8 & <=12</td><td>3</td></tr><tr><td>>12</td><td>4</td></tr></table></td></tr>
<tr><td>Client Site Support Performance</td><td>80% of the Level 2 Incidents at each site should be resolved within 6 business hours from the time a call is received / logged which ever is earlier. The maximum resolution time for any incident of this nature shall not exceed 48 hours.

Severity of Violation: Medium</td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>This service level will be measured on a monthly basis for each implementation site.

If the performance in a month for an implementation site falls below the minimum service level, it will be treated as one (1) instance. The total number of instances for the six-month period will be the cumulative number of instances across all the months across all sites in the six-month period.

Average number of instances per month = (Total number of instances for the six-month period) / 6

<table>
<tr><td>Average number of instances per month</td><td>Violations for calculation of penalty</td></tr>
<tr><td>>0 & <=4</td><td>1</td></tr>
<tr><td>>4 & <=8</td><td>2</td></tr>
<tr><td>>8 & <=12</td><td>3</td></tr>
<tr><td>>12</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>Client Site Support Performance</td><td>Replacement of hardware equipment shall be done within 7 days of notification by the Haryana Police. These equipments would have failed on four or more occasions in a period of less than three months or six times in a period of less than twelve months. (Mean Time Between Failure Condition)

Severity of Violation: High

Each instance of non-meeting this service level will be treated as one (1) violation.</td></tr>
</table>

4. <u>Handholding Support: Application Support</u>

(a) **Level 1 Defects**. The failure to fix has an immediate impact on the Haryana Police's ability to service its police stations / higher offices, inability to perform critical back-office functions or a direct impact on the organization.

(b) **Level 2 Defects.** The failure to fix has an impact on the Haryana Police's ability to service its police stations / higher offices that while not immediate, can cause service to degrade if not resolved within reasonable time frames.

(c) **Level 3 Defects.** The failure to fix has no direct impact on the Haryana Police's ability to serve its police stations / higher officers, or perform critical back-office functions.

(d) The severity of the individual defects will be mutually determined by the Haryana Police and SI.

(e) This service level will be monitored on a monthly basis.

(f) The below tables gives details on the Service Levels the SI should maintain.

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td>Application Support Performance</td><td>95% of the Level 1 defects shall be resolved within 4 business hours from the time of reporting full details.

Severity of Violation: High

This service level will be monitored on a monthly basis.

<table>
<tr><td>Performance over the six-month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>< 95% & >= 90%</td><td>1</td></tr>
<tr><td>< 90% & >= 85%</td><td>2</td></tr>
<tr><td>< 85%</td><td>3</td></tr>
</table>

In addition to the above, if the service level in any month in the six-month period falls below 85%, one (1) additional violation will be added</td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>for each such month to the overall violations for this service level.</td></tr>
<tr><td>Application Support Performance</td><td>95% of the Level 2 defects shall be resolved within 72 hours from the time of reporting full details.

Severity of Violation: High

This service level will be monitored on a monthly basis.

<table><tr><td>Performance over the six-month period</td><td>Violations for calculation of penalty</td></tr><tr><td>< 95% & >= 90%</td><td>1</td></tr><tr><td>< 90% & >= 85%</td><td>2</td></tr><tr><td>< 85%</td><td>3</td></tr></table>
In addition to the above, if the service level in any month in the six-month period falls below 85%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Application Support Performance</td><td>100% of the Level 3 defects shall be resolved within 120 hours from the time of reporting full details.

Severity of Violation: High

This service level will be monitored on a monthly basis.

<table><tr><td>Performance over the six-month period</td><td>Violations for calculation of penalty</td></tr><tr><td>< 100% & >= 90%</td><td>1</td></tr><tr><td>< 90% & >= 80%</td><td>2</td></tr><tr><td>< 80%</td><td>3</td></tr></table></td></tr>
</table>

Service Level Description	Measurement
	In addition to the above, if the service level in any month in the six-month period falls below 80%, one (1) additional violation will be added for each such month to the overall violations for this service level.
Application Support Performance	Up to date of the documentation of the design, modifications, enhancements, and defect-fixes in the half-yearly period. Severity of Violation: Medium This service level will be measured on a half-yearly basis. Each instance of non-meeting this service level will be treated as one (1) violation.

5. <u>Network Uptime:</u>

Severity of Violation: High

This service level will be monitored on a monthly basis.

The below tables gives details on the Service Levels the SI should maintain.

Service Level Description	Measurement
Network Uptime	Availability of the network and all related components at all the implementation sites shall be at least 99% Severity of Violation: High This service level will be measured on a monthly basis for each implementation site. If the network availability in a month falls below the minimum service

Service Level Description	Measurement
	level, it will be treated as one (1) violation. The total number of violations for the six-month period will be the cumulative number of violations across all the months across all sites in the six-month period.

6. Handholding Support: Helpdesk and Data Center Support

(a) **Level 1 Calls**. The failure to fix has an immediate impact on the Haryana Police's ability to service its police stations / higher offices, inability to perform critical back-office functions or a direct impact on the organization.

(b) **Level 2 Calls.** The failure to fix has an impact on the Haryana Police's ability to service its police stations / higher offices that while not immediate, can cause service to degrade if not resolved within reasonable time frames.

(c) **Level 3 Calls.** The failure to fix has no direct impact on the Haryana Police's ability to serve its police stations / higher offices, or perform critical back-office functions.

(d) This service level will be monitored on a monthly basis.

(e) The scheduled operation time for the Helpdesk shall be 24X7

(f) The below tables gives details on the Service Levels the SI should maintain.

Service Level Description	Measurement
Helpdesk Performance	98% of the calls shall be answered within 45 seconds. Severity of Violation: High This service level will be monitored on a monthly basis.

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>
<table>
<tr><th>Performance over the six-month period</th><th>Violations for calculation of penalty</th></tr>
<tr><td>< 98% & >= 90%</td><td>1</td></tr>
<tr><td>< 90% & >= 80%</td><td>2</td></tr>
<tr><td>< 80%</td><td>3</td></tr>
</table>

In addition to the above, if the service level in any month in the six-month period falls below 80%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Helpdesk Performance</td><td>98% of the incidents within helpdesk resolution capacity shall be resolved in a cycle time of 24 hours

Severity of Violation: High

This service level will be monitored on a monthly basis.

<table>
<tr><th>Performance over the six-month period</th><th>Violations for calculation of penalty</th></tr>
<tr><td>< 98% & >= 90%</td><td>1</td></tr>
<tr><td>< 90% & >= 80%</td><td>2</td></tr>
<tr><td>< 80%</td><td>3</td></tr>
</table>

In addition to the above, if the service level in any month in the six-month period falls below 80%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Helpdesk Performance</td><td>98% of the non SI supported incidents shall be routed to the appropriate service provider within 30 minutes.

Severity of Violation: Medium</td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>This service level will be monitored on a monthly basis.

<table><tr><td>Performance over the six-month period</td><td>Violations for calculation of penalty</td></tr><tr><td>< 98% & >= 90%</td><td>1</td></tr><tr><td>< 90% & >= 80%</td><td>2</td></tr><tr><td>< 80%</td><td>3</td></tr></table>
In addition to the above, if the service level in any month in the six-month period falls below 80%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Helpdesk Performance</td><td>80% of the Level 1 calls shall be resolved within 2 hours from call received / logged which ever is earlier. The maximum resolution time for any incident of this nature shall not exceed 8 business hours.

Severity of Violation: High

This service level will be monitored on a monthly basis.

<table><tr><td>Performance over the six-month period</td><td>Violations for calculation of penalty</td></tr><tr><td>< 80% & >= 70%</td><td>1</td></tr><tr><td>< 70% & >= 60%</td><td>2</td></tr><tr><td>< 60%</td><td>3</td></tr></table>
In addition to the above, if the service level in any month in the six-month period falls below 60%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Helpdesk Performance</td><td>80% of the Level 2 calls shall be resolved within 6 hours from call received / logged which ever is earlier. The maximum resolution time</td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>for any incident of this nature shall not exceed 48 hours.

Severity of Violation: High

This service level will be monitored on a monthly basis.

<table><tr><td>Performance over the six-month period</td><td>Violations for calculation of penalty</td></tr><tr><td>< 80% & >= 70%</td><td>1</td></tr><tr><td>< 70% & >= 60%</td><td>2</td></tr><tr><td>< 60%</td><td>3</td></tr></table>
In addition to the above, if the service level in any month in the six-month period falls below 60%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Helpdesk Performance</td><td>80% of the Level 3 calls shall be reported on status and action to be communicated within 24 hours from call received / logged which ever is earlier. The maximum resolution time for any incident of this nature shall not exceed 72 hours.

Severity of Violation: High

This service level will be monitored on a monthly basis.

<table><tr><td>Performance over the six-month period</td><td>Violations for calculation of penalty</td></tr><tr><td>< 80% & >= 70%</td><td>1</td></tr><tr><td>< 70% & >= 60%</td><td>2</td></tr><tr><td>< 60%</td><td>3</td></tr></table>
In addition to the above, if the service level in any month in the six-</td></tr>
</table>

Service Level Description	Measurement
	month period falls below 60%, one (1) additional violation will be added for each such month to the overall violations for this service level.
Datacenter Support Performance	Replacement of hardware equipment shall be done within 15 days of notification by the Haryana Police. These equipments would have failed on four or more occasions in a period of less than three months or six times in a period of less than twelve months. (Mean Time Between Failure Condition) Severity of Violation: High Each instance of non-meeting this service level will be treated as one (1) violation.
Datacenter Support Performance	Up to date of the documentation of the design, modifications, enhancements, and fixes. Severity of Violation: Medium This service level will be measured on a half-yearly basis. Each instance of non-meeting this service level will be treated as one (1) violation.

7. Reporting

(a) The below tables gives details on the Service Levels the SI should maintain for client site systems availability.

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td>Availability and Performance Report</td><td>Provide monthly SLA compliance reports, monitoring and maintenance related MIS reports by the 5th of the following month.

Severity of Violation: Medium

This service level will be monitored on a monthly basis.

If the monthly SLA compliance report related to the service level metrics is not provided in the given timeframe, it will be treated as one (1) instance.

The total number of instances for the six-month period will be the cumulative number of instances across all the months in the six-month period.

<table>
<tr><td>Total number of instances over the six month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>>0 & <=3</td><td>1</td></tr>
<tr><td>> 3</td><td>2</td></tr>
</table>
</td></tr>
</table>

8. Credits for Successful Application Uptake

The below tables gives details of the credits that can gained by the SI for successful uptake of the application in the State/UT. The credits will not be calculated for the first reporting period and would commission from next reporting period.

Service Level Description	Measurement
CCTNS Uptake	The following metrics will be measured at the end of each reporting period for each District that has been declared as “Go Live”:

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>
1. Number of key transactions carried through internet (ex: Transactional such as submitting an application for a no-objection certificate and Informational such a requesting the status of a case)
2. Number of active users profiles in CCTNS
3. Number of read-write transactions on CCTNS system
4. Number of Searches carried out on data in CCTNS
5. Total number of FIRs prepared through CCTNS
6. Total number of Crime Details Forms prepared through CCTNS
7. Total number of Key Investigation Forms prepared through CCTNS
8. Total number of Arrest Cards prepared through CCTNS
9. Total number of ChargeSheets prepared through CCTNS
10. Quality (recency and accuracy) of information available in CCTNS
11. Number of cases reported to be solved because of the availability of CCTNS
12. Number of ad-hoc requests successfully responded to using CCTNS
13. Turnaround Time for submitting the monthly and annual crime/criminal information to NCRB from the State/UT

A credit will be gained for each of the above parameters if the uptake for that parameter shows significant improvement.

The following table applies for each of the above parameters:

<table>
<tr><td>% increase over the measurement in the last reporting period</td><td>Credits</td></tr>
<tr><td>>5 & <=10%</td><td>2</td></tr>
<tr><td>>10 & <=15%</td><td>3</td></tr>
<tr><td>> 15%</td><td>4</td></tr>
</table>
</td></tr>
</table>

9. Violations and Associated Penalties

(a) 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.

(b) A six monthly performance evaluation will be conducted using the six monthly reporting periods of that period.

(c) **Penalty Calculations.** The framework for Penalties, as a result of not meeting the Service Level Targets are as follows:

(i) 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.

(ii) The number of violations in the reporting period for each level of severity will be totaled and used for the calculation of Penalties.

a. If the total number of credits gained by the SI is lower than the total number of high severity violations in the reporting period, the total number of credits will be subtracted from the total number of High Severity Violations in the reporting period for the calculation of Penalties.
b. If the total number of credits gained by the SI is higher than the total number of high severity violations in the reporting period, the resultant total number of high severity violations in the reporting period for calculation of penalties will be considered as zero (0).

(iii) Penalties applicable for each of the high severity violations is two (2) % of respective half yearly payment to the SI.

(iv) Penalties applicable for each of the medium severity violations is one (1%) of respective half yearly payment to the SI.

(v) Penalties applicable for each of the low severity violations is half percentage (0.5%) of respective half yearly payment to the SI.

(vi) Penalties applicable for not meeting **a high (H) critical** performance target in two consecutive half years on same criteria shall result in additional deduction of 5% of the respective half yearly payment to the SI. Penalty shall be applicable separately for each such high critical activity

(vii) Penalties applicable for not meeting **a medium (M) critical** performance target in two consecutive half yearly periods on same criteria shall result in additional deduction of 3% of the respective half yearly payment to the SI. Penalty shall be applicable separately for each such medium critical activity

(viii) Penalties applicable for not meeting **a low (L) critical** performance target in two consecutive half yearly periods on same criteria shall result in additional deduction of 2% of the respective half yearly payment to the SI. Penalty shall be applicable separately for each such medium critical activity

(ix) It is to be noted that if the overall penalty applicable for any of the review period during the currency of the contract exceeds 25% or if the overall penalty applicable for any of the successive half year periods during the currency of the contract is above 15%; then the Haryana Police shall have the right to terminate the contract.

5 ANNEXURE

5.1 Annexure – A: Format for Change Control Notice

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.)		
Authorised by Haryana Police	Date:	
Name:		
Signature: Received by the SI	Date:	
Name:		
Signature:		
Change Control Note		**CCN Number:**
Part B : Evaluation		
(Identify any attachments as B1, B2, and B3 etc.) Changes to Services, charging structure, payment profile, documentation, training, service levels and component working arrangements and any other contractual issue.		
Brief Description of Solution:		
Impact:		
Deliverables:		
Timetable:		

Charges for Implementation: (including a schedule of payments)	
Other Relevant Information: (including value-added and acceptance criteria)	
Authorised by the System Integrator	**Date:**
Name:	
Signature:	

Change Control Note	**CCN Number :**
Part C : Authority to Proceed	
Implementation of this CCN as submitted in Part A, in accordance with Part B is: (tick as appropriate)	
Approved	

Rejected **Requires Further Information** (as follows, or as Attachment 1 etc.)	
For Haryana Police and its nominated agencies	**For the Implementation Partner**
Signature	Signature
Name	Name
Title	Title
Date	Date

5.2 Annexure – B: List of Services to be provided by the SI

Various services including, but not limiting, to be offered by the selected Bidder will include:

i. Project initiation & Solution Design including SRS, Design documents, hardware requirement report & detailed deployment plan for the software applications & other components of the project,

ii. Development / Customization of the CCTNS Solution including the testing and user acceptance

iii. Site Preparation and LAN creation

iv. Procurement, deployment and commissioning of the necessary Hardware at all the Police locations mentioned in geographical scope of RFP Volume I

v. Procurement, deployment and commissioning of the required Networking equipments & connectivity,

vi. Data Entry and digitization of the records available in the paper files and migration of the data available in the existing databases,

vii. Training to the staff members and stakeholders of the Department and necessary Change Management, and

viii. Provisioning of Change Management and Handholding support for a period of one year post successful Go Live of CCTNS Solution

ix. Operations and maintenance of the system including providing technical support for IT solution for a period of 5 years starting from the date of successful Go Live of CCTNS Solution

Note:

- SI will have to implement the Solution keeping in mind the functions and services of the department and at the end the solution shall include all the necessary application modules as well as hardware components as per the requirements of Haryana Police
- The selected SI shall implement the solution based on the requirements identified in this RFP and shall suggest improvements (if any) at the time of the designing the solution. It is expected that SI will validate the Requirements/ Architecture deigns, etc. proposed in this RFP and will improve upon it, if required.

5.4 Annexure – C: Minimum Required Deliverables and Associated Timelines

S. No.	Project Activity	Deliverables	Timelines (T - from date of signing of contract)
1.	Project planning	i. Detailed Project Plan for Implementation of the Project ii. Risk Management and Mitigation Plan iii. Manpower Deployment Plan	T
Study and Design			
2.	System Study – study the legislation, business processes and organization design of Haryana Police along with relevant reports such as PIM	iv. A comprehensive System Study document v. Updated/ vetted FRS report including list of additional features that would result in further improvement in the overall application performance for consideration of the department	T + 8 Weeks
3.	Detailed assessment of functional requirements and MIS requirements	vi. A comparative report on the extent of functionality currently available in the vendor's application (CAS provided by Centre) other applications/ COTS products and with the FRS for CRP	
4.	Finalization/ Vetting of FRS	vii. Detailed integration and interfacing model viii. Change/Reference document including all the changes or deviations from the base version of the CAS(State)/ FRS of other modules	
5.	Preparation of System Requirement Specification report and Software Requirement Specification report	ix. System Requirement Specification Report and Software Requirement Specification reports meeting all the Business, Functional and technical requirement of Haryana Police and incorporating all the functional specifications, standards provided by the NCRB, Haryana Police specific requirements and different integration points with CAS (Centre), external agencies and other applications of Haryana Police x. List of additional features proposed in complete CCTNS Application xi. CAS (State) Implementation document w.r.t. Configuration, Customization, Extension and Integration as per Haryana Police's requirements	

S. No.	Project Activity	Deliverables	Timelines (T - from date of signing of contract)
6.	Procurement of IT infrastructure at Data Centre and DR		T + 8 Weeks
7.	Preparation of Solution Design documents	A detailed Design document including: xii. Technical Architecture Document (Application, Network, and Security) xiii. High Level Design (including but not limited to) a. Application architecture documents b. ER diagrams and other data modelling documents c. Logical and physical database design d. Data dictionary and data definitions e. Application component design including component deployment views, control flows, etc. xiv. Low Level Design (including but not limited to) a. Application flows and logic including pseudo code b. GUI design (screen design, navigation, etc.) c. Database architecture, including defining data structure, data dictionary as per standards laid-down by GoI/ GoH xv. CCTNS Application Test Plans and Test Cases	T + 10 Weeks
8.	Site Survey	xvi. A site survey report detailing the current status of each site and the enhancements to be made at each site (s) based on the State's requirement and the guidelines of MHA, NCRB	T + 10 Weeks
9.	IT infrastructure sizing	xvii. Final BoM with Technical specifications for the IT Hardware, Network and other IT Infrastructure Requirements xviii. Strategy for Data Centre and DR Site xix. Report on the reusability of existing infrastructure xx. Hardware procurement & Deployment plan	T + 11 Weeks
10.	Others	xxi. Data Migration Strategy and Methodology	T+11 Weeks

S. No.	Project Activity	Deliverables	Timelines (T - from date of signing of contract)
11.	Commissioning and operationalization of IT infrastructure at Data Centre and DR		T + 11 Weeks
Implement (This shall only begin after CAS (State)[3] has been received from NCRB, MHA) – T1			
12.	Study and analyze the CAS (State) system as received from NCRB against the requirements of Haryana Police and conduct Conference Room Pilot (CRP) based on the requirement specifications	xxii. Feedback Report based on CRP I and CRP II	T1 + 4 Weeks
13.	Finalization of requirement specifications	xxiii. Final FRS, SyRS, SRS and other requirements with all the Solution Design documents	T1 + 6 Weeks
14.	Configuration & Customization of CAS (State) and development of additional modules		T1 + 14 Weeks
15.	Integration with CAS (Centre)		T1+ 14 Weeks
16.	Data migration and digitization of historical data		T1 + 14 Weeks
17.	Migration of CIPA and CCIS Police Stations/ non-CIPA and CCIS Police Stations/ Higher Offices to CCTNS		T1 + 15 Weeks
18.	Testing of configured & deployed solution (CAS) and additional functionalities		T1 + 16 Weeks
19.	Site preparation at Pilot Phase Client site locations		T1 + 18 Weeks
20.	Procurement, Commissioning and Operationalizing the IT infrastructure at Pilot phase Police locations		T1 + 20 Weeks
21.	User Acceptance and Testing of Pilot Phase implementation		T1 + 20 Weeks

[3] As per the guidelines of CCTNS MMP, Core Application Software (State) would be provided by NCRB.

S. No.	Project Activity	Deliverables	Timelines (T - from date of signing of contract)
22.	User Training on Pilot Phase CCTNS Solution		T1 + 22 Weeks
23.	Pilot rollout in two districts	xxiv. Report on amendments / enhancements / modifications made based on inputs of Haryana Police	T1 + 22 Weeks
24.	Go-Live of Pilot	xxv. Pilot phase Acceptance from Haryana Police	T1 + 24Weeks
25.	Improvement of application according to the experience of Phase I	xxvi. Pilot phase Go-Live Report including a. Site Preparation and Infrastructure Deployment / Commissioning Report for Pilot Sites, Data Centre and DR Site b. Data Migration report for Pilot phase c. Performance and Load Testing Report for Pilot phase	T1 + 24 Weeks
26.	CCTNS Solution customization for Phase II and integrating with external agencies		T1 + 32 Weeks
27.	Site preparation at Phase II Client locations		T1 + 42 Weeks
28.	Procurement, Commissioning and Operationalizing of IT infrastructure at Phase II Client locations		T1 + 42 Weeks
29.	Capacity Building and Change Management		T1+ 44 Weeks
30.	User Training on complete CCTNS Solution		T1 + 44 Weeks
31.	State wide rollout of Phase II	xxvii. Report on amendments / enhancements / modifications made based on inputs of Haryana Police / Third Party's Acceptance Testing for State-wide Roll-Out	T1 + 45 Weeks
32.	3rd party Acceptance testing, audit and certification of complete CCTNS Solution	xxviii. Third Party Acceptance Testing Certificate	T1 + 48 Weeks
33.	SLA and Performance Monitoring Plan	xxix. Detailed plan for monitoring of SLAs and performance of the overall system	Before "Go-Live"
34.	Go-Live for complete CCTNS Solution	xxx. Go-Live Acceptance from Haryana Police xxxi. Report on roll-out across State including a. Site Preparation and Infrastructure Deployment Report across State b. Manpower Deployment Report c. Data Migration Report including Test Plans and	T1 + 50 Weeks

S. No.	Project Activity	Deliverables	Timelines (T - from date of signing of contract)
		Test Results for Data Migration d. Training Delivery Report e. Overall Test Report	
Post Implementation - Operation and Maintenance			**5 Years since the "Go-Live" of Complete CCTNS Solution**
1.	Handholding support		For next 1 year from "Go-Live of each of the phases - Pilot and complete CCTNS solution respectively"
2.	Project Operation and Maintenance	xxxii. Fortnightly Progress Report on Project including SLA Monitoring Report and Exception Report xxxiii. Project Quality Assurance report xxxiv. Details on all the issues logged	**5 Years from the date of "Go-Live" of Complete CCTNS Solution**

5.5 Annexure – E: Bill of Material

Indicative Bill of Material

A. Bill of Material – Software Solution

The below list is indicative only [4]	Proposed Solution (Provide the Product Name or fill Custom Built, in case of a new development) [5]	Unit of Measurement	Number of Licenses (Development Environment) [6]	Number of Licences (UAT) [4]	Number of Licences (Training) [4]	Number of Licences (Data Center - Production) [4]	Number of Licences (DR Site) [4]
CAS (State) Solution							
Web server							
Application Server							
Database							
Operating System							

[4] In case the number of licenses offered are different for each of the services within the solution (ex, multiple services within EMS are provisioned with different licenses), please insert rows under the solution head and provide the information

[5] It is possible that the SI has not suggested the solution as the list is indicative only. In case any of the item is not provided, the SI may indicate N/A in the corresponding cells

[6] Please indicate N/A where not applicable. Please indicate N/L where there is no license requirement

The below list is indicative only [4]	**Proposed Solution (Provide the Product Name or fill Custom Built, in case of a new development)** [5]	**Unit of Measurement**	**Number of Licenses (Development Environment)** [6]	**Number of Licences (UAT)** [4]	**Number of Licences (Training)** [4]	**Number of Licences (Data Center - Production)** [4]	**Number of Licences (DR Site)** [4]
Others							
Reporting Engine							
Email/Messaging							
Search Engine							
Portal Server							
Workflow Engine							
Rules Engine							
Directory Services							
DMS/CMS							
Security							
Identity Management							
Audit							

The below list is indicative only [4]	**Proposed Solution (Provide the Product Name or fill Custom Built, in case of a new development)** [5]	**Unit of Measurement**	**Number of Licenses (Development Environment)** [6]	**Number of Licences (UAT)** [4]	**Number of Licences (Training)** [4]	**Number of Licences (Data Center - Production)** [4]	**Number of Licences (DR Site)** [4]
ETL							
Any Other Proposed							
CAS (State) Offline Solution							
Synchronization Solution							
Application Container							
Database							
Others							
Operating System (In case the suggested solution will need a particular kind of O/S on the client machine)							
Any Other Proposed							

The below list is indicative only [4]	**Proposed Solution (Provide the Product Name or fill Custom Built, in case of a new development)** [5]	**Unit of Measurement**	**Number of Licenses (Development Environment)** [6]	**Number of Licences (UAT)** [4]	**Number of Licences (Training)** [4]	**Number of Licences (Data Center - Production)** [4]	**Number of Licences (DR Site)** [4]
Technical Environment at Police HQ							
Project Management Information System							
Configuration Management							
Issue Tracker							
Any Other Proposed							
Infrastructure Services (at DC/DR)							
EMS							
Load Balancers							
Backup Software							

The below list is indicative only [4]	**Proposed Solution (Provide the Product Name or fill Custom Built, in case of a new development)** [5]	**Unit of Measurement**	**Number of Licenses (Development Environment)** [6]	**Number of Licences (UAT)** [4]	**Number of Licences (Training)** [4]	**Number of Licences (Data Center - Production)** [4]	**Number of Licences (DR Site)** [4]
Helpdesk							
Antivirus							
SAN Management Software							
Any Other Proposed							

Note: *The SI will ensure that all the licenses of proposed application / system software etc. procured for this project are procured in the name of Haryana Police and shall be unrestricted user enterprise edition perpetual licenses.*

B. Bill of Material – Infrastructure

	Reference of the server/storage information in the Submitted Proposal (Please provide page number/section-number/volume)	Services proposed to be hosted on the Server	Quantity	Make and Model	Year of Introduction	Operating System along with version (if applicable)	Processor and Number of Cores Offered (if applicable)	Architecture (RISC/EPIC/CISC) (if applicable)	RAM (if applicable)	HDD (if applicable)	LAN Ports (if applicable)	HBA (if applicable)	Additional Information as required to indicate the compliance to the requirements in the RFP (ex, Capacity, Disk Space, ….)	Compliance Matrix Provided as per the format given in the RFP (Yes/No) In case the matrix is not provided, please provide the same	Data Sheets Provided in the Proposal (Yes/No) In case the datasheets are not provided, please provide the same
Data Centre															
Production CAS (State) Application Services Related Servers (Web,															

Portal, Application, Database, Directory….)															
Insert each item in a separate row as required															
Infrastructure Services Related Servers (EMS, Antivirus, Backup, DNS,…)															
Insert each item in a separate row as required															
SAN Storage															

SAN Switch															
FC-IP Router															
Tape Library															
Technical Environment at NCRB (Project Management, Configuration Management, Issue Tracker,…)															
Insert each item in a separate row as required															

UAT Environment															
Insert each item in a separate row as required															
Training Environment															
Insert each item in a separate row as required															
Disaster Recovery															
Production CAS (State) Application Services Related Servers (Web, Portal,															

Application, Database, Directory….)															
Insert each item in a separate row as required															
Infrastructure Services Related Servers (EMS, Antivirus, Backup, DNS,…)															
Insert each item in a separate row as required															
SAN Storage															

SAN Switch															
FC-IP Router															
Tape Library															

C. Indicative Hardware Requirements

Hardware Requirements	
Police Stations - 270 in number	**Indicative Quantity # (units)**
Desktops at Police Stations	
Desktop with pre-loaded OS as per the technology stack adopted – 4 at each location	1080
Desktop Virtualization Mode[7]l at Police Stations	
1 Set each comprising of 4 TFT Screens, four keyboards, four optical mouse, and one CPU with additional one more CPU as backup and associated h/w & s/w for desktop virtualization with pre-loaded OS as per the technology stack adopted	270
Other Hardware	
Desktops	656
HDD 320 GB or higher	270
Multi-Function Laser (Print/Scan/Copy)	376
SNMP based UPS for 120min backup	376
2KVA Generator Set	270
16-Port Switch	130
24-Port Switch	2
Fingerprint Reader	270
Digital Camera	270
Electronic Pen	270
Duplex Laser Printer (Black/ White)	310
600 VA UPS with 60 Min backup	332
Office productivity software Enterprise edition perpetual licenses - latest	Same as total

[7] Haryana Police reserves the right to adopt either model of Desktops deployment at Police Stations.

version	number of desktops specified based on the model proposed
Hardware for SDC and DR	
Servers	9
SAN Storage	2
SAN Management Software	As required
SAN Switch	4
Tape Library	2
Backup Software	2
KVM Switches	2
Server Load Balancer	1
RDBMS Licenses (full use and perpetual licenses for 2 Database servers)	Number to be proposed based on the technology stack adopted
CAL License of Enterprise Management System (EMS) for Police Department equipments considering the expansion of atleast 20-25% in near future	Total number of network based component as per model (Desktop or Virtualization model)
Server Operating Systems	9
Router using separate IP scheme to terminate aggregated bandwidth from SWAN and VPN over broadband network.	1
24 Port L3 Switch to connect the IT Infrastructure of Haryana Police inside the SDC	2
Civil Works	***No. of Locations***
Flooring	270
Wall Finishing and Painting	270
Roller Blinds	270

Ceiling Mounted Light fixtures	270
4 mm thick Glass for door renovation	270
Split Type AC	270
Workstations with allied furniture	270
Cabinets (48 Sq. Ft. Approx of 1.8 ft. depth)	270
Creation of LAN (structured cabling with creation of LAN nodes, laying CAT-6 UTP cables, patch panels, cable crimping, installing RJ-45, etc.)	***No. of Locations***
Police Stations (approx. no. of nodes 6 per location)	100
Sub-Division Offices (approx. no. of nodes 6 per location)	60
District Head Offices (approx. no. of nodes 12 per location)	10
Commissionerates (approx. no. of nodes 25 per location)	2
Range Headquarters (approx. no. of nodes 5 per location)	4
SCRB (approx. no. of nodes 5 per location)	1
Police Headquarters (approx. no. of nodes 50 per location)	1

Note:

- *These are only indicative numbers of material desired for the implementation of this project. Department reserves the right to increase or decrease the quantity of material at any time during the currency of the project to any extent and department shall make payments for each component on actual number provided by SI.*

- *SI shall be responsible for proposing other hardware/ software components as part of their Bill of Material for the successful implementation of this project*

Indicative Technical Specifications

A. Minimum Technical Specifications Requirement at State Data Center & Disaster Recovery Site

1. Enterprise Management and Monitoring Solution (EMS)

Haryana State has procured and is currently running a comprehensive Enterprise Management Solution for its SDC and at its State NOC respectively, which addresses the following areas:

- Network management comprising of Fault and root cause analysis solutions
- Performance monitoring for network and Servers
- Application Performance & Traffic Monitoring
- Host level security for servers
- Trouble ticketing system

As part of implementing the monitoring tool for this project, SI is required to procure full use CAL licenses of the existing EMS with Haryana State for this project from the OEM. SI shall be responsible for configuring and integrating the Haryana Police sites on the existing EMS. SI shall be required to provide all the necessary hardware/ software to meet the below mentioned indicative requirements from EMS.

Basic Requirements

- Solution should be inclusive with hardware, OS, patches, etc.
- Solution should provide for future scalability of the whole system without major architectural changes.
- Should be SNMP v1, v2, v3 and MIB-II compliant.
- Filtering of events should be possible, with advance sort option based on components, type of message, time etc.
- Should support Web / Administration Interface.
- Should provide compatibility to standard RDBMS.
- Solution should be open, distributed, and scalable and open to third party integration.
- Should provide fault and performance management for multi-vendor TCP/IP networks.

Security

- Should be able to provide secured windows based consoles / secured web-based consoles for accessibility to EMS.
- Should have web browser interface with user name and Password Authentication.
- Administrator/ Manager should have privilege to create/modify/delete user.

Polling Cycle

- Support discriminated polling

- Should be able to update device configuration changes such as re-indexing of ports

Fault Management

- Should be able to get fault information in real time and present the same in alarm window with description, affected component, time stamp etc.
- Should be able to get fault information from heterogeneous devices — routers, switches, servers etc.
- Event related to servers should go to a common enterprise event console where a set of automated tasks can be defined based on the policy.
- Should have ability to correlate events across the entire infrastructure components of DC/DR.
- Should support automatic event correlation in order to reduce events occurring in DC/DR.
- Should support advanced filtering to eliminate extraneous data / alarms in Web browser and GUI.
- Should be configurable to suppress events for key systems/devices that are down for routine maintenance or planned outage.
- Should be able to monitor on user-defined thresholds for warning/ critical states and escalate events to event console of enterprise management system.
- Should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis.
- Should have self-certification capabilities so that it can easily add support for new traps and automatically generate alarms.
- Should provide sufficient reports pertaining to asset and change management, alarms and availability of critical network resources as well as network response times for critical links.
- The tool shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network and system components. The current performance state of the entire network and system infrastructure shall be visible in an integrated console.
- Should provide an integrated performance view for all the managed systems and networks along with the various threshold violations alarms in them. It should be possible to drill-down into the performance view to execute context specific reports
- Should provide the following reports for troubleshooting, diagnosis, analysis and resolution purposes: Trend Reports, At-A-Glance Reports, & capacity prediction reports
- Should be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits

Discovery

- Should provide accurate discovery of layer 3 and heterogeneous layer 2 switched networks for Ethernet, LAN and Servers etc.
- Manual discovery can be done for identified network segment, single or multiple devices.

Presentation

- Should be able to discover links with proper colour status propagation for complete network visualization.
- Should support dynamic object collections and auto discovery. The topology of the entire Network should be available in a single map.
- Should give user option to create his /or her map based on certain group of devices or region.
- Should provide custom visual mapping of L2 and L3 devices connectivity and relationships.

Agents

- Should monitor various operating system parameters such as processors, memory, files, processes, file systems etc. where applicable using agents on the servers to be monitored.
- Provide performance threshold configuration for all the agents to be done from a central GUI based console that provide a common look and feel across various platforms in the enterprise. These agents could then dynamically reconfigure them to use these threshold profiles they receive.

System Monitoring

- Should be able to monitor/manage large heterogeneous systems environment continuously.
- Windows OS
    - Should monitor / manage following:
        - Event log monitoring
        - Virtual and physical memory statistics
        - Paging and swap statistics
        - Operating system
        - Memory
        - Logical disk
        - Physical disk
        - Process
        - Processor
        - Paging file
        - IP statistics
        - ICMP statistics
        - Network interface traffic
        - Cache

        - Active Directory Services
    - Should be capable of view/start/stop the services on windows servers
- Unix / Linux
    - Should monitor with statistics :
        - CPU Utilization, CPU Load Averages
        - System virtual memory (includes swapping and paging)
        - Disk Usage
        - No. of Inodes in each file system
        - Network interface traffic
        - Critical System log integration

Infrastructure Services

- IIS / Tomcat / Apache / Web server statistics
- HTTP service
- HTTPS service
- FTP server statistics
- POP/ SMTP Services
- ICMP services
- Database Services – Monitor various critical relational database management system (RDBMS) parameters such as database tables / table spaces, logs etc.

Application Performance Management

- End to end Management of applications (J2EE/.NET based)
- Determination of the root cause of performance issues whether inside the Java application in connected back-end systems or at the network layer.
- Automatic discovery and monitoring of the web application environment
- Ability to monitor applications with a dashboard.
- Ability to expose performance of individual SQL statements within problem transactions
- Monitoring of third-party applications without any source code change requirements.
- Proactive monitoring of all end user transactions; detecting failed transactions; gathering evidence necessary for problem diagnose.
- Storage of historical data is for problem diagnosis, trend analysis etc.
- Monitoring of application performance based on transaction type
- Ability to identify the potential cause of memory leaks.

Reporting

- Should able to generate reports on predefined / customized hours.
- Should be able to present the reports through web and also generate “pdf” / CSV / reports of the same.

- Should provide user flexibility to create his /or her custom reports on the basis of time duration, group of elements, custom elements etc.
- Should provide information regarding interface utilization and error statistics for physical and logical links.
- Should create historical performance and trend analysis for capacity planning.
- Should be capable to send the reports through e-mail to pre-defined user with pre-defined interval.
- Should have capability to exclude the planned-downtimes or downtime outside SLA.
- Should be able to generate all sorts of SLA Reports.
- Should be able to generate web-based reports, historical data for the systems and network devices and Near Real Time reports on the local management console.
- Should be able to generate the reports for Server, Application, infrastructure services and Network devices in DC/DR environment.

Availability Reports

- Availability and Uptime – Daily, Weekly, Monthly and Yearly Basis
- Trend Report
- Custom report
- MTBF and MTTR reports

Performance Reports

- Device Performance – CPU and Memory utilized
- Interface errors
- Server and Infrastructure service statistics
- Trend report based on Historical Information
- Custom report
- SLA Reporting
- Computation of SLA for entire DC/DR Infrastructure
- Automated Daily, Weekly, Monthly, Quarterly and Yearly SLA reports

Data collection

- For reporting, required RDBMS to be provided with all licenses.
- Should have sufficient Storage capacity should to support all reporting data for 5 Years of DC/DR operation.

Integration

- Should be able to receive and process SNMP traps from infrastructure components such as router, switch, servers etc.
- Should be able integrate with Helpdesk system for incidents.
- Should be able to send e-mail or Mobile –SMS to pre-defined users for pre-defined faults.

- Should trigger automated actions based on incoming events / traps. These actions can be automated scripts/batch files.

Network Management

- The Network Management function must monitor performance across heterogeneous networks from one end of the enterprise to the other.
- It should proactively analyze problems to improve network performance.
- The Network Management function should create a graphical display of all discovered resources.
- The Network Management function should have extensive reporting facility, providing the ability to format and present data in a graphical and tabular display
- The Network Management function should collect and analyze the data. Once collected, it should automatically store data gathered by the NMS system in a database. This enterprise-wide data should be easily accessed from a central location and used to help with capacity planning, reporting and analysis.
- The Network Management function should also provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment, WAN links and routers.
- Alerts should be shown on the Event Management map when thresholds are exceeded and should subsequently be able to inform Network Operations Center (NOC) and notify concerned authority using different methods such as pagers, emails, etc.
- It should be able to automatically generate a notification in the event of a link failure to ensure proper handling of link related issues.
- The Systems and Distributed Monitoring (Operating Systems) of EMS should be able to monitor:
    - Processors: Each processor in the system should be monitored for CPU utilization. Current utilization should be compared against user-specified warning and critical thresholds.
    - File Systems: Each file system should be monitored for the amount of file system space used, which is compared to user-defined warning and critical thresholds.
    - Log Files: Logs should be monitored to detect faults in the operating system, the communication subsystem and in applications. The function should also analyze the files residing on the host for specified string patterns.
    - System Processes: The System Management function should provide real-time collection of data from all system processes. This should identify whether or not an important process has stopped unexpectedly. Critical processes should be automatically restarted using the System Management function.
    - Memory: The System Management function should monitor memory utilization and available swap space.

- Event Log: User-defined events in the security, system, and application event logs must be monitored.

SLA Monitoring

- The SLA Monitoring function of the EMS is by far the most important requirement of the DC/DR Project. The SLA Monitoring component of EMS will have to possess the following capabilities:
  - EMS should integrate with the application software component of portal software that measures performance of system against the following SLA parameters:
    - Response times of Portal;
    - Uptime of data centre;
    - Meantime for restoration of Data Centre etc;
  - EMS should compile the performance statistics from all the IT systems involved and compute the average of the parameters over a quarter, and compare it with the SLA metrics laid down in the RFP.
  - The EMS should compute the weighted average score of the SLA metrics and arrive at the quarterly service charges payable to the Agency after applying the system of penalties and rewards.
  - The SLA monitoring component of the EMS should be under the control of the authority that is nominated to the mutual agreement of Director, the partner so as to ensure that it is in a trusted environment.
  - The SLA monitoring component of the EMS should be subject to random third party audit to vouchsafe its accuracy, reliability and integrity.

Reporting

- The Reporting and Analysis tool should provide a ready-to-use view into the wealth of data gathered by Management system and service management tools. It should consolidate data from all the relevant modules and transform it into easily accessible business-relevant information. This information, should be presented in a variety of graphical formats can be viewed interactively
- The tool should allow customers to explore the real-time data in a variety of methods and patterns and then produce reports to analyze the associated business and service affecting issues.
- The presentation of reports should be in an easy to analyze graphical form enabling the administrator to put up easily summarized reports to the management for quick action (Customizable Reports). The software should be capable of supporting the needs to custom make some of the reports as per the needs of the organization.
- Provide Historical Data Analysis: The software should be able to provide a time snapshot of the required information as well as the period analysis of the same in order to help in projecting the demand for bandwidth in the future.

ITIL based Helpdesk System

- Helpdesk system would automatically generate the incident tickets and log the call. Such calls are forwarded to the desired system support personnel deputed

by the Implementation Agency. These personnel would look into the problem, diagnose and isolate such faults and resolve the issues timely. The helpdesk system would be having necessary workflow for transparent, smoother and cordial DC/DR support framework.

- The Helpdesk system should provide flexibility of logging incident manually via windows GUI and web interface.
- The web interface console of the incident tracking system would allow viewing, updating and closing of incident tickets.
- The trouble-ticket should be generated for each complaint and given to asset owner immediately as well as part of email.
- Helpdesk system should allow detailed multiple levels/tiers of categorization on the type of security incident being logged.
- It should provide classification to differentiate the criticality of the security incident via the priority levels, severity levels and impact levels.
- It should allow SLA to be associated with a ticket based on priority, severity, incident type, requestor, asset, location or group individually as well as collectively.
- It should maintain the SLA for each item/service. The system should be able to generate report on the SLA violation or regular SLA compliance levels.
- It should be possible to sort requests based on how close are the requests to violate their defined SLA's.
- It should support multiple time zones and work shifts for SLA & automatic ticket assignment.
- It should allow the helpdesk administrator to define escalation policy, with multiple levels & notification, through easy to use window GUI / console.
- System should provide a knowledge base to store history of useful incident resolution.
- It should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.
- The web-based knowledge tool would allow users to access his / her knowledge article for quick references.
- It should provide functionality to add / remove a knowledge base solution based on prior approval from the concerned authorities
- Provide seamless integration to generate events/incident automatically from NMS / EMS.
- Each incident could be able to associate multiple activity logs entries manually or automatically events / incidents from other security tools or EMS / NMS.
- Allow categorization on the type of incident being logged.
- Provide audit logs and reports to track the updating of each incident ticket.
- Proposed incident tracking system would be ITIL compliant.

- It should be possible to do any customizations or policy updates in flash with zero or very minimal coding or down time.
- It should integrate with Enterprise Management System event management and support automatic problem registration, based on predefined policies.
- It should be able to log and escalate user interactions and requests.
- It should support tracking of SLA (service level agreements) for call requests within the help desk through service types.
- It should be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and should support notification and escalation over email, web etc.
- It should provide status of registered calls to end-users over email and through web.
- The solution should provide web based administration so that the same can be performed from anywhere.
- It should have a customized Management Dashboard for senior executives with live reports from helpdesk database.

NOTE: EMS tools deployed shall have the ability to manage the entire IT infrastructure proposed by the SI

2. Web Server (Container to execute the presentation logic)

- The web server should be capable of supporting clustering.
- All components of the web server should be based on standards and selected such as to provide ease of management and to avoid compatibility issues
- All web server components must be maintainable with an ease such that corrective and preventive maintenance can be performed on the system without affecting the entire working of system.
- All the web server components must be capable of being managed from a remote management station and provide information on performance parameters

3. Application Server

- Application Server should be fully standards compliant providing support for Web Services, SOAP, WSDL, UDDI, LDAP v3, SSL v3, XML 1.0 and equivalent standards
- Provide comprehensive XML support compliant with the W3C XML standards and contain the basic building blocks to XML-enable applications -including reading, manipulating, transforming and viewing XML documents
- Support developing, publishing and consuming web services
- Support wireless enabled web sites and portals
- The application server should be capable of supporting clustering.

- All components of the application server should be based on standards and selected such as to provide ease of management and to avoid compatibility issues
- All application server components must be maintainable with an ease such that corrective and preventive maintenance can be performed on the system without affecting the entire working of system.
- All the application server components must be capable of being managed from a remote management station and provide information on performance parameters

4. Database

- The database should address all the structured and un-structured data storage requirements of the proposed system
- The RDBMS database should have a high tolerance of failure
- The underlying database should support 24x7 high availability
- The database should provide horizontal scalability, by adding additional servers for the same database without any downtime
- The data scalability and manageability should be integral part functionality of the database.
- The database should provide enterprise class web management tools for management and maintenance of databases even from remote places
- The database should support native automated disaster recovery capability without any third party support using cost effective option of automatically synchronizing the transaction logs to disaster site, which in case of fail over the other node provides the availability of all data. This flexibility of log synchronization should be supported from Enterprise to Entry Level server edition of the database
- The database should be capable to support plug and play data transfer across platforms or operating systems
- The database should be able to support various types of content like Texts, Images, Multi-media, Spatial and XML content natively
- The database should ensure data synchronization between database servers on near real-time basis by capturing messages at the source database, stage messages in a queue, propagate messages from one queue at the source to another queue at the target and consuming messages
- The database should support both way data synchronization across database servers in one-to-many and many-to-one situations and automatically detect data conflicts and resolve the same as per predefined conflict resolution algorithms
- The database should support data synchronization across database servers in heterogeneous platforms
- The database should be capable to deploy fine-grained access control, separation and segregation of duties and native encryption capabilities. The database should also prevent access to sensitive application data by highly privileged users.

- The database should control access to the applications, databases and data with flexible security controls.
- The solution should provide options or utility to encrypt/decrypt sensitive data
- The solution should support data export and import facility to variety of databases and other software packages
- The solution should provide backup (hot & cold) and recovery facility
- The solution should be able to schedule a backup/restore task
- The solution should be compatible with 3rd party system monitoring package.
- The solution should support selective encryption of the stored data
- The database should support a single unified data model hosted on a single database.
- The database design & architecture should be in line with the functional and non-functional requirements of the proposed system
- The database should be highly available with every processing node providing full view of data. This means, in case of failure of one server, each remaining server in the cluster should provide full access to all data at any point in time
- It should support clustering exploiting rapidly emerging disk storage and interconnect technologies
- It should provide automated disaster recovery solution to maintain transaction consistency, providing an option of zero data loss where required
- It should provide restrictive data access that enables different types of users to have secure, direct access to mission-critical data sharing
- It should control data access down to the row-level (row-level security) so that multiple communities of users with varying access privileges can share data within the same database
- It should provide encryption capabilities while transferring data over networks
- It should possess ability to encrypt data stored in the database at the column level
- It should provide Public Key Infrastructure (PKI) support
- It should provide support for comprehensive auditing for ‘inserts’, ‘deletes’, ‘updates’ and ‘selects’, and quickly spot and respond to security breaches
- It should store XML content native to database
- It should have the ability to index, search, and analyze text and documents stored in database
- It should support different partitioning schemes to split large volumes of data into separate pieces or 'partitions' which can be managed independently
- A centrally Monitored Based GUI Administration Tool should be available with the RDBMS to Create, Delete & Manipulate different Database Objects and also Schedule Queries priorities centrally.
- Server Configuration Tools be available to automatically configure clients, network etc.
- Database should have received the security certification (EAL) such as International Common Criteria for Information Technology Security Evaluation or equivalent.

- Database should support industry standard TPC benchmark or Equivalent.
- The database software should provide the following capabilities:
    a. Advanced Web Based Reporting Services
    b. Data warehousing and Analysis Services
    c. Business Intelligence
    d. Complete ETL functionality
    e. Performance Management Tools
    f. Clustering Tools
    g. Tuning and Diagnostics Tools
    h. Spatial Database Capabilities
    i. Database Compression and Encryption Tools
    j. Replication Technologies for Failover to Remote Sites.

All the above functionalities should support scalable and high available functionality.

- DBMS ETL Tool Capabilities:
    a. ETL Should support Import and Export Wizard and supporting connections, source and destination adapters, and tasks
    b. ETL Should support performing persistent lookups, Data Profiling; Should support fuzzy lookups and fuzzy search
    c. The ETL tool should provide for integrating data from various relational or non-relational sources. The tool should provide native access interface to the following PC Files – Spreadsheets, Flat Files, DBF, etc..
    d. The ETL tool should be rich in the set of in-built transformations and functions. The tool should provide at least 50 in-built transformation functions.
    e. Should support Central Management of Replications, Fine grained scheduling of data replication, Scale out of replication architecture, Capability for both Push and Pull Replications
- DBMS Reporting capabilities like :
    a. Should provide facilities to Create, Design, Generate & manage the reports.
    b. Should support Visualization tools such as maps, gauges, and charts
    c. Should support for remote and non-relational data sources
    d. Should have centralized reporting functionality that gives users a single place for locating the latest reports, spreadsheets, or key performance indicators.
    e. Should Provide Reporting which can be published through a variety of mediums like web application, client application, mail, ftp folder, mobile handhelds etc. Should support multiple formats like html, PDF, XML, CSV, etc. and other custom formats as out of the box.
    f. Should provide customization features for reporting where user can filter on various parameters to be reported on the screen.
    g. Should allow administrators to create reporting boundaries (without programming) using which adhoc reporting can be done by end users.

h. Should allow Creation of filters to control data displayed on a report. And allow Parameters passing to the reports at run- time.

i. Should provide Offline viewing of previously created Reporting results.

5. Server Load Balancer

- 10/100/1000Mbps Ethernet Ports – minimum 2 ports upgradeable to 4 ports
- Memory: Minimum 1 GB
- Minimum of 2 Gbps throughput
- Minimum of 1 Gbps SSL throughput
- Minimum of 4000 SSL connections scalable to 7500 SSL connections
- Server Load Balancing Mechanism
    - Cyclic, Hash, Least numbers of users
    - Weighted Cyclic, Least Amount of Traffic
    - NT Algorithm / Private Algorithm / Customizable Algorithm / Response Time
- Redundancy Features
    - Supports Active-Active and Active-Standby Redundancy
    - Segmentation / Virtualization support along with resource allocation
- Server Load Balancing Features
    - Server and Client process coexist
    - UDP Stateless
    - Service Failover
    - Backup/Overflow
    - Direct Server Return
    - Client NAT
    - Port Multiplexing-Virtual Ports to Real Ports Mapping
    - DNS Load Balancing
- Load Balancing Applications
    - Application/ Web Server, MMS, RTSP, Streaming Media
    - DNS, FTP- ACTIVE & PASSIVE, REXEC, RSH,
    - LDAP, RADIUS
- Content Intelligent SLB
- HTTP Header Super Farm
- URL-Based SLB
- SLB should support below Management options
    - Secure Web Based Management
    - SSH
    - TELNET

- SNMP v1, 2, 3 Based GUI
- Command Line

6. Link Load Balancer (may be proposed if State/UT has to build own DC in case SDC's are not operational)

- 10/100/1000Mbps Ethernet Ports – minimum 2 ports upgradeable to 4 ports
- Memory: Minimum 1 GB
- Minimum of 2 Gbps throughput
- Minimum of 1 Gbps SSL throughput
- Minimum of 4000 SSL connections scalable to 7500 SSL connections
- Server Load Balancing Mechanism
  - Cyclic, Hash, Least numbers of users
  - Weighted Cyclic, Least Amount of Traffic
  - NT Algorithm / Private Algorithm / Customizable Algorithm / Response Time
- Redundancy Features
  - Supports Active-Active and Active-Standby Redundancy
  - Segmentation / Virtualization support along with resource allocation
- Link Load Balancer should support below Management options
  - Secure Web Based Management
  - SSH
  - TELNET
  - SNMP v1, 2, 3 Based GUI
  - Command Line

7. Production CAS (State) Application Services related servers (Web, Portal, Application, Database, Directory, etc…)

Blade Chassis Specification

- Single blade chassis should accommodate minimum 6 (Quad core Processor) / 8 (Dual core Processor) or higher hot pluggable blades.
- Processor should be latest series/generation for the server model being quoted
- 6U to 12U Rack-mountable
- Dual network connectivity for each blade server for redundancy should be provided. Backplane should be completely passive device. If it is active, dual backplane should be provided for redundancy
- Should accommodate Intel, AMD, RISC / EPIC Processor based Blade Servers for future applications
- Should have the capability for installing industry standard flavours of Windows, Linux, Unix, Solaris for x86 Operating Environments
- Single console for all blades in the enclosure or KVM Module

- DVD ROM can be internal or external, which can be shared by all the blades allowing remote installation of S/W and OS
- Minimum 2 external USB connections functionality
- Two hot-plug, redundant 1Gbps Ethernet module with minimum 10 ports (cumulative), which enable connectivity to Ethernet via switch. Switch should be (Internal/external) having Layer 3 functionality - routing, filtering, traffic queuing etc
- Two hot-plugs, redundant 4 Gbps Fiber Channel for connectivity to the external Fiber channel Switch and ultimately to the storage device.
- Power Supplies
    - Hot Swap redundant power supplies to be provided
    - Power supplies should have N+N. All Power Supplies modules should be populated in the chassis
- Hot Swappable and redundant Cooling Unit
- Management
    - Systems Management and deployment tools to aid in Blade Server configuration and OS deployment,
    - Remote management capabilities through internet browser
    - It should provide Secure Sockets Layer (SSL) 128 bit encryption and Secure Shell (SSH) Version 2 and support VPN for secure access over internet.
    - Ability to measure power historically for servers or group of servers for optimum power usage
    - Blade enclosure should have provision to connect to display console / central console for local management like trouble shooting, configuration, system status / health display
- Built in KVM switch or Virtual KVM feature over IP.
- Dedicated management network port should have separate path for management
- Support heterogeneous environment: AMD, Xeon and RISC/EPIC CPU blades must be in same chassis with scope to run Win2003/2008 Server, Red Hat Linux / 64 Bit UNIX, Suse Linux / 64 Bit UNIX / Solaris x86

Blade Servers (Web, Portal, Application, Directory, etc…)

- Blade can be half / full height with I/O connectivity to backplane
- 2 Quad core @ 2.0 GHz or above with 4 MB shared L2 cache, 1066 MHz / 2000 MT/s FSB
- Processor should be latest series/generation for the server model being quoted
- Min 32 GB FBD RAM with min 8 Nos. free slots for future expandability.
- Minimum Memory: 32 GB scalable to 128 GB per blade

- The Blade should have redundant 4 Gbps Fiber Channel HBA (only for database server)
- 2 X (1000BASE-T) Tx Gigabit LAN ports with TCP / IP offload engine support / dedicated chipset for network I/O on blade server
- 2 X 146GB HDD or more hot swappable system disk with mirroring using integrated RAID 0,1 on internal disks, or min.16 GB compact flash card to be provided. It should be possible to hot swap the drives without shutting down the server.
- VGA / Graphics Port / Controller
- Should support heterogeneous OS platforms

Blade Servers for Infrastructure Services (EMS, Backup, DNS, Antivirus, etc…)

- Blade can be half / full height with I/O connectivity to backplane
- 2 Quad core @ 2.0 GHz or above with 4 MB shared L2 cache, 1066 MHz / 2000 MT/s FSB
- Processor should be latest series/generation for the server model being quoted
- Min 16 GB FBD RAM with min 8 Nos. free slots for future expandability.
- Minimum Memory: 16 GB scalable to 128 GB per blade
- The Blade should have redundant 4 Gbps Fiber Channel HBA
- 2 X (1000BASE-T) Tx Gigabit LAN ports with TCP / IP offload engine support / dedicated chipset for network I/O on blade server
- 2 X 146GB HDD or more hot swappable system disk with mirroring using integrated RAID 0,1 on internal disks, or min.16 GB compact flash card to be provided. It should be possible to hot swap the drives without shutting down the server.
- VGA / Graphics Port / Controller
- Should support heterogeneous OS platforms

Database Server

- Minimum 4x Quad core processor with 2.1GHz or above with 1066Mhz FSB / 2000 MT /s expandable to 4 physical processor with min 4 MB L3 cache per processor
- Processor should be latest series/generation for the server model being quoted
- OS support: Microsoft® Windows Server 2003 / 2008, Enterprise Edition / Red Hat® Enterprise Linux 5 & 4 AP / SUSE® Linux Enterprise Server 9 / Solaris for x86
- Memory (RAM): Min. 64 GB scalable to 256 GB
- RAID controller with RAID 0/1/5 with 256 MB cache
- HDD hot pluggable: 4 x 146 GB 2.5” 10 K RPM HDD or more

- Disk bays: Support for min 8 small form factor hot plug SAS / SCSI hard drives in disk drive carriers that slides out from front
- Atleast 4 x 10/100/1000 Mbps Ethernet ports or more
- 2 x 4 Gbps Fiber Channel Ports
- Ports Rear: Two USB ports (Ver 2.0); RJ-45 Ethernet; keyboard and mouse; no parallel port Front: One USB (Ver 2.0)
- Graphics controller: SVGA / PCI bus / ATI® ES 1000 / min 16MB SDRAM std/max / 1280x1024 at 16M colors
- Optical / diskette: 8X / 24X slim-line DVD ROM drive shared across chassis
- Security: Power-on password / admin password / unattended boot / selectable boot / boot without keyboard
- Power supplies: Hot plug redundant AC power supply
- Management feature to identify failed components even when server is switched off.
- Rack Mountable
- It should provide Secure Sockets Layer (SSL) 128 bit
- Encryption and Secure Shell (SSH) Version 2 and support VPN for secure access over internet.
- Should be able to manage systems through a web-browser.

8. Storage and Backup Solution

SAN Switches

- Minimum 16 Active ports (each with minimum port speed 4 GB) within same switch upgradeable to 32 ports with minimum 2 Nos. of additional 10 Gbps FC ports
- All cable of length of 10 meter each and accessories for connecting Servers /Devices to SAN.
- Should have capability of ISL trunking of minimum 8 ports.
- Should support multiple OS.
- Non disruptive subsystem maintenance.
- Should have dual Fans and Hot plug power supplies switching and service modules.
- Should have web based management software for administration and configuration.
- Non disruptive microcode / firmware upgrades and hot code activation.
- Switch shall support in built diagnostics, power on self test, command level diagnostics, online and offline diagnostics.
- Should support hardware ACL based Port security, Port Zoning and LUN Zoning
- Should support Secure Shell (SSH) encryption to provide additional security for Telnet sessions to the switch.

- Should support multilevel security on console access prevent unauthorized users from altering the switch configuration
- Should support Fibre Channel trace route and Fibre Channel Ping for ease of troubleshooting and fault isolation
- Should support the following diagnostics:
    - Online Diagnostics
    - Internal Loopbacks
    - FC Debug
    - Syslog
    - Online system health
    - Power on self test (POST) diagnostics
- Should support Applications for device management and full fabric management. The management software shall be able to perform following:
    - Fabric View
    - Summary View
    - Physical View
    - Discovery and Topology Mapping
    - Network Diagnostics
    - Monitoring and Alerts

Storage Area Network

- **SAN controller**
    - Dual Active Active Controller
- **Cache**
    - 8 GB Total Mirrored Cache for Disk IO Operations scalable to min 16 GB
- **Host interface**
    - 4 host ports per controller, Fibre Channel (FC),4 Gbps per port
- **Drive interface**
    - 4 drive ports per controller—Fibre Channel (FC) Switched or FC Arbitrated Loop (FC-AL) standard per controller, 4 Gbps per port
- **RAID levels Supported**
    - 0, 1, 5 / 6
- **Fans and power supplies**
    - Dual redundant, hot-swappable
- **SAN support**
    - Box should be compatible of SAN environment
- **SAN specifications shall have the following**

- The storage array shall be configured with at least 8 GB cache scalable to min 16 GB mirrored across two storage controllers for disk I/O operations.
- Storage subsystem shall support 146GB, 300GB 15K RPM disks and 400GB or higher 10 K RPM Fiber channel drives & 750GB, 1TB SATA or higher SATA / equivalent drives in the same device array
- Presently, the storage sub system shall be configured with 300 GB of Performance drives and 750 GB or higher on SATA / equivalent for archiving purpose.
- The storage system must provide upgrade path to larger or future array controller and software technology while maintaining the existing investment.
- The storage array proposed should have an upgrade path from the earlier generation product to the current generation product.
- All the necessary software to configure and manage the storage space, RAID configuration, logical drives allocation, virtualization, snapshots (including snap clones and snap mirrors) for entire capacity etc.
- Redundant power supplies, batteries and cooling fans and data path and storage controller.
- Load balancing must be controlled by system management software tools.
- The multi-path software should not only support the supplied storage and operating systems but should also support heterogeneous storage and operating systems from different OEMs.
- The storage array must have complete cache protection mechanism either by de-staging data or providing complete cache data protection with battery backup for up to 72 hours or more.
- The storage system should be scalable from 30 …. to …. TB of raw capacity using 40% on Fiber Channel drives and 60% on SATA / equivalent drives using the same configuration as Quoted in this tender". The Storage should have at least 2ports of 4 Gbps Frontend ports and 2 no's of back end ports of 4Gbps"The storage array must have the capability to do array based remote replication using FCIP or IP technology.
- The storage array should support block level Synchronous and Asynchronous replication across heterogeneous storage arrays from different OEMs.
- The storage array should support Operating System Platforms & Clustering including: Windows Server 2003 (Enterprise Edition), Sun Solaris, HP-UX, IBM-AIX, Linux / Solaris for x86.
- Storage should support non-disruptive online firmware upgrade for both Controllers and disk drives.
- The storage array should support hardware based data replication at the Block level across all models of the offered family.
- The storage should provide automatic rerouting of I/O traffic from the host in case of primary path failure.

- Should provision for LUN masking, fiber zoning and SAN security (as disk based encryption.
- Should support storage virtualization, i.e. Easy logical drive expansion.
- Should support hot-swappable physical drive raid array expansion with the addition of extra hard disks
- The storage system should be scalable from …TB to … TB of raw capacity using 40% on Fiber Channel drives and 60% on SATA / equivalent drives using the same configuration
- Should be able to support clustered and individual servers at the same time.
- Should be able to take "snapshots" of the stored data to another logical drive on a different Disk/RAID Group for backup purposes
- Should be configured with "snapshots and clone"
- Vendor should also offer storage performance monitoring and management software.
- The vendor must provide the functionality of proactive monitoring of Disk drive and Storage system for all possible hard or soft disk failure

Tape Library

Tape drives

- Minimum 2 latest generation LTO drives. The State can size for more as per theit requirements.

Interface

- Fiber Channel Interface

Other Specifications

- Should have sufficient speed backup to Tape Library in High Availability for backing up data from the SAN without any user intervention.
- Should be able to backup 50% of the entire production landscape in 8 hours window.
- Should support latest generation LTO drives or latest technology based library with at least 2 latest generation LTO drives tape drives (>=4), rack mountable with redundant power supplies.
- Cartridges should have physical capacity up to 1600 GB per cartridge compressed; 800 GB native.
- At least 50 latest generation LTO drive Media Cartridges with 5 Cleaning Cartridges, Barcode labels shall also be provided

Backup Software

- The proposed Backup Solution should be available on various OS platforms such as Windows and UNIX platforms and be capable of supporting SAN based backup / restore from various platforms including UNIX, Linux, and Windows etc.

- Centralized, web-based administration with a single view of all back up servers within the enterprise. Single console must be able to manage de-duplicated and traditional backups.
- The proposed backup solution should allow creating tape clone facility after the backup process.
- The proposed Backup Solution has in-built frequency and calendar based scheduling system.
- The proposed backup Solution supports the capability to write multiple data streams to a single tape device or multiple tape devices in parallel from multiple clients to leverage the throughput of the Drives using Multiplexing technology.
- The proposed backup solution support de-multiplexing of data cartridge to another set of cartridge for selective set of data for faster restores operation to client/servers
- The proposed backup solution should be capable of taking back up of SAN environment as well as LAN based backup.
- The proposed backup solution shall be offered with 4 Nos. UNIX based licenses, 26 Nos. Windows based licenses and the rest 20 Nos. LINUX based licenses for both SAN based backup and the LAN based backup.
- The proposed solution also supports advanced Disk staging.
- The proposed Backup Solution has in-built media management and supports cross platform Device & Media sharing in SAN environment. It provides a centralized scratched pool thus ensuring backups never fail for media.
- Backup Software is able to rebuild the Backup Database/Catalog from tapes in the event of catalog loss/corruption.
- The proposed Backup Software should offer online backup for all the Operating Systems i.e. UNIX, Windows & Linux etc
- The proposed Backup Solution has online backup solution for different type of Databases such as Oracle, MS SQL, and Sybase / DB2 etc. on various OS.
- The Proposed backup solution shall provide granularity of single file restore.
- The Proposed backup solution shall be designed in such a fashion so that every client / server in a SAN can share the robotic tape library.
- Backup Solution shall be able to copy data across firewall.
- The backup software must also be capable of reorganizing the data onto tapes within the library by migrating data from one set of tapes into another, so that the space available is utilized to the maximum. The software must be capable of setting this utilization threshold for tapes
- The backup software should be able to support versioning and should be applicable to individual backed up object's
- Should have the ability to retroactively update changes to data management policies that will then be applied to the data that is already being backed up or archived

- All software licenses should be in the name of Haryana Police and should be full use perpetual license, i.e. the software license should not expire after the contract period. The software Licenses should be comprehensive and no further licenses should be required for DC/DR operations. The software installed should necessarily be the latest version at the time of actual implementation.

FC-IP Router

Fibre Channel Ports

- min 4 FC ports

FC Port Speed

- Autosensing 1/2/4 Gb/s

iSCSI (Ethernet) Ports

- min 8 Ethernet ports

iSCSI (Ethernet) Port Speed

- 1 Gigabit Ethernet

Aggregate Bandwidth

- min 125 MB/s

Protocol Support

- FCP
- iSCSI

High-Availability Features

- Two-way active/active clustering with failover and failback capabilities
- Multiple iSCSI connections provide multipathing support from a single gateway to as many as 100 servers.

Management Features

- CLI (by Telnet, SSH, or console)

iSCSI Gateway Manager

- SNMP
- Allows for monitoring traffic statistics on each storage and network interface, fan and temperature and iSCSI session details.

9. Networking Equipments (for SDC/ DR/ all Other Police Locations)

A. Router

a) General Architecture:

(i) High speed CPU
(ii) Rack mountable configuration
(iii) Health LED for all modules to indicate status

b) Router Port Requirements:

(i) 10/100 Mbps Ethernet- 2 Nos
(ii) WAN Ports E1- 2 Nos

(iii) Packet Forwarding Speed- Minimum 60 Kbps

c) Router Features:

(i) Support for router redundancy protocol
(ii) Router software must have on line reconfiguration facilities
(iii) High MTBF
(iv) Capable of booting from a remote system where router image is present
(v) Support for standard routing protocols like OSPF, RIP & BGP
(vi) Flash min 128 MB
(vii) Minimum of 256 MB RAM
(viii) Configurationally changes should be done without rebooting the router or modules
(ix) Stateful firewall functionality and IDS.

d) Software features:

Following standard IP routing protocols:

(i) Static
(ii) RIP, OSPF
(iii) OSPF Over Demand Circuits
(iv) Policy Routing
(v) IP Version 6 Support
(vi) Support for IPSec & 3DES through a simple software upgrade as and when required.

Following WAN protocols:

(i) PPP
(ii) Multilink PPP
(iii) Compression-Payload and TCP/IP Header

Following Multicasting and Quality of Service (QoS):

(i) Resource Reservation Protocol (RSVP) as per RFP 2205 and Internet Group Management Protocol Version 2 (IGMPv2) as per RFC 2236.
(ii) Support for IP Precedence, Committed Access Rate (CAR),
(iii) DiffServ QoS
(iv) The router shall support Application recognition and it should be possible to frame policies based on the applications.

e) Security Features:

(i) Support DES / 3 DES / AES
(ii) PPP PAP or CHAP support.
(iii) VPN support
(iv) Time based Access Lists
(v) Multiple Privilege Levels.
(vi) Support for RADIUS or AAA.

f) Power: 230 V AC, 50 Hz

B. Switch:

(i) Layer 2 switch
(ii) 24 No 10/100 ports
(iii) 2 Nos. 10/100/1000

(iv) Nonblocking architecture
(v) 8 Gbps switching fabric and 6 Mpps forwarding rate
(vi) Support IGMP Snooping with Broadcast Control IGMP v3.
(vii) Support for minimum 8000 MAC addresses.
(viii) Ethernet, Fast Ethernet support
(ix) Spanning tree/Rapid Spanning Tree support
(x) Per VLAN Spanning Tree
(xi) Support for dynamic VLAN Registration
(xii) Dynamic Trunking Protocol or equivalent.
(xiii) VLAN Trunking Protocol or equivalent
(xiv) Traffic classification should be based on user-definable application types: TOS, DSCP, Port based, Mac address, IP address, TCP/UDP port number
(xv) Multicast filtering per port should be supported
(xvi) Support SNMP upto ver.3
(xvii) Prioritization support
(xviii) Minimum 250 vlans
(xix) SNMP and Telnet support
(xx) Web-based and CLI management
(xxi) Four RMON groups (1,2,3&9)
(xxii) Additional features: Advanced QoS, Rate limiting
(xxiii) L3 Features : Static routes & RIP
(xxiv) Mounting: 19" Rack mountable
(xxv) Source power supply: 230 V AC Single phase 50Hz

B. Minimum Technical Specifications Requirement at Police Units

1. Desktops

a. Client Systems

High End Client Systems - all Police Units/ Offices	
Minimum Technical Specifications for Desktop PC	
	Processor: Intel Core i5-650 processor (3.20 GHz) with Q57 Chipset or higher
	Cache: 6 MB
	Memory Type: 4 GB DDR-III @ 1066 MHZ or higher
	Memory Slot: 4 DIMM Slots
	Internal Hard Disk/Speed: 320 GB SATA (7200 RPM) or higher
	Optical Drive: SATA SuperMulti LightScribe DVD Writer Drive
	Display size: 18.5 inch (measured diagonally)
	Graphics Controller: Intel Graphics Media Accelerator 4500 integrated graphics
	Form Factor: Convertible Minitower

	External I/O ports: Rear: 6 USB 2.0, 1 standard serial port, 1 optional serial port, 1 optional parallel port, 2 PS/2, 1 RJ-45, 1 VGA, 1 Display Port, audio in/out; Front: 2 USB 2.0, headphone and microphone
	Expansion slots: 3 full-height PCI, 1 full-height PCI Express x1, 2 full-height PCI Express x16
	Network interface: Integrated Intel 82567LM Gigabit Network Connection
	Power requirements: Input voltage 90 – 264 / 100 – 240 VAC, 50/60 Hz, 47 – 63 Hz, active PFC (85% High Efficiency)
	Management: Desktop Management Tool
	Bilingual Keyboard: PS/2 or USB Standard Keyboard
	Pointing device: USB 2-Button Optical Scroll Mouse
	Security management: TPM 1.2 TPM Security Chip (except for Russia), TPM Pre-Boot Authentication (via BIOS), Smartcard Pre-boot Authentication (via BIOS), Stringent Security (via BIOS), SATA port disablement (via BIOS), HP ProtectTools Embedded Security Software, Serial, Parallel, USB Enable/Disable (via BIOS), Removable Media Write/Boot Control, Power-On Password (via BIOS), Setup Password (via BIOS)
	Warranty: 3 Years Part, 3 Years Labour, 3 Years On-Site

2. Multi-Function Laser (Print/ Scan/ Copy)

Multifunction Laser Printer LAN 3 in 1 Printer (Black & White)	
Minimum Technical Specifications for Multi-Function Laser Printer	
Printer	High-speed printing, Black-and-white: up to 35ppm (draft); up to 15ppm,Duty Cycle: Up to 15,000 pages per month Automatic two-sided printing,250-sheet input tray, Print, scan and copy unattended with the Automatic Document feeder, enhanced print permanence, Capable of installation, configuring, monitoring and troubleshooting in the network, from anywhere on the network
Scanner	Flatbed with automatic document feed, upto 4800 dpi; Enhanced upto 19200 dpi; Scan size maximum (flatbed): 215.9 x 297 mm (8.5 x11.7 inches), front panel scan (scan to application.
Copier	Black-white colour-Upto 1200x600 dpi, Copy speed (black, draft quality, A4):Up to 35 cpm, Copy resolution (black graphics): Up to 1200 x 600 dpi, Copier resize: 25 to 400%, Maximum number of copies: Up to 99, Copier smart software features: Up to 99 multiple copies, reduce/enlarge from 25 to 400%, 2-up or 4-up allowing 2 or 4 pages to be

	copied onto 1 page, contrast (lighter/darker), resolution (copy quality), tray select, collate, margin, shift

3. SNMP based UPS

SNMP Based UPS - all Police Units/ Offices	
Minimum Technical Specifications for UPS	
1.	ISO 9001 certified brand
2.	True On Line Type
3.	Backup period should be atleast 2 Hr with minimum 3000 VAH for 3 KVA
4.	IGBT with High Frequency PWM (Pulse with Modulation) Technology
5.	Output wave form should be Sine wave
6.	Compatible with local Electricity Power Generator.
7.	Total Harmonic Distortion should be less than 3%.
8.	Support input voltage range of 160 V to 270 V.
9.	Output Voltage should be 230 Volt AC (+/- 1%)
10.	Output frequency should be 50 Hz +/- 0.05 Hz (Crystal Controlled)
11.	Closed housing for batteries with suitable stand.
12.	Inherent protection should be provided for over loading, low battery, over temperature, short circuits, over and under input voltage.
13.	LED indicators should be provided for at least load indication, load on battery, low battery, overload, Mains ON.
14.	Audible indicator should be provided for at least load on battery, low battery, Mains failure, Overload

4. 2 KVA Generator Set

2KVA Generator Set - all Police Units/ Offices		
Minimum Technical Specifications for DG Set		
1.	The proposed DG set should be able to support the Police Unit equipments along with AC, in absence of primary power source. Engine shall be vertical multi cylinder 4 stroke type in accordance with IS 10002-1981 with latest amendments.	
	Type	Multi cylinder
	Method of starting	Electric start 12 V DC
	Type of cooling	Water cooled /Air cooled
	Type of governor	Mechanical/Electronic
	Type of fuel	High speed diesel
	Rating	Continuous
	Output alternator	Suitable HP rated to match the
	Rated speed	1500 RPM
	Over load capacity	10% overload – minimum 1 hour

	50% overload – minimum 1 minute
2.	**Accessories** ♦ Flywheel to suitable diameter and fuel injection equipment ♦ Air cleaner ♦ Lubricating oil cooler ♦ Electric motor starting equipment like motor, battery, charging generator with voltage regulator etc. ♦ Heavy duty radiator with fan ♦ Residential type silencer with exhaust piping with vibration isolator ♦ Fuel tank suitable for 8 Hrs of continuous running with necessary piping and fuel gauge, drain valve, inlet and outlet connections. ♦ Anti vibration mounting pads (Dunlop) ♦ Speed controlling governor ♦ Suitable coupling system to the Alternator ♦ Tachometer ♦ Lubricating oil pressure gauge ♦ Hour meter to indicate number of Hrs of operation ♦ Auto trip on low oil pressure ♦ Over speed alarm with trip ♦ Thermal insulation for exhaust line with glass wool, Aluminium sheet, chicken mesh, Diesel line 12 mm dia including beads flanger etc ♦ Battery 12 V with lead and terminal ♦ Battery charger. ♦ Protection: Protection against low lubricating oil pressure, high water temperature and over speed shall be provided for engine with alarm and fuel shut off.

5. Finger Print Reader

Finger Print Reader - all Police Stations	
Minimum Technical Specifications for Finger Print Reader	
Fingerprint Sensor	▪ Scanner: Optical sensor ▪ Resolution: 500 dpi at 256-bit (416 X 416 pixels) ▪ Platen Area: 0.83 in x 0.83 in (21 mm x 21 mm) ▪ Distortion: <1%
Biometric Matching	▪ Authentication: <1 second (including detection, encoding and matching) ▪ Identification: <2 seconds in 1:3000 mode (including detection, encoding and matching) ▪ False Acceptance Ratio (FAR): 1 in 10,000 or better, configurable based on security specifications
Interfaces	▪ Standard USB
Environment	▪ Temperature: 0° C to 50° C ▪ ESD Protection: 15 KV
Format Supported	▪ AANSI/ INCITS 378, ▪ ISO 19794-2

6. Digital Pen

Digital Pen- all Police Stations
Minimum Technical Specifications for Digital Pen

Average battery life	Min. 2.5 hours continuous writing use
Average usage life	150,000 hours
Approximate battery recharge time	2 hours
Battery type	Lithium-ion polymer rechargeable battery
Standard connectivity	USB 1.1 (also called High Speed USB 2.0)
Humidity non-operating	0 to 95% RH (excluding rain, non-operating)
Humidity range	0 to 95% RH (excluding rain)
Humiditiy recommended operating range	0 to 90% RH (non-condensing, operating)
Operating temperature maximum	104°F
Operating temperature recommended range	32 to 104°F
Storage temperature range	-4 to 104°F
Storage life	Up to 5 years
Image compression	Pattern images to X, Y coordinate samples with relative time of capture
Image processing rate	75 Hz
Image resolution	Atleast 500 dpi
Image scaling	Perspective, rotation, tilt, and error correction
Languages supported	English and Hindi
Internal fixed memory	Atleast 10 MB (1.3 MB available for user strokes)

7. Digital Camera

Digital Camera - all Police Stations
Minimum Technical Specifications for Digital Camera

Basic Features	▪ Atleast 14 Mega Pixels ▪ Sensor Type 1/2.3 Super HAD CCD ▪ Optical Zoom: 4x ▪ Precision Digital Zoom: 8x ▪ Lens: Carl Zeiss Vario-Tessar or equivalent ▪ F Number 2.7 - 5.7 ▪ Auto Focus Range (W: Approx. 4cm to Infinity, T: Approx. 60cm to Infinity) ▪ Compatible Recording Media Memory Stick Duo / Memory Stick PRO Duo / Memory Stick PRO Duo (High Speed) / Memory Stick PRO-HG Duo / SD Memory Card / SDHC Memory Card ▪ LCD: 2.7 (6.9 cm) (230K pixels), Clear Photo LCD ▪ Battery Life: 240 shots or 120mins ▪ Battery System: Lithium ION Battery ▪ USB 2.0 Hi-Speed
Main Features	▪ Photo Mode Intelligent Auto, Easy Shooting, Program Auto, Steady Shot ▪ Scene Selection Twilight / Twilight Portrait / Landscape / Soft Snap / Snow / Beach / High Sensitivity / Underwater / Gourmet / Pet ▪ Still Image Size 14M 4,320 x 3,240 ▪ Still Image Size 16:9 Mode 11M(4,320 x 2,432) / 2M(1,920 x 1,080) ▪ Movie Recording Mode (QVGA) 320 x 240, 29.97fps ▪ Movie Recording Mode (VGA) 640 x 480, 29.97fps ▪ Movie Recording Time Up to 2GB per shoot ▪ Recording Format Motion JPEG / AVI ▪ Still Image Recording Mode Normal (JPEG) / Burst (JPEG) ▪ ISO Sensitivity Setting Auto / 80 / 100 / 200 / 400 / 800 / 1600 / 3200 ▪ Image Stabilizer Steady Shot ▪ Focus Mode Multi-point AF (9 points) / Center-weighted AF / Spot AF ▪ Auto Focus Mode Intelligent ▪ Exposure Compensation Plus / Minus 2.0EV, 1 / 3EV step ▪ White Balance Auto / Daylight / Cloudy / Fluorescent / Incandescent / Flash ▪ Underwater White Balance Auto / Underwater 1-2 ▪ Light Metering Multi-Pattern / Center Weighted / Spot ▪ Flash Mode Auto, Flash On, Flash Off, Slow Synchro ▪ Flash Range ISO Auto: Approx. 0.3 - 3.5m (W) / 0.6 - 1.8m (T), ISO3200: up to Approx. 7.1m (W) / 3.7m (T) ▪ Pre-flash ▪ Auto Daylight Syncro ▪ Dynamic Range Optimiser Standard / Off / Plus ▪ Face Detection ▪ Red-eye Reduction ▪ Clear RAW NR (Noise Reduction)
User Interface	▪ Self-Timer (10sec / 2sec / off) ▪ Auto Review ▪ Index Playback ▪ Playback Moving Image Mode (QVGA / VGA) ▪ Slide Show Playback (SD) ▪ Image Rotation / Divide (MPEG) / Cue & Review ▪ Hand Shake Alert ▪ LCD Brightness Setting ▪ Speaker Volume Control ▪ Internal Memory Full Data Copy (to Memory Stick) ▪ Multi-use Terminal ▪ USB Connecting Auto / Mass Storage

5.6 Annexure – F: Roles & Responsibilities of the Parties

5.6.1 Roles and Responsibilities of System Integrator

1. Preparation of Detailed Project Plan in line with the overall plan provided in the RFP. The same should be prepared in consultation with Haryana Police or its nominated agency
2. Procure, install, commission, operate and maintain:
    a. Requisite hardware & system software at Police Units, Data Center and other locations as per the requirements mentioned in this RFP
    b. Networking equipments, connectivity and LAN as per the requirements mentioned in this RFP,
    c. Meet the defined SLAs for the performance of the system.
3. Addressing technology obsolescence by appropriate upgradation, replacement and / or replenishment of systems deployed at various locations (data center, HQ and other locations).
4. Insure the entire hardware against the infrastructure deployed at various locations for the entire duration of the contract against vandalism, theft, fire and lightening.
5. Keep all system software i.e. OS, antivirus, office applications etc., for Servers, PCs etc. at Data Centre and various locations, up to date by installing regular upgrades / patches.
6. Rectification of system software problems due to crashing or malfunctioning of the OS, RDBMS or front end within the time limits to meet the SLAs as defined in RFP Volume 1.
7. Develop / customize, deploy and maintain the requisite Software Solution as per the requirements of the Department at concerned locations.
8. Provide necessary support for the resolution of bugs, patches & upgrades of the software solution.
9. Provide necessary manpower for managing the Change Requests.
10. Design various manuals like User manual, Trouble Shooting manual etc. for the system.
11. Provide training on application modules to the staff members and stakeholders of the Department
12. Maintain the business continuity.
13. Deploy requisite manpower and infrastructure for the digitization of the existing data.
14. Deploy the required manpower to manage the operations.
15. Ensuring the SLAs for downtime of system, software development / customization, procurement and delivery of hardware & networking equipments, errors in data entry, etc. as defined in RFP Volume 1 are met.
16. Management and quality control of all services and infrastructure.
17. Any other services which is required for the successful execution of the project.
18. Regular Backup as per the schedule and Disaster Recovery.
19. Generation of MIS reports as per the requirements of Haryana Police

20. Generation of the report for the monitoring of SLAs.
21. Meet the minimum defined Technical Specifications for the IT Infrastructure including Hardware and networking equipments keeping in mind the application and future requirements of the Client

5.6.2 Roles and Responsibilities of Client i.e. Haryana Police or its nominated agency

1. Provide adequate space for setting up of infrastructure, software development and other activities to be carried out by the Bidder.
2. Coordination between all the Police Units for providing necessary information for the study and development / customization of the necessary solution.
3. Co-ordination with Hartron, Haryana SWAN operators and other state agencies to assist the selected bidder in execution of the project.
4. Coordinate with Bidder for conducting workshops for the Stakeholder departments.
5. Provide the data available in the form of physical files or existing databases to the selected bidder for digitization purposes.
6. Deployment of staff members of the Department for verification of the digitized data within the defined timelines.
7. Ensure that Data Backups are being taken regularly by bidder as per the schedule agreed upon.
8. Ensure that the hardware and other infrastructure deployed by the bidder at HQ, DC etc. meets the minimum specifications as mentioned in RFP and is maintained properly to meet the SLAs as defined in RFP.
9. Monitoring of overall timelines, SLAs and calculation of penalties accordingly.
10. Conducting UAT for the application solution deployed.
11. Issuing the Acceptance Certificate on successful deployment of the software application, hardware deployed, digitized data and for other components of the Scope of Work (wherever required).
12. Any other requirements that could arise during operations for effective governance and to meet any administrative requirement.
13. To create internal capacity now for execution of the project after takeover from the bidder.
14. Ensuring the staff members and other stakeholders attend the training programs as per the schedule defined by the bidder and agreed upon by Client or its nominated agency
15. Provide sign off on the deliverables of the project including SRS, design documents etc. as defined in the RFP document