CRIME & CRIMINAL TRACKING NETWORK AND SYSTEMS (CCTNS)

DRAFT MODEL RFP TEMPLATE

FOR

SELECTION OF SYSTEM INTEGRATOR BY THE STATE

IMPLEMENTATION OF CCTNS

IN

<<STATE / UT>>

VOLUME – I: TECHNO-FUNCTIONAL REQUIREMENTS

This draft model RFP for selection of State/UT System Integrator is only a template to be used by the State / UT as a reference. The detailed RFP with all the contractual and legal terms shall be prepared by the State / UT utilizing the services of State Project Management Consultant (SPMC).

1. **The SPMC shall prepare this RFP based on PIM report assessment in consultation with the State/UT (State Police Department). The aim of this RFP is to seek proposals from eligible bidders for providing "Bundle of Services" for implementation of CCTNS project in the State/UT. The SPMC shall design the RFP in such a manner that the eligible bidders for selection of SI shall respond to this RFP with a comprehensive end to end solution for the implementation of CCTNS project in the State/UT through the Bundle of Services.**
2. **SPMC shall utilize this template only as a reference and shall source information for developing the RFP from the PIM report and other SPMC deliverables. SPMC shall provide tables and matrices wherever required to elicit unambiguous and objective responses from eligible bidders (Potential SIs) to respond to the RFP.**
3. **SPMC to provide tables of Bill of Materials (based on the details provided in the PIM report with suitable modifications with due approvals) for all scope elements to enable the SI to respond to the bid with specific information on various components of CCTNS project implementation.**
4. **SPMC shall consult State/UT while finalizing the scope and timelines of the project. Approvals are essential for all additional scope elements (Additional applications/modules/customization, additional police units, additional hardware/infrastructure items, etc.), from the State/UT as per MHA guidelines.**
5. **SPMC to provide overall Capacity building plan with an objective on ensuring sustainable outcomes through CCTNS project for enabling the eligible bidders to respond to the various components of Capacity building and change management in line with CB-CM framework circulated to States/UTs.**
6. **SPMC shall assess the State specific requirements as given in the PIM report for proposing any additional applications/CAS-customization and extensions. SPMC shall also provide reasonable effort estimate for the eligible bidders to respond for the same. SPMCs to consider that Application maintenance and management support for all the additional applications/CAS-customizations and extensions shall be the responsibility of SI.**
7. **The specifications of the two stacks of CAS provided in the RFP are the stacks on which CAS is being developed by SDA at the Centre. The eligible bidders shall respond to the RFP by bidding for one CAS stack for implementation of CCTNS project in the State/UT. The State/UT shall come up with a proposal mentioning the choice of the stack.**
8. **It may be noted that the scope of work specified in this RFP does not necessarily mean that it would be funded by Government of India under CCTNS scheme. The SPMC in consultation with State/UT should ensure availability of funds through various sources while proposing for items/services mentioned in this RFP and not covered under CCTNS funds.**
9. ***A draft model RFP template (Version1.0) of SI was initially circulated to all States/UTs as a reference document. The Revised version of Model RFP template (Version-2.0) after inclusion of specifications of CAS (State) was circulated to States/UTs for feedback. This document is the version 3.0 of the Model RFP template prepared after incorporation of the feedback from the States/UTs, which shall be utilized by the State/UT for preparation of RFP for selection of System Integrator. The SPMC shall prepare the RFP in consultation with the State/UT using this template as a reference. The SPMC shall add relevant information wherever necessary to make the RFP complete in all respects for seeking response from eligible bidders for selection of System integrator.***

Calendar of Events and Other Relevant Details

S. No	Information	Details
1.	RFP reference No and Date	
2	Non Refundable Tender Cost	
3	Sale of RFP Document	
4	EMD	
5.	Last date for submission of written queries for clarifications and date of pre-proposal conference	
6.	Release of response to clarifications on	
7.	Last date (deadline) for receipt of proposals in response to RFP notice	
8.	Place, Time and Date of opening of Technical proposals received in response to the RFP notice	
9.	Place, Time and Date of opening of Financial proposals received in response to the RFP notice	
10.	Contact Person for queries	
11	Addressee and Address at which proposal in response to RFP notice is to be submitted:	

LIST OF ABBREVIATIONS

Table of Contents

1 Introduction

1.1 Project Background

Availability of relevant and timely information is of utmost importance in conduct of business by Police, particularly in investigation of crime and in tracking & detection of criminals. Police organizations everywhere have been handling large amounts of information and huge volume of records pertaining to crime and criminals. Information Technology (IT) can play a very vital role in improving outcomes in the areas of Crime Investigation and Criminals Detection and other functioning of the Police organizations, by facilitating easy recording, retrieval, analysis and sharing of the pile of Information. Quick and timely information availability about different facets of Police functions to the right functionaries can bring in a sea change both in Crime & Criminals handling and related Operations, as well as administrative processes.

Creation and maintenance of databases on Crime & Criminals in digital form *for sharing by all* the stakeholders in the system is therefore very essential in order to effectively meet the challenges of Crime Control and maintenance of public order. In order to achieve this, *all the States should meet a common minimum threshold in the use of IT, especially for* ***crime & criminals*** *related functions.*

Additional information can be found on NCRB website (http://ncrb.nic.in)

1.2 Background of Police Systems in India

Several initiatives have been introduced in the past to leverage IT in police functioning. Some of these initiatives include centrally initiated programs such as the NCRB-led CCIS (Crime and Criminals Information System) and CIPA (Common Integrated Police Application), and State-led initiatives such as e-COPS (in Andhra Pradesh), Police IT (in Karnataka), Thana Tracking System (in West Bengal), CAARUS (in Tamil Nadu) and HD IITS (in Gujarat).

Presently automation in the area of Civil Police is addressed mainly through the two GOI-led initiatives – CCIS and CIPA – and in some States such as Andhra Pradesh, Karnataka and Gujarat, through State-led initiatives.

This section explores the details of such GOI-led initiatives.

<< SPMC to provide relevant information on Project background both from State/UT level and national level context>>

1.2.1 Crime and Criminals Information System (CCIS)

CCIS is an NCRB-driven program and has been launched in 1990. Since then, it has been implemented in 35 states and union territories and spans over 700 locations. Most of the State/UT police headquarters and district headquarters are covered by CCIS and so are some of the 14,000+ police stations in the country.

CCIS is primarily an initiative to create crime- and criminals-related database that can be used for crime monitoring by monitoring agencies such as National Crime Records Bureau (NCRB), State Crime Records Bureaus (SCRBx) and District Crime Records Bureaus (DCRBx) and to facilitate statistical analysis of crime and criminals related information with the States and monitoring agencies.

CCIS data is used for publishing online reports such as Missing Persons report and is also used as the basis for online query facilities that are available through the NCRB website. In addition, it is also used by NCRB to publish an annual nation-wide Crime Report. CCIS focuses exclusively in Crime and Criminals information and does not address the other aspects of Police functioning.

CCIS was originally built on Unix OS and Ingres database, but has since been ported to Windows platform and has released its last three versions on Windows (the last release having taken place in September 2002).

1.2.2 Common Integrated Police Application (CIPA)

A feature common to most of the early efforts has been a predominant focus on collection of data as required by the monitoring agencies and on specific functions such as records management, statistical analysis and office automation; rather than on police stations, which are the primary sources of crime- and criminals-related data generation.

In order to provide an application that supports police station operations and the investigation process, and that is common across all states and union territories, MHA had conceptualized the Common Integrated Police Application (CIPA) in 2004. It has been initiated as part of the “Modernization of State Police Forces (MPF)” scheme of the Ministry of Home Affairs. The aim of CIPA is to bring about computerization and automation in the functioning at the police station with a view to bringing in efficiency and transparency in various processes and functions at the police station level and improve service delivery to the citizens. So far about 2,760 police stations, out of a total of 14,000+ police stations across the country, have been covered under the Scheme.

CIPA is a *stand-alone* application developed to be installed in police stations and to support the crime investigation and prosecution functions. CIPA is a centrally managed

application: an application core centrally developed and is installed in police station. Any state-specific customizations are evaluated and made on a need basis.

The core focus of the CIPA application is the automation of police station operations. Its core functionality includes the following modules: (i) Registration Module (ii) Investigation Module (iii) Prosecution Module. There is also a Reporting module that addresses basic reporting needs.

CIPA is built on client-server architecture on a NIC Linux platform using Java and PostgreSQL database.

Benefits realized from CIPA include the ability to enter registration (FIR) details into the system and print out copies and the ability to create and manage police station registers on the system, etc.

It was felt, however, that a standalone application couldn't provide the enhanced outcomes in the areas of Crime Investigation and Criminals Detection that are necessary. And for this reason, MHA has decided to launch the Crime and Criminal Tracking Network System (CCTNS) program.

1.2.3 Crime and Criminal Tracking Network System (CCTNS)

The Crime and Criminal Tracking Network Systems* (CCTNS) was conceptualized by the Ministry of Home Affairs in detailed consultation with all stakeholders and will be implemented as a "Mission Mode Project (MMP)" and will adopt the guidelines of the National e-Governance Plan (NeGP).

CCTNS aims at 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. CCTNS will operate through the creation of a nationwide networked infrastructure for evolution of IT-enabled state-of-the-art tracking system around "investigation of crime and detection of criminals" in real time, which is a critical requirement in the context of the present day internal security scenario.

The scope of CCTNS[1] spans all 35 States and Union Territories and covers all Police Stations (14,000+ in number) and all Higher Police Offices (6,000+ in number) in the country. The CCTNS project includes vertical connectivity of police units (linking police units at various levels within the States – police stations, district police offices, state headquarters, SCRB and other police formations – and States, through state headquarters and SCRB, to NCRB at GOI level) as well as horizontal connectivity, linking police functions at State and Central level to external entities. CCTNS also provides for a

[1] Also refer NCRB website (http://ncrb.nic.in)

citizen's interface to provide basic services to citizens.

1.3 CCTNS Implementation Framework

CCTNS would be implemented in a way where the States and UTs play a major role. CCTNS would be implemented in alignment with the NeGP principle of "centralized planning and de-centralized implementation". MHA and NCRB would play a key role in planning the program in collaboration with the Police leadership within States, in the development of a few core components and in monitoring and reviewing the program. It is, however, the States and UTs that would drive the planning and implementation at the State level.

The role of the Centre (MHA and NCRB) focuses primarily around planning, providing the Core Application Software (CAS) (to be configured, customized, enhanced and deployed in States. States would drive the implementation at the state level and would continue to own the system after deployment.

The implementation of CCTNS would be taking an "integrated service delivery" approach rather than that of procurement of hardware and software.

The central feature of CCTNS implementation at the State level is the "bundling of services" concept. According to this, each States selects one System Integrator (SI) who would be the single point of contact for the State for all the components of CCTNS. These components include the application (the changes made to the core application provided by MHA), hardware, communications infrastructure, associated services such as Capacity Building and Handholding, etc.

1.3.1 Goals of this Request for Proposal (RFP)

The primary goal of this RFP is to serve as a framework or a model RFP to be released by States and UTs to select SI for their state through a competitive bidding process. This volume of RFP intends to bring out all the details with respect to solution and other requirements that are deemed necessary to share with the potential bidders. The goals of RFP are further elaborated below:

- To seek proposals from potential bidders for providing the "bundle of services" in implementing and managing the CCTNS solution in states.
- To understand from the bidders how they propose to meet the technical and operational requirements of CCTNS.
- To ascertain how potential bidders propose to deliver the services and sustain the demand and growth in the requirements.
- To ascertain from bidders on how they will ensure scalability and upgradeability of the infrastructure and solution proposed to be deployed.

- To understand from the bidders as to how they intend to innovate further on this service delivery model.

State (through CCTNS Apex Committee and Empowered Committee) shall be the final authority with respect to qualifying a bidder through this RFP. Their decision with regard to the choice of the SI who qualifies through this RFP shall be final and the State reserves the right to reject any or all the bids without assigning any reason. The State further reserves the right to negotiate with the selected agency to enhance the value through this project and to create a more amicable environment for the smooth execution of the project.

2 Project Overview

2.1 Need for the Project

The Ministry of Home Affairs has conceptualized the Crime & Criminals Tracking Network and Systems (CCTNS) project as a Mission Mode Project under the National e-Governance Plan (NeGP). This is an effort of the Government of India to modernize the police force giving top priority to citizen services, information gathering, and its dissemination among various police organizations and units across the country.

A need has been felt to adopt a holistic approach to address the requirements of the police, mainly with relation to functions in the police station and traffic management. There is also a need to strengthen the citizen interfaces with the police. Interfaces need to be built with external agencies like courts, transport authorities, hospitals, and municipal authorities etc to be able to share information between departments. Therefore, it becomes critical that information and communication technologies are made an integral part of policing in order to enhance the efficiency and effectiveness of the Police Department.

In order to realize the benefits of e-Governance fully, it is essential that a holistic approach is adopted that includes re-engineering and standardizing key functions of the police and creating a sustainable and secure mechanism for sharing critical crime information across all Police Formations. The CCTNS has been conceptualized in response to the need for establishing a comprehensive e-Governance system in police stations across the country.

2.2 Vision and Objectives of Project

The broad objectives of the project are as follows:

i. Improve Service Delivery to the Public

Citizens should be able to access police services through multiple, transparent, and easily accessible channels (Portal, Mobile, Call Centre etc.) in a citizen-friendly manner. The focus is not only to improve the current modes of the service delivery but also provide alternate modes such as internet for the public to communicate with the police.

ii. Provide Enhanced Tools for Law & Order Maintenance, Investigation, Crime Prevention, & Traffic Management

Law & Order Maintenance, Investigation, Crime Prevention, and Traffic Management are core components of policing work. Information technology can both enable and improve the effectiveness and efficiency of the core activities of the police. Police

should be provided with data amenable for easier and faster analysis in order to enable them to make better and informed decisions.

iii. Increase Operational Efficiency

Police should spend more time on the public facing functions. Information technology solutions should help in reducing the repetitive paperwork/records and making the back-office functions more efficient.

iv. Create a platform for sharing crime & criminal information across the country

There is a critical need to create a platform for sharing crime and criminal information across police stations within and between the different states in order to increase the effectiveness in dealing with criminals across the state borders.

2.3 Stakeholders of Project

The impact of the police subject being sensitive, a consultative and a bottom-up approach has to be adopted in designing the MMP impacting the following stakeholders:

- Citizens/ Citizens groups
- MHA/NCRB/Others
- State Police department
- External Departments of the State such as Jails, Courts, Passport Office, Transport Department, Hospitals etc.
- Non-Government/Private sector organizations

3 State Police Department

3.1 Organization Structure

State shall furnish the details about the organizational structure of the police department in this section to enable SI to understand the Police Department. It should at a minimum provide:

1. Reporting hierarchy under the DGP
2. Functional Units/wings within the Police Department at State Police Headquarters, a typical District Headquarters, and a typical Commissionerate (if exists in the State/UT)along with a brief description of the functional wings
3. Reporting hierarchy for the Police Stations and a brief description of each of the units

The addresses, designations and contact details of the nodal officer appointed for the CCTNS Project / Bid Management should also be given

SPMC should provide a broad level organization structure clearly showing the hierarchy and the number of organizational units of the police departments at all levels relevant to CCTNS project implementation.

3.2 Existing Legacy Systems

State shall furnish the details about the existing legacy systems that are currently in operation in the Police Department in this section to enable SI to assess the scope of integration and data migration. It should at a minimum provide:

1. Name and description of the legacy system
2. Whether this application will be migrated or continue to run and needs to be integrated with the new solution to be developed as part of this RFP.
3. System Functionality
4. Current number of users
5. Details on the architecture, technology platform of the system
6. Deployment details – Geographical reach, Number of Police stations covered
7. Current data available in the system and whether the data can be used during data migration
8. Issues and challenges relating to the functioning and usage of the legacy systems

The detailed information pertaining to the legacy systems shall be provided to the SI as Annexure to this RFP.

<< SPMC to add the relevant annexure pertaining to the details of the legacy systems >>

3.3 Existing Data Center Infrastructure

State shall furnish the details about the existing Data Center Infrastructure such as State Data Center (SDC) that will be provided to the SI for the commissioning the IT infrastructure that will be used to deploy the application. The proposed location and current status of the Data Center and Disaster Recovery Center has to be provided to the SI.

The detailed information pertaining to the Data Centers shall be provided to the SI as an Annexure to this RFP.

<< SPMC to add the relevant annexure pertaining to the details of the data centers>>

3.4 Existing WAN Infrastructure

State shall furnish the details about the existing Network Infrastructure that can be utilized for this project. The information on the bandwidth and availability of the SWAN and any other police networks or private networks that have already been commissioned to provided connectivity to the police stations and other client sites that can possibly be utilized should be provided in this section.

The detailed information pertaining to the WAN Infrastructure shall be provided to the SI as an Annexure to this RFP. << SPMC to add the relevant annexure pertaining to the WAN infrastructure>>

3.5 Existing Client Site Infrastructure

State shall furnish the details about the existing client site infrastructure including any hardware, peripherals, LAN infrastructure etc. at the various client sites (Police Stations, Higher Offices…) that can be utilized for this project.

The detailed information pertaining to the Client Site Infrastructure shall be provided to the SI as an Annexure to this RFP. ***<< SPMC shall add the relevant annexure pertaining to the client site infrastructure >>.***

3.6 Existing Capacity Building Infrastructure (DTCs/RTCs/PTCs/Police Academies)

State shall furnish the details about the existing capacity building infrastructure including any hardware, peripherals, LAN infrastructure at the various District Training Centers and Police Training Colleges that can be utilized for this project for Capacity Building Programs. The detailed information pertaining to the Capacity Building Infrastructure shall be provided to the SI as an Annexure to this RFP.

<< SPMC to add the relevant annexure pertaining to the Capacity Building infrastructure >>

<<SPMC to provide the details of existing infrastructure and organizational setup in the above sections to provide relevant information to the eligible bidders for responding to the CCTNS project implementation requirements in the RFP>>

3.7 Core Application Software (CAS)

The CCTNS application software will contain a "core" for the States/ UTs that is common across all 35 States and UTs. The CCTNS Core Application Software (henceforth referred to as CAS) will be developed at NCRB premises and provided to States and UTs for deployment. Each State/UT would customize the CAS according to their unique requirements and thereafter commission the same. States and UTs also have an option to develop and deploy additional applications over and above the customized CAS. The choice of such applications lies exclusively with the State/UT.

<<The States/UTs shall specify the list of additional applications and CAS extensions / customization along with FRS as an annexure based on PIM report>>.

The Core application Software (CAS) is expected to be ready by ***<July 2011>.***

This section provides the details of the CAS (State) and CAS (Center) that will be developed by the Software Development Agency at the Center. The details provided here should be read in conjunction with the RFP and the associated addendums issued by NCRB for the selection of the Software Development Agency for the Design, Development and Management of CCTNS Core Application Software (CAS).

3.7.1 Volume I - Scope of Services

a. Annexure-1 - Functional Requirements
b. Annexure-1 - Functional Requirements - Wire Frames
c. Annexure-2 - Non Functional Requirements
d. Annexure-3 - Technical Requirements

The functional requirements and the technical architecture of the CAS (State) and CAS (Center) is provided in detail in the RFP issued by NCRB for the selection of the SDA. The relevant sections of the SDA-RFP shall be included as Annexure to this RFP.

The CCTNS application software can be conceptualized as comprising different services that fall under two broad categories, CAS (Center) and CAS (State).

3.8 CAS (Center)

CAS (Centre): CAS (Centre) would reside at NCRB and would cater to the functionality that is required at the GOI level (by MHA and NCRB). Like CAS (State), CAS (Centre) would also be developed by NCRB. CAS (Centre) would enable NCRB to receive crime and criminals' related data from States/UTs in order to organize it suitably to serve NCRB's requirements and to provide NCRB with the analysis and reporting abilities to meet their objective as the central level crime and criminals' data repository of the nation. This would address the crime- and criminals-related information needs of MHA, NCRB, the Parliament, and central government ministries and agencies, citizens and citizen groups. CAS (Centre) also facilitates the flow if crime and criminals information across States/UTs on a need-basis. CAS (Centre) will be developed and deployed at NCRB. Also, CAS (Centre) is expected to interface with external agencies such as passports, transport authorities, etc.

Overview of Services for CAS (Center)
State-SCRB-NCRB Data Transfer and Management
The service shall enable the NCRB to receive, transform, and collate the crime, criminal, and related data from States/UTs, to organize it suitably to serve NCRB requirements.
Crime and Criminal Reports
The service shall enable authorized personnel to generate the reports and perform analysis on the central crime, criminals, and related data repository of the nation.
Crime and Criminal Records and Query Management
The service shall enable the authorized personnel to view various registers and perform basic and advanced queries on the central crime, criminals, and related data repository of the nation.
Talaash Service
The service will enable the user to search for missing persons across a central/ national database.
Person of Interest
The service will enable the user to search for persons of interest such as persons wanted on outstanding warrants, accused, charged habitual offenders, convicts, etc. across the national database.
Registered Vehicle and Vehicle of Interest Service
The service will enable the user to search for registered vehicles and vehicles of interest such as, missing / stolen vehicles, abandoned / unclaimed vehicles, and vehicles involved in traffic incidents across the national database.
Publication Service
This functionality will help the NCRB to publish the periodic crime reviews to the NCRB portal.
NCRB Citizen Interface

The service shall enable the citizens to access/ search the NCRB National Database on the data (ex, Stolen Vehicles / Property, Missing Persons, etc.) that is approved to be made accessible to public.

NCRB Interface for RTI

Due to the sensitivity of the information that pertains to national security and harmony, this service shall enable a limited and restricted access to the authorized external stakeholders to search the NCRB National Database, upon submission of any RTI requests.

3.9 CAS (State)

CAS (State): CAS (State) covers functionality that is central to the goals of CCTNS and is common to all States and UTs. It would focus primarily on functionality at police station with special emphasis on crime investigation and criminals' detection. This part would be developed at NCRB and provided to the States and UTs for configuration, customization and enhancements / extensions. The State / UTs would determine the requirements for configuration, customization and enhancements / extensions. The following are the main function blocks that would comprise CAS (State):

- Registration
- Investigation
- Prosecution
- Records Management
- Search and Basic Reporting

CAS (State) will also include the functionality required at Higher Offices such as State Police HQ, Range Offices, District HQ and SCRB.

It is envisioned that CAS (State), once operational, will significantly enhance the outcomes in core police functions at Police Stations. It will do so primarily through its role- and event-orientation, providing role based user access and controls and an event driven interface that helps police personnel (playing different roles) in more effectively performing their core functions and that relieves police personnel from repetitive tasks that claim much of their time while returning low or no value.

In order for CAS (State) to achieve the above goals, it is envisaged to meet the following requirements:

- It will lay special emphasis on the functions at police stations with focus on usability and ease of use of the application
- It will be designed to provide clear and tangible value to key roles at the Police Station: specifically the SHO (Station House Officer), the IO (Investigation Officer) and the Station Writer.
- It will be event and role-driven. Access controls will be developed and role based access will be provided in the application.
- It will be content/forms-based, with customized forms based on requirements

- It will be a flexible application, event and role-driven system where actions on a case can be taken as required without rigid sequence / workflows
- It will eliminate the need for duplicate and redundant entry of data, and the need for repetitive, manual report preparation – this freeing valuable time and resources for the performance of core police functions
- It will be intelligent and help police perform their roles by providing alerts, highlighting key action areas, etc.
- Ability to view and exchange information amongst Police Stations, between Police Stations and other Police formations and with external entities including citizens
- Reporting and data requirements of higher offices must be met at the State Data Centre/SCRB level and not percolate to the police station level.<< However, if a need is felt for allowing access to certain types of information at the police station level the same may be mentioned by the SPMC>>
- Central facilitation and coordination; but primarily driven and owned by States/UTs where States/UTs can configure and customize the CAS for their unique requirements without the intervention of the central entity

Services in CAS (State)

Citizens Portal Service
This service shall enable Citizens to request services from Police through online petitions and track status of registered petitions and requests online. Citizens requests/services include passport verification services, general service petitions such as No Objection Certificate (NOC) for job, NOC for vehicle theft, NOC for lost cell phone/passport, Licenses for arms, processions etc.
Petition Management Service
The service shall enable the police personnel to register and process the different kinds of general service petitions and complaints.
Unclaimed/Abandon Property Register Service
The service shall enable the police personnel to record and maintain unclaimed/abandoned property registers and match unclaimed/ abandoned property with property in lost/stolen registers.
Complaint and FIR Management Service
The service shall enable the police personnel to register and process the complaints (FIR for cognizable complaints, Non-Cognizable Report for non-cognizable, Complaint Report for genera complaints, etc.) reported by the public.
PCR Call Interface and Management Service
The service shall enable the police personnel to register and process the complaints as received through the Police Control Room through the Dial 100 emergency contact number.
Investigation Management Service

The service shall enable the police personnel to process the complaints through capturing the details collected during the investigation process that are required for the investigation officer to prepare a final report.

Court and Jail Interface and Prosecution Management Service

The service shall enable the police personnel to interface with the courts and jails during the investigation process (for producing evidence, producing arrested, remand etc) and during the trial process.

Crime and Criminal Records and Query Management Service

The service shall enable the police personnel to view various registers and perform basic and advanced queries on the crime and criminal information.

Police Email and Messaging Service

The service shall enable the police personnel to send / receive official as well as personal correspondence.

Periodic Crime, and Law & Order Reports and Review Dashboard Service

The service shall enable the police personnel to view relevant reports and dashboards and to conduct periodic crime, and law & order reviews of the police station(s) under the officer's jurisdiction.

Notification of Alerts, Important Events, Reminders and Activity Calendar or Tasks Service

The service shall capture / generate the required alerts, important events, reminders, activity calendar and tasks.

State-SCRB-NCRB Data Transfer and Management Service

The service shall enable the States/UTs to collate, transform and transfer the crime, criminal, and other related data from state to NCRB.

State CAS Administration and Configuration Management Service

The service shall enable the individual State/UT to configure/ customize the application to suit to their unique requirements.

User Help and Assistance Service

The service shall enable the end user to view the help manuals of the application and in guiding the end user in using the application.

User Feedback Tracking and Resolution Service

The service shall enable the police personnel in logging the issues/defects occurred while using the system.

Activity Log Tracking and Audit Service

The service shall capture the audit trail resulting from execution of a business process or system function.

User Access and Authorization Management Service

The service shall enable the administrative user in setting the access privileges and will provide authentication and authorization functionality

3.10 Development of CCTNS Core Application Software (CAS)

CAS (Centre) and CAS (State) will be developed at NCRB under the overall guidance and supervision of MHA, and a dedicated team from NCRB. NCRB, on behalf of MHA, engaged a professional software development agency (SDA) to design and develop CAS (Centre) and CAS (State) and offer associated services. The SDA would enhance and maintain CAS (Centre) and CAS (State) until the end of the engagement with NCRB and subsequent to that, CAS (Centre) would be managed by NCRB under the guidance of NIC, DIT and MHA and CAS (State) would be managed by the State under guidance of the State IT Department.

CAS (State) would be built as a platform at NCRB addressing the core requirements of the Police Station to provide a basic framework to capture and process crime and criminal information at the police station while providing the States/UTs with the flexibility to build their state specific applications around it and in addition to it. CAS (State) will be provided to States and UTs for deployment. Each State/UT would customize the CAS according to their unique requirements and thereafter commission the same. A bulk of the functionality would be added at States/UTs' discretion and would be added as extensions to the CAS (State) by the System Integrators (SI) chosen by the States/UTs without comprising on the simplicity and performance of the system.

In order to achieve the above stated goals of simultaneously ensuring consistency and standardization across States/UTs (where necessary and possible), and enabling States/UTs to meet their unique requirements, CAS will be built as a highly configurable and customizable application. CAS would therefore be a *product-like* application that could be centrally managed and at the same time customized to meet the unique requirements of the States/UTs and deployed in all States/UTs. The following sections provide details of the configuration and customization requirements of CAS.

In order to achieve the key CCTNS goal of facilitating the availability of *real time* information across police stations and between police stations and higher offices, CAS would be built as a web application. However, given the connectivity challenges faced in a number of police stations, especially rural police stations, the application must be built to work in police stations with low and/or unreliable connectivity.

3.11 Technology Stack for CAS (State)

CAS (State) will be developed in two distinct technology stacks by the Software Development Agency at the Center. The details of the Technology Stacks are provided as an Annexure to this RFP. The SI is expected to bid with one of the technology stacks in response to this RFP. SI shall procure all necessary underlying solution components required to deploy CAS (State) solution for the State / UT.

4 Role of Software Development agency (SDA) in supporting CAS

The SDA will provide Services for CAS (State) for a period of three (3) years followed by two optional one-year periods from the date of successful completion of the CAS (State) Certification. The decision on the two optional one-year periods will be taken in entirety by NCRB. During the contract period, the SDA shall offer the following services:

i. Application maintenance and management Services for CAS (Center) and CAS (state).

ii. Technical Program Management of Implementation of CAS (State) for all 35 States/UTs throughout the duration of the engagement with NCRB/MHA.

Each of these activities is detailed out below.

Application Management Services for CAS (State) and CAS (Center)

The SDA shall provide Application Management services to the CAS (State) and CAS (Center). The application management services include the following:

- Provision of bug fixes, minor changes, error resolutions and minor enhancements.
- Minor enhancements (the usual run-of-the-mill enhancements and not the ones identified as part of Continuous Improvement).
- Change request management based on feedback from the users.
- Release Management; Version control of CAS (State) to be managed centrally, with state-specific configuration incorporated.
- Any changes to CAS code that may be required because of patches to licensed software being used (if any).
- Updating and maintenance of all project documents.
- SI shall be responsible for application management services and maintenance support for additional applications, customizations and extensions at the State / UT.

All planned changes to the application, especially major enhancements and changes in functionality that are deviations from the signed-off FRS/SRS, shall be coordinated within established Change control processes to ensure that:

- Appropriate communication on change required has taken place.
- Proper approvals have been received from CAS Core Group/CTT/CPMU.
- Cost and effort estimate shall be mutually agreed upon between SDA and NCRB

The SDA will define the Software Change Management and version control process and obtain approval for the same from NCRB. For all proposed changes to the application, the SDA will prepare detailed documentation including proposed changes, impact on the system in terms of functional outcomes/additional features added to the system, etc.

Technical Program Management of Implementation of CAS (State)

After successful certification, the SDA will handover the certified CAS (State) to States and UTs through NCRB. While NCRB will facilitate the transfer, the successful transfer of CAS to States/UTs on time is SDA's responsibility. During the period of CAS Solution Design and Development and the Operations and Maintenance Phase following that, the SDA shall provide technical program management services in implementing CAS in States/UTs. Through the Technical Program Management, the SDA shall extend all the necessary support to the State SI and ensure that the SI successfully configures, customizes and deploys CAS (State) in States/UTs. The SDA's Technical Program Management responsibilities include but are not limited to:

- Preparation of technical manuals to enable the SI to configure, customize, enhance and deploy CAS in States/UTs; to be made available to SIs through the CAS online repository managed by the SDA.
- Preparation of "CAS Implementation toolkits" that comprehensively covers details on all the aspects of the CAS (State) and CAS (Centre) applications including but not limited to technical details of CAS, configuration, customization, and extension details, infrastructure sizing details, installation, commissioning, maintenance, infrastructure environment turning, and performance tuning details that are required for the SI to successfully commission the CAS (State) application in the State, integrate CAS (State) with external agencies and third party solutions in the State and integrate CAS (State) with CAS (Centre) to seamless transfer the required data to NCRB. The implementation toolkit shall also include the following:
    - All completed and updated training and support material needed for customizing and deploying CAS
    - All completed and updated project documents including FRS, SRS, HLD, LLD and Test Plans
    - Relevant software assets/artifacts (including configuration utilities / tools, deployment scripts to state SIs to deploy CAS (State) in States/UTs)
    - Relevant standards and design guidelines to the SI for customization, further enhancements, and integration of the application with external systems and third party components that will be implemented by the SI at the State
- Conduct of direct knowledge transfer through monthly contact sessions at NCRB covering all State SIs during the contract period. During the contact sessions, the SDA shall conduct structured training sessions on the CAS Implementation Toolkit prepared by the SDA
- *Dedicated State Points of Contact*: Members of the SDA's team shall act as points of contacts for the state level SIs. The number of States/UTs serviced by each SDA contact person shall be determined in consultation between the CAS Core Group and the SDA. The point of contact will be responsible for addressing queries from an SI and in meeting SLA targets (in responding to States/UTs' needs).
- ***Helpdesk Support*: SDA shall provide Helpdesk support to the State SIs during customization, deployment and stabilization phases with 8 contact hours (during normal business hours of 10 AM to 6 PM), 6 days (Monday through Saturday, both included). The SDA shall deploy a team of at least 5 qualified and certified**

resources in NCRB to address the questions from the SIs.

- *Deployment Scripts*: The SDA shall develop the necessary deployment scripts to deploy CAS (State) in States/UTs and provide the same to State SIs
- *Data Migration Utility*: The SDA shall develop a Data Migration Utility/application with all the formats and tools to load the data into the state databases. This will be provided to States/UTs will enable the State SIs to migrate data from legacy/paper based systems to the CAS databases. The data migration tool will be an extension of the one provided by the SDA. In case the Data Migration Tool developed by the SDA does not incorporate support for any state specific formats etc, the Data Migration Tool developed by the SI will have to support these.
- *Language Localization Support*: Proving interface in local languages is a key requirement of CAS (State). The SDA shall build CAS (State) with interfaces in English and Hindi; and also build CAS (State) in such a way that it can be configured for interfaces in other local languages at the State level by the State SIs. It is the responsibility of the SI to customize CAS (State) for development of local language interfaces. However the SDA shall assist the State SIs where ever required only to support the development of such interfaces.
- Supporting the SI to ensure that the CAS (State) that is configured and customized by the SI in the State successfully passes the User Acceptance Testing (UAT) milestone.
    - Configuration of CAS (State)
    - Customization of CAS (State)
    - Data Migration of CAS (State) related data from the legacy systems and / or manual records to CAS (State)
    - Infrastructure Sizing related to CAS (State)
    - Commissioning and Deployment of CAS (State)
    - Infrastructure Environment Performance Turning related to CAS (State)
    - Maintenance of CAS (State)
    - Integration of CAS (State) with external agency solutions
    - Integration of CAS (State) with additional solutions being integrated by the SI at the State
- Seamless data exchange from CAS (State) to CAS (Centre)
- Troubleshooting, resolution and escalation with State SIs; and ownership of end-to-end data exchange between the CAS (State) and CAS (Centre) needs to ensure seamless and real-time data exchange.

<<SPMC to provide details on readiness for CAS (State) implementation based on the project plan provided in the PIM report>>

Scope of the Project

4.1 Geographical Scope

The State shall specify the locations across which the application and the bundle of services shall be rolled out. This should list all the police stations, circle offices, and other such higher offices which will be covered during the implementation. The section on implementation and roll out plan should specify how the SI is expected to phase out the implementation

- The state map and all the district maps with the location of the police stations shall be provided as annexure to this RFP.

- The information pertaining to the number of police stations, circle offices, and other such units, the approximate number of personnel within each unit shall be provided to the SI as an Annexure to this RFP.

- The building details of all the police stations in the districts along with the exact room identified for setting up computers and other related peripherals including networking components shall be provided as an annexure to this RFP.

- The police stations / higher offices which are difficult in terms of availability of power / connectivity shall be provided as an annexure to this RFP.

<< SPMC to provide the above details in annexure for enabling the eligible bidders to assess and plan the magnitude of the effort involved in project implementation >>

4.2 Functional Scope

The State shall provide the business processes description (augmented with process maps where required) that will be covered under the implementation. In case of any processes unique to the State, the same shall be identified and detailed. For the business processes covered under CAS (State), the detailed specifications will be made available by NCRB at the appropriate time.

This section will provide the IT solutions along with the detailed functional requirements that will be covered under the project. It will contain functional requirements at the different levels of the organization/s covering police stations and higher offices. This section will also list the functionality that the state wants specifically for itself. These can be additional modules or customization requirements of the core application developed and provided by the Centre to the States.

The section shall also cover all the configuration and customization requirements on CAS (State) that are specific to the State that will be the responsibility of the System Integrator during the System Study and Development of the Solution. The requirements shall be provided as functional specifications.

If the State has requirement of new modules / solutions, the functional specifications of the same shall be listed in the Annexure to this RFP.

In case of any legacy systems currently in operation that need to be maintained and integrated, State shall furnish the details about interfaces that need to be developed on the existing legacy systems to interface with CAS(State) and the new modules / solutions. Details of legacy systems can be inserted by SPMC as an Annexure if felt necessary.

In case of any legacy systems currently in operation that need to be migrated to CCTNS, State shall furnish the detailed functional requirements of the legacy systems for the SI to migrate to CCTNS.

Integration with CAS (Center) shall also be detailed out in the functional scope.

In case of any external interfaces that need to be interfaced with CAS (State) and the new modules / solutions, the State shall provide details about interfaces that need to be developed.

External Interfacing shall be provided to interface with Common Service Centres (CSC), e-forms applications (of State portals), Transport Department, Courts, Jails, Hospitals, Universities, Telephone Service Providers, other external government departments etc. to facilitate electronic exchange of information.

<< SPMC shall prepare the list of state MMPs (Targeted Public Distribution System, State portal, SSDG, etc) that needs to be integrated with the CCTNS based on PIM report assessment study and in consultation with State/UT Police Department>>

The suggested technical architecture and standards are provided as an Annexure to this RFP. The non-functional requirements for the solution are provided as an Annexure to this RFP.

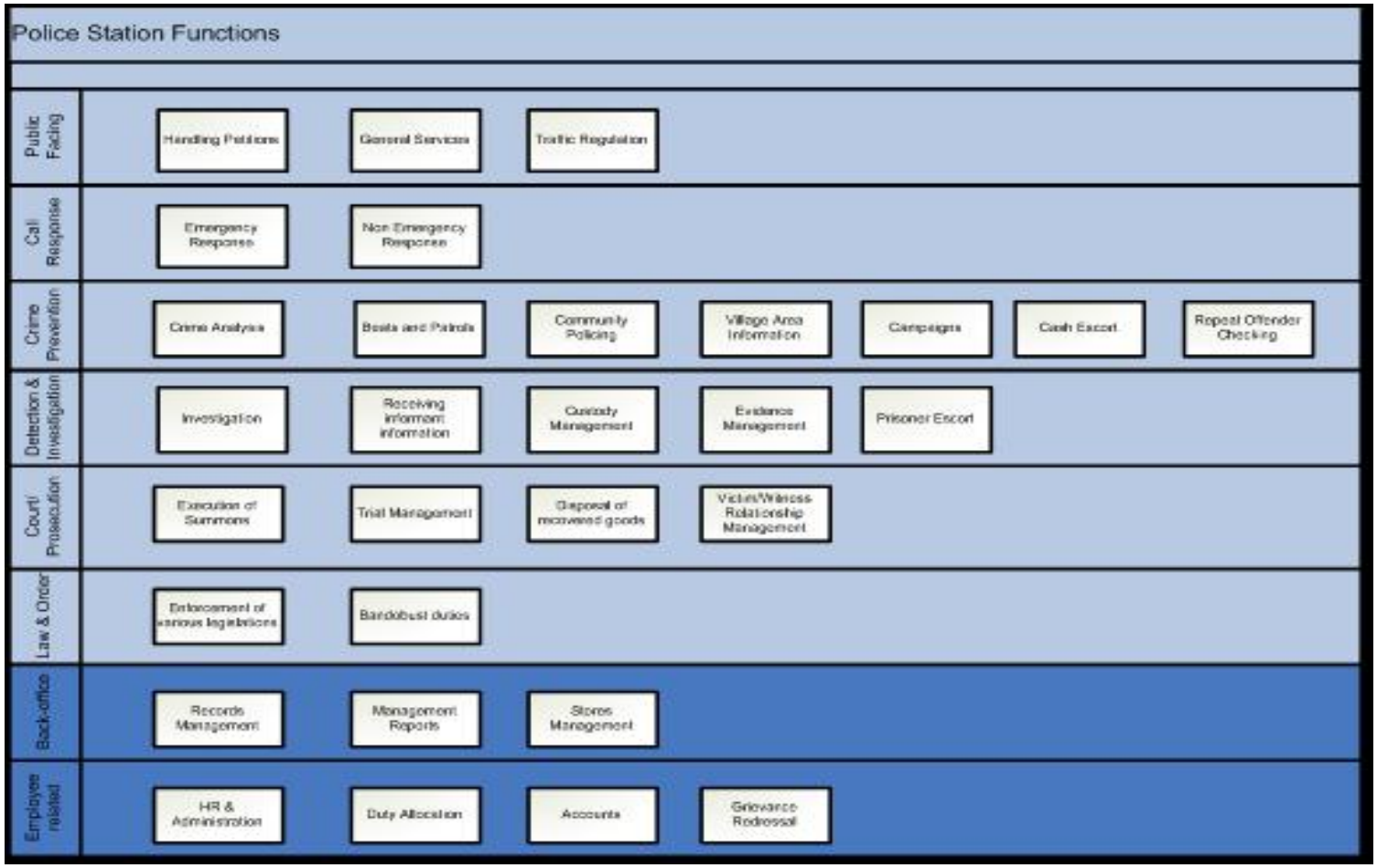
Brief Description of Police Station Process

<< The SPMC may add the additional functions as per State specific requirements in addition to the core Police Station functions in consultation with State/UT keeping in view the adherence of MHA guidelines>>

The police station is a hub of several activities. Maintenance of law and order, crime investigation, protection of state assets, VIP protection, traffic control, service of summons, production of witnesses in courts, intelligence gathering, *bandobust* duties, crime prevention are some of multifarious functions that the police station and its officers have to discharge. Police stations also serves as front-end of the entire police department in dealing with public complaints and requests, and at the same time they occupy a pivotal place as the primary information collection agent for the other functions/wings within the department. In order to achieve the end-objective of bringing in efficiency and effectiveness in the police station, it is crucial to understand the different responsibilities of the police station and identify the key services that need to be addressed in this study.

The first step in identifying the key functions is to segment them under core and supporting, where the core includes services like crime prevention, petition handling and the supporting include the employee related personnel and pay functions, store management etc. The efficiency gains are achieved through addressing the supporting services where the police station is provided with tools to perform the tasks faster with fewer resources, and the effectiveness gains are achieved by addressing the core services where the police station can improve the quality of the services.

Based on the study in the police stations, the various functions of a police station have been mapped in the diagram below.



Functions in a Police Station

SPMC shall provide details of police functions and processes relevant to CAS (State) application for implementation of CCTNS in State/UT as per detailed assessment study made in the PIM report.

4.3 Scope of Services during Implementation Phase

This section provides the detailed scope of CCTNS project in the State/UT through implementation of Bundle of Services to be provided by the System Integrator. The scope of work shall comprise the following activities:

a) Project planning and management

b) System study, design, application development and integration of the CCTNS Application Software based on Core Application Software (CAS) provided by NCRB

c) Configuration Customization and Extension (New Modules) of CAS (State) and Integration with CAS (Center) and External Agencies. CAS (State) will be developed in two distinct technology stacks by the SDA at the Center. The SI is expected to bid with one of the technology stacks in the response to this RFP. SI shall procure all the necessary underlying solution components required to deploy the CAS (State) solution for the State/UT.

d) Infrastructure at the District Training Centers (*If the State/UT has already completed infrastructure implementation at DTC/RTC/PTC, the SPMC may modify this activity accordingly*) including computers, networking components, projectors and UPS.

e) Site preparation at the Client site locations (police stations, circle offices, Commissionerates (if any), Range offices, Zones, SCRB, SDPOs, District HQ and State HQ), Training Centers and Data Center.

f) IT Infrastructure at the Client site locations (police stations, circle offices, Commissionerates (if any), Range offices, Zones, SCRB, SDPOs, District HQ and State HQ).

g) Network connectivity (SPMC to modify this activity based on PIM report assessment)

h) IT infrastructure at the Data Center and Disaster Recovery Center including the necessary hardware, software and other networking components.

i) Data migration and Digitization of Historical Data

j) Migration of CIPA and CCIS Police Stations / Higher Offices to CCTNS

k) Capacity building

l) Handholding Support

m) Support to 3rd party acceptance testing, audit and certification

In implementing the above, the SI shall strictly adhere to the standards set by the MHA, NCRB, and State. The project will be managed out of the Office of the State Nodal Office in State HQ. At all points in the execution of the project, key senior resources including the project manager must be based at State Nodal Officer's office in State HQ.

<< The item (n) above refers only to the mandatory support to be provided by SI during the execution of the activity>>

<< The item (a) above refers to Project planning and management functions from the side of SI which should align with the overall Project planning and management functions of the State/UT executed through State/UT Nodal officer with the support of SPMU >>

4.3.1 Project Planning and Management

This project is a geographically spread initiative involving multiple stakeholders. Its implementation is complex and though its ultimate success depends on all the stakeholders; the role of SI is key and hence SI is required to design and implement a comprehensive and effective project management methodology together with efficient & reliable tools.

To have an effective project management system in place, it is necessary for the SI to use a Project Management Information System (PMIS). The SI shall address at the minimum the following using PMIS:

a. Create an organized set of activities for the project
b. Coordinate and collaborate with various stakeholders including the police departments, SPMU, CPMU and SDA
c. Establish and measure resource assignments and responsibilities
d. Construct a project plan schedule including milestones
e. Measure project deadlines, budget figures, and performance objectives
f. Communicate the project plan to stakeholders with meaningful reports
g. Provide facility for detecting problems and inconsistencies in the plan
h. During the project implementation the SI shall report to the State Nodal Officer, on following items:
    (i) Results accomplished during the period;
    (ii) Cumulative deviations to date from schedule of progress on milestones as specified in this RFP read with the agreed and finalized Project Plan;
    (iii) Corrective actions to be taken to return to planned schedule of progress;
    (iv) Proposed revision to planned schedule provided such revision is necessitated by reasons beyond the control of the SI;
    (v) Other issues and outstanding problems, and actions proposed to be taken;
    (vi) Interventions which the SI expects to be made by the Project Director and / or actions to be taken by the Project Director before the next reporting period
i. Progress reports on a fortnightly basis
j. Interventions which the SI expects to be made by the State Nodal Officer and/or actions to be taken by the State Nodal Officer before the next reporting period;
k. Project quality assurance reports
l. Change control mechanism
m. As part of the project management activities, the SI shall also undertake:
    i. Issue Management to identify and track the issues that need attention and resolution from the State.
    ii. Scope Management to manage the scope and changes through a formal management and approval process
    iii. Risk Management to identify and manage the risks that can hinder the project progress

The Project plan prepared by the SI would be reviewed by the Governance Structure (please refer to Annexure on details on Governance Structure to be setup in the State) in the State and approved by the Apex / Empowered Committee on the advice of the State Mission Team and State Project Management Unit.

The SI would update and maintain the Project Plan throughout the duration of the engagement. All changes are to be reviewed and approved by the CAS Core Group.

Requirements Traceability Matrix

The SI would ensure that developed solution is fully compliant with the requirements and specifications provided in the RFP such as functional, non-functional and technical requirements. For ensuring this, the SI shall prepare a Requirements Traceability Matrix on the basis of Functional Requirements Specifications (FRS), Non Functional Requirements Specification, and Technical Requirements provided by State (updated, expanded and fine-tuned by the SI as necessary) and the System Requirements Specifications (SRS) prepared by the SI. This matrix would keep track of the requirements and trace their compliance through different stages of the project including software design, coding, unit testing and acceptance testing. The Requirements Traceability Matrix would be a live document throughout the project, with the SI team updating the matrix at every stage to reflect the meeting of each specification at every stage.

Through the duration of the project, the State Mission Team will periodically review the Traceability Matrix. State Governance Structure would provide the final approval on the advice of the State Mission Team and SPMU once they are satisfied that all requirements are met.

Project Documentation

The SI shall create and maintain all project documents that would be passed on to State as deliverables as per the agreed project timelines. The documents created by the SI will be reviewed and approved by the Governance Structure Setup in the State (Please refer to Annexure for details on Governing Structure to be set up in the State). State Mission Team would also approve any changes required to these documents during the course of the project. State will finally sign-off on the documents on the recommendation of State Mission Team / SPMU / Empowered Committee.

Project documents include but are not limited to the following:

- Detailed Project Plan
- Updated/vetted FRS
- SRS document
- HLD documents (including but not limited to)
-
    - Application architecture documents
    - ER diagrams and other data modeling documents

  - Logical and physical database design
  - Data dictionary and data definitions
  - Application component design including component deployment views, control flows, etc.
- LLD documents (including but not limited to)
  - Application flows and logic including pseudo code
  - GUI design (screen design, navigation, etc.)
- All Test Plans
- Requirements Traceability Matrix
- Change Management and Capacity Building Plans
- SLA and Performance Monitoring Plan
- Training and Knowledge Transfer Plans
- Issue Logs

The SI shall submit a list of deliverables that they would submit based on the methodology they propose. The SI shall prepare the formats/templates for each of the deliverables upfront based upon industry standards and the same will be approved by State prior to its use for deliverables.

All project documents are to be kept up-to-date during the course of the project.

The SI shall maintain a log of the internal review of all the deliverables submitted. The logs shall be submitted to State Nodal Officer on request.

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

Procure, Commission and maintain Project Management, Configuration Management and Issue Tracker Tools at State HQ / SCRB

Project Management Tool: The SI shall keep the project plan and all related artifacts up-to-date during the course of the project. In order to help with the project management, the SI shall use a suitable standard, proven off-the-shelf project management tool (preferably with unrestricted redistribution licenses). The SI shall install the project management software at State's premises right at the beginning of the project. The tool shall provide the dashboard view of the progress on project milestones by the Nodal Officer and other Supervisory Officers of CCTNS.

Configuration Management Tool: The SI shall keep all project documents up-to-date during the course of the project. In order to help with the version/configuration management for all documents (including source code and all other project artifacts), the SI shall use a suitable standard, proven off-the-shelf configuration management tool (preferably with unrestricted redistribution licenses). The SI shall install the configuration management software at State's premises right at the beginning of the project.

Issue Tracker: The SI shall employ a suitable and proven tool for tracking issues (preferably with unrestricted redistribution licenses) through the execution of the project. The SI shall install the Issue Tracking System at State's premises to enable State's users to access and use the same.

The SI shall procure and commission the required infrastructure (software, servers) for *Project Management Tool, Configuration Management Tool* and *Issue Tracker* tool and maintain the same through the duration of the project. These tools along with the servers on which they are deployed will become property of the State and will be used by State even beyond the contract period.

The SI would setup an online repository on PMIS / Configuration Management Tool for providing centralized access to all project documents including manuals and other materials. The online repository would be maintained by the SI through the engagement period. The SI should ensure that the repository is built on appropriate security features such as role- and necessity-based access to documents.

4.3.2 Configuration, Customization, and Extension (New Modules) of CAS (State) and Integration with CAS (Center) and External Agencies

System Study, Design, Application Development and Integration

In terms of functionality, CAS would cover those police functions that are central to the goals of the CCTNS project and are common across States/UTs. This includes core functions in the areas of Complaints/ Case Management, Police Station Efficiency and Analysis & Reporting. It is estimated that of the possible police functions that could potentially be part of the CCTNS application at the State level, the functionality covered by CAS is a relatively small part. Therefore, CAS is being developed as a product-like application that could be centrally managed and at the same time customized to meet the unique requirements of the States/UTs and deployed in all States/UTs. SI would be responsible for adding the functionality over and above the CAS (State) as provided in the Annexure.

<< State to provide the Annexure detailing out the additional functionality that the SI would be required to add>>

CAS (State) contains functionality that is common across all States/UTs. CAS (State) would be configured, customized, extended by the SI based on the unique requirements of the State and deployed at the State Data Centre. In order to ensure consistency between States/UTs and facilitate the exchange of crime and criminals related information between States/UTs and the Centre and between States/UTs, NCRB would develop, own and maintain the CAS. The services that will be provided by the Software Development Agency (SDA) for the CAS (State) are articulated in Annexure 1.

For the additional functionality that the State / UT wants to be added to CAS(State), the SI shall carry out a detailed systems study to refine the Functional Requirements Specifications provided as Annexure to this RFP ***<< Information to be provided by the SPMC>>*** and formulate the System Requirements Specifications (SRS) incorporating the functional specifications and

standards provided by the NCRB and the state-specific requirements. The SRS preparation shall take into account the BPR recommendations suggested by the NCRB.

The SI shall carry out a detailed systems study to refine the Functional Requirements Specifications provided as Annexure to this RFP and formulate the System Requirements Specifications (SRS) incorporating the functional specifications and standards provided by the NCRB and the state-specific requirements. The SI shall also study CAS-State and CAS-Center being developed at NCRB and / or already running application in the State/UT during the system study phase. The study should also include different integration points of CAS state with external agencies as per state requirement. The SRS preparation shall take into account the BPR recommendations suggested by the NCRB / State. The SI should also prepare a detailed document on the implementation of CAS (State) with respect to configuration, customization and extension as per the requirement of state. The SI would also prepare a change/reference document based on changes or deviations from the base version of the CAS (State) with appropriate references to all the artifacts /documents provided by NCRB / State.

1. Conduct of System Study at selected locations. <<SPMC to identify the locations for the SI's System Study>>
2. Preparation of System Requirements Specifications (SRS) for additional functionalities and different integration points with CAS (Center) and External agencies.
3. Preparation of CAS(State) implementation document with respect to Configuration, Customization and extensions as per the requirement of state.
4. Preparation of the Solution Design
5. Solution Development and/or Customization and/or Configuration and/or Extension as required
6. Development of reports
7. Formulation of test plans and test cases for additional functionalities and different integrations with external agencies including CAS (Center)
8. Change/Reference document include all the changes or deviations from the base version of the CAS(State)
9. Testing of the configured solution (CAS) and additional functionalities.

Enhancements of functions / additions of new modules / services to CAS-State as per state specific requirements / integration requirements to various interfaces / SSDGs shall also be incorporated in the SRS and shall form the scope of work for the SI.

Creation of Test Plans

Once the SRS is approved and design is started, the SI would prepare all necessary Test Plans (including test cases), i.e., plans for Unit Testing, Integration and System Testing and User Acceptance Testing. Test cases for UAT would be developed in collaboration with domain experts identified at state headquarters. The Test Plans also include planning for the testing any integration with 3rd party COTS solutions, CAS (Center), any external agencies. The Test Plans should also specify any assistance required from State and should be followed upon by the SI.

The SI should have the Test Plans reviewed and approved by the State Mission Team/SPMU/ Empowered Committee. The State headquarters will sign off on the test plans on the advice of State Mission Team/SPMU.

High Level Design (HLD)

Once the SRS is approved, the SI would complete the HLD and all HLD documents of the additional functionalities, integration with CAS Center and external agencies upon the approved SRS. The SI would prepare the HLD and have it reviewed and approved by the State mission team/SPMU. The State will sign off on the HLD documents on the advice of State Mission Team/ SPMU.

Detailed (Low Level) Design (LLD)

The LLD would interpret the approved HLD to help application development and would include detailed service descriptions and specifications, application logic (including "pseudo code") and UI design (screen design and navigation). The preparation of test cases will also be completed during this stage. The SI would have the design documents reviewed and approved by the State Mission Team/SPMU. State headquarters/Nodal officer will sign off on the LLD documents upon the advice of State Mission Team/SPMU.

Application Development and Unit Testing

The SI would develop the application in accordance with the approved requirements specifications and design specifications and according to the approved Project Plan; and carry out the Unit Testing of the application in accordance with the approved test plans. The SI shall consider the local language support and prepare necessary configuration files for both CAS and additional functionalities/modules developed as part of CAS.

The SI would also implement the changes proposed in the Change/Reference document to Core Application Software and carry out a thorough regression testing includes running some of the previously executed scripts for the functionality from the traceability matrix provided by NCRB/State.

The SI shall also develop a Data Migration Utility/application for the additional functionalities with all the formats and tools to load the data into the state databases. This will migrate data from legacy/paper based systems of the new modules to the CAS databases.

The user acceptance testing and fine-tuning of the application would be at State Headquarters premises. Also, the key senior resources would continue to be based onsite at State Headquarter premises.

Configuration of CAS (State)

The SI shall configure CAS (State) to the requirements of the State that include but not limited to:

1. Developing Local Language Interfaces and Support

2. Configuring users
3. Configuring Police Stations / Higher Offices
4. Configuration of the UI as required by the State

The collection of the data required for the configuration of the CAS (State) shall be the responsibility of the SI. SPMC in coordination with the State Departments shall validate the data collected by the SI.

Setup of Technical Environment at State Headquarters

The SI shall procure, setup and maintain the required software and the infrastructure for systems testing, functional testing and User Acceptance Testing; and training activities within State Headquarter premises; and for any other activities that may be carried out of State Headquarter premises such as issue management (Issue Tracker), document repository (configuration management tool), etc.

Regression, Integration, System and Functional Testing

After successful unit testing of all components, the SI would conduct full-fledged integration testing, system testing and functional testing in accordance with the approved Test Plans for the configured/customized CAS (State), additional functionalities and also integration with CAS (Center) and external agencies. This would include exhaustive testing including functional testing, performance testing (including load and stress), scalability testing and security testing. Functional testing will be led by the SI's experts.

A thorough regression testing should be conducted for those functionalities identified in Change/Reference document to provide a general assurance that no additional errors were cropped up in the process of addressing the customizations and/or Extensions. Customized CAS (State) Integrations with CAS (Center) and with any external agencies should be thoroughly tested.

Making all necessary arrangements for testing including the preparation of test data, scripts if necessary and setup of test environment (across multiple platforms) shall be the responsibility of the SI.

The SI along with State Mission Team/ SPMU should take the responsibility in coordinating with NCRB and other external agencies for a smooth integration.

Test Reports

The SI shall create test reports from testing activities and submit to State Mission Team/SPMU/Empowered Committee for validation

Test Data Preparation

The SI shall prepare the required test data and get it vetted by State Mission Team/SPMU. The test data shall be comprehensive and address all scenarios identified in the test cases. The SI should also prepare the test data for all required integrations including CAS (Center) and external agencies.

User Acceptance Testing (UAT)

Test Plans for UAT would be prepared by the SI in collaboration with the State Mission Team /SPMU domain experts. The SI will plan all aspects of UAT (including the preparation of test data) and obtain required assistance from State Headquarters to ensure its success. State Mission Team/SPMU will assemble representatives from different user groups based on inputs from the SI and would facilitate UAT. The SI would make the necessary changes to the application to ensure that CAS successfully goes through UAT.

It's mandatory for SI to incorporate/consider test cases as part of UAT test cases for those customized and/or extensions and/or configured functionalities identified from traceability matrix provided by NCRB / State.

4.4 Infrastructure at the District Training Centers

The SI is expected to setup the district training centers at each District Headquarters and Police Commissionerates (if any). The premises will be provided by the State/UT but the entire infrastructure such as projectors, computers, networking components, UPS required to run the training lab shall be provided by the SI.

<< **In addition to District Training Centers, SPMCs shall also provide details of RTC/PTC/Police Academy wherever relevant. The above details shall apply only to State/UTs which intend to strengthen Capacity Building infrastructure through SI. SPMC shall provide details only if such exercise has not been taken up, in consultation with State/UT nodal officer.>>**

4.5 Site Preparation at Police Stations and Higher Offices

The SI is expected to prepare the client sites for setting up the necessary client site infrastructure. Site preparation at Police Stations & Higher Offices will include but not limited to:

i. Provision of Local area network (LAN cables, LAN ports,)
ii. Provision of computer furniture for Police Stations
iii. Ensure adequate power points in adequate numbers with proper electric-earthling
iv. Earthing and electric cabling as required at the site
v. In addition to the above Supply and fixing of furniture like computer tables, chairs and other item shall be carried out to ensure successful site preparation and installation of CCTNS at every access location

Site Preparation shall cover all the activities necessary to enable the Police Station to setup the client side infrastructure and operate on CCTNS.

4.6 Infrastructure at the Client Side Locations

The premises for offices will be provided by the department at respective locations. The list of Police Stations, Circle offices, and other locations where the infrastructure is required is provided under the Geographical Scope Section. SI shall procure the CCTNS infrastructure required at the locations statewide.

At each such location the following shall be carried out.

1. Supply of the hardware, software, networking equipments, UPS, DG set to the location as per the requirements
2. Ensure adequate number of power points with proper electric-earthing
3. Redundant Network Connectivity - Ensuring last mile connectivity and testing. (At some locations SWAN may be available. SI shall ensure there is redundancy in the connection)
4. Installation, Testing and Commissioning of UPS, DG-Set
5. Physical Installation of Desktops, Printer, Scanner, /MFD, Switch- Connecting peripherals, devices, Plugging in
6. Operating System Installation and Configuration
7. Installation of Antivirus and other support software if any
8. Configuring the security at the desktops, switch and broadband connection routers
9. Network and browser Configuration
10. Test accessibility and functionality of CCTNS application from the desktops
11. Ensuring all the systems required are supplied, installed, configured, tested and commissioned and declaring the site to be operational.
12. In addition to the above supply and fixing of furniture like computer tables, chairs and other items shall be carried out to ensure successful site preparation and installation of CCTNS at every location

CCTNS application will be accessed and used at various access locations across the state like Police Stations, Circle Office, Sub Division office, District Office and other higher offices.

<<Based on the total number of Police Stations, Higher Offices to be covered, SPMC to provide the total number and specifications for client systems, printers, UPS, network components and other peripherals as per the details in the PIM report. >>

<< SPMC to provide a table for Technical Bill of Materials for all the hardware and infrastructure items. >>

The minimum infrastructure required at Police Station include-

Police Station Hardware	
Items	Qty
Client Systems	4
HDD 160GB	1
Duplex Laser Printer	1
Multi-Function Laser (Print/Scan/Copy)	1
UPS for 120min backup	1
2KVA Generator Set	1
16-Port Switch	1
Fingerprint Reader	1
Digital Camera	1
Electronic Pen	1
Paper /Toner	

The infrastructure required at Higher Offices includes:

Higher Office Hardware / Site Preparation Cost						
Higher Offices		PC	UPS	MFP	Switch	Paper / Toner
Circle	Qty	3	1	1	1	
Sub-Division	Qty	3	1	1	1	
Range / Zone	Qty	4	1	1	1	
SCRB	Qty	4	1	1	1	
Higher Offices		PC	MFP	UPS / Switch		Paper / Toner
Commissionerates (if any)	Qty	25	25	As per requirement		
Districts	Qty	10	10	As per requirement		
Police Headquarters	Large/ Medium/ Small	50 /30 /15	50 /30 /15	As per requirement		

4.7 Network Connectivity for PS, Higher Offices, and DTC

The WAN connectivity for the CCTNS project will be provided by BSNL through MPLS connectivity at select offices and VPN on Broadband for rest of the offices. For offices which cannot be connected through conventional means, VSAT connectivity would be provided. SWAN connectivity will be used to backup. However, SI will be responsible for setting up and maintenance of LAN at the individual offices.

The SI shall provide the last mile connectivity to the Police Stations / Higher Offices / District Training Centers wherever required. SI shall procure the connectivity from a service provider and the SI is expected to setup the last mile connectivity to the client site. SI shall use SWAN for the connectivity redundancy where feasible. SI shall prepare comprehensive network architecture for connecting all the Police Stations / Higher Offices to the State DC and DRC and also the connectivity from the State DC / DRC to the DC / DRC at the Center hosting the CAS (Center).

Guidelines on Network architecture and details provided by BSNL with respect to connectivity are provided as Annexure to this RFP.

The connectivity between the State Data Center / Disaster Recovery Center and the NCRB data center that hosts CAS (Center) will be provided by the SI.

<<SPMC shall define the scope of network connectivity for CCTNS based on PIM report assessment and MHA guidelines. >>

<< SPMC to provide a table for Technical Bill of Materials for all the hardware and infrastructure items. >>

4.8 IT Infrastructure at the data center and Disaster Recovery Center

The SI shall provide system integration services to procure and commission the required software and infrastructure at the State Data Centre and Disaster Recovery Centre, deploy the configured and customized CAS (State), addition modules developed if any, and integrate with CAS (Centre) and any External Agencies as provided in the functional scope.

The SI shall be completely responsible for the sourcing, installation, commissioning, testing and certification of the necessary software licenses and infrastructure required to deploy the Solution at the State Data Centre and at the Disaster Recovery Centre (DRC).

SI shall ensure that support and maintenance, performance and up-time levels are compliant with SLAs. SI shall coordinate with SDC in isolating the issues between solution stack and common infrastructure provided by SDC; and in ensuring that they are reported to concerned parties so that they are resolved in timely manner.

To ensure redundancy requirements are met, SI shall ensure that infrastructure procured by the

SI has redundancy built in. SI shall also provide descriptive 'Deployment Model, Diagrams and Details' so that redundancy requirements for the common Data Center infrastructure can be addressed

CAS (State) will be developed in two distinct technology stacks by the SDA at the Center. The SI is expected to bid with one of the technology stacks in the response to this RFP. SI shall procure all the necessary underlying solution components required to deploy the CAS (State) solution for the State/UT.

State will provide the premises for Primary Data Centre (DC) for hosting the solution as well as the Disaster Recovery Centre (DRC). The SI is responsible for sizing the hardware to support the scalability and performance requirements of the solution. The SI shall ensure that the servers and storage are sized adequately and redundancy is built into the architecture that is required meet the service levels mentioned in the RFP.

- The SI shall be responsible for the sizing of necessary hardware and determining the specifications of the same in order to meet the requirements of State.

- SI shall provide a Bill of Material that specifies all the hardware, software and any additional networking components of solution for the State Data Centre and DRC, in detail so as to facilitate sizing of common Data Centre and DRC infrastructure such as Racks, Power and Cooling, Bandwidth among other components. The common DC and DRC infrastructure shall be provided by State.

- SI shall ensure that effective Remote Management features exist in solution so that issues can be addressed by the SI in a timely and effective manner; and frequent visits to Data Centre /DRC can be avoided.

- After commissioning and testing of the entire system at State Data Center / DRC, the SI shall support the State in getting the system certified by a 3rd party agency identified by State.

- State will provide the premises for Primary Data Centre (DC) and Disaster Recovery Centre (DRC) for hosting the solution. The solution shall be hosted in a collocation model in the Data Centres.

The following common data Centre services will be available to the SI through the Data Centre Operator / Data Centre Service Provider (DCO):

1. Rack
2. Power and Cooling
3. UPS, DG set power backup
4. Bandwidth and Connectivity

5. LAN
6. VPN
7. Firewall
8. Intrusion Protection System
9. Fire prevention
10. Physical security surveillance
11. Network Operation Centre
12. Common Data Centre facility Maintenance and Support

The SI is responsible for the below at the Data Centre / DRC:

1. Servers (Web, Application, Database, Backup, Antivirus, EMS, etc.)
2. Enterprise Management System (EMS)
3. Antivirus Software
4. SAN Storage
5. SAN Switches
6. Tape Library
7. All necessary software components including but not limited to Operating System, Backup Software, and SAN Storage Management Software

SI shall develop / procure and deploy an EMS tool that monitors / manages the entire enterprise wide application, infrastructure and network related components. The SI shall also deploy a backup software to periodically backup all data and software.

The indicative specifications for the Web Server, Application Server, Database Server and Networking components shall be provided as Annexure to this RFP.

<< SPMC to add the relevant annexure pertaining to the technical specifications of Web Server, Application Server, Database Server, Networking components, Storage etc..>>

<< SI shall provide Bill of Materials for all the hardware, infrastructure items and other items which are part of the scope. SPMC to add a detailed table of Bill of materials. Given below is an indicative format for Technical Bill of Materials>>

Item	**Original Equipment Manufacturer**	**Item Desc.(Model/Make)**	**Unit of measurement**	**Quantity # (units)**
Please insert details as required				

4.9 Data Digitization & Data Migration

Data Migration

Migrating the data from the other systems/manual operations to the new system will include identification of data migration requirements, collection and migration of user data, collection and migration of master data, closing or migration of open transactions, collection and migration of documentary information, and migration of data from the legacy systems.

The SI shall perform the data digitization & migration from manual and/or the existing systems to the new system. The Data digitization & migration to be performed by the SI shall be preceded by an appropriate data migration need assessment including data quality assessment.

The Data migration strategy and methodology shall be prepared by SI and approved by State/UT. In case these have already been prepared by the SPMC, the SI can take the SPMC's documents as inputs and add / modify as necessary. Though State/UT is required to provide formal approval for the Data Migration Strategy, it is the ultimate responsibility of SI to ensure that all the data sets which are required for operationalization of the agreed user requirements are digitized or migrated.

Any corrections identified by State/UT or any appointed agency, during Data Quality Assessment and Review, in the data digitized/ migrated by SI, shall be addressed by SI at no additional cost to State/UT. So far as the legacy data is concerned, they are either available as structured data in the IT systems that are currently used by State/UT for related work or in the form of paper documents (Cases Documents and Police Station Registers). Almost all of such data items relevant for a Police Station are maintained at the same Police Station.

Data Migration Requirements

1. Since there could be structural differences in the data as stored currently from the new system there should be a mapping done between the source and target data models that should be approved by Project Director
2. Carry out the migration of legacy electronic data
3. Carry out the migration of the data available in the existing registers, reports, case files,etc.(Physical Copies)
4. Scan images and pictures within the case file in color and store them in the digital format.
5. Provide checklists from the migrated data to State Nodal Officer for verification, including number of records, validations (where possible), other controls / hash totals. Highlight errors, abnormalities and deviations.
6. Incorporate corrections for the errors discovered during verification process, as proposed
7. Get final sign off from State Nodal Officer/ Empowered Committee for migrated / digitized data
8. At the end of migration, all the data for old cases and registers must be available in the new system

Scope of Data Migration

SPMC shall bring out the following:

1. *Status of digitization of historic data (particularly in States where the Pilots have to run)*
2. *Scope for Data Migration including the broad data sets to be migrated and volume of cases/complaints/FIRs/open transactions to be migrated (at least last 10 years of historical data)*
3. *Sources of such data (Any legacy systems, Police Stations/Higher Offices/DCRB/CCRB/SCRB/any other Crime/Criminal Information Repositories such as Central Crime Station,).*
4. *Data Migration Plan with respect to the process to be adopted for data migration, validations to be carried out, the responsibilities of the Police Department and System Integration during the Data Migration, and the phasing of data migration.*

The data reconciliation and de-duplication is a major activity to be carried out as part of the data migration.

Recommended Methodology of Data Migration

Data migration methodology will comprise the following steps, explained as below. However this is just a guideline for data migration effort and the SI will be required to devise his own detailed methodology and get it approved by State Nodal Officer.

1. *Analysis*

Analysis of the legacy data and its creation, conversion, migration and transfer to the proposed new data base schema will be started during the scoping phase and shall take a parallel path during the design and development phase of the application. It will cover the following steps:

a) Analyze the existing procedures, policies, formats of data in lieu of the new proposed system to understand the amount of the data and the applicability in CCTNS
b) Write a specification to create, transfer and migrate the data set
c) Document all exceptions, complex scenarios of the data
d) This phase will generate the specification for Data Take–On routines

2. *Transformation*

Transformation phase can be commenced after integration testing phase. It will entail the following steps:

a) Identify the fields, columns to be added/deleted from the existing system
b) Identify the default values to be populated for all ‘not null’ columns
c) Develop routines to create (Entry if any by data entry operators), migrate, convert the data from hard copies, old database (if any), computer records to the new database
d) Develop test programs to check the migrated data from old database to the new database
e) Test the migration programs using the snapshot of the production data
f) Tune the migration programs & iterate the Test cycle

g) Validate migrated data using the application by running all the test cases

h) Test the success of the data take-on by doing system test

3. Data Take–On

Take–On phase will be initiated when the proposed solution is ready to be deployed. It will entail the following steps:

i) Schedule data transfer of the computerized data that has been newly created by the data entry operators based on the hard copy records.

j) Schedule data transfer of the existing digital data in the proposed new format

k) Migrate the data from an old system (legacy) to the envisaged database

l) Test on the staging servers after the data take-on with testing routines

m) Migrate from staging servers to production servers

n) Deploy and rollout the system as per the project plan

Additional Guidelines for Data Migration

1. SI shall migrate/convert/digitize the data at the implementation sites of State/UT.
2. SI shall formulate the "Data Migration Strategy document" which will also include internal quality assurance mechanism. This will be reviewed and signed–off by State prior to commencement of data migration.
3. SI shall incorporate all comments and suggestions of State in the Data Migration Strategy and process documents before obtaining sign–off from State.
4. SI shall perform mock data migration tests to validate the conversion programs.
5. SI shall ensure complete data cleaning and validation for all data migrated from the legacy systems to the new application.
6. SI shall validate the data before uploading the same to the production environment.
7. SI shall generate appropriate control reports before and after migration to ensue accuracy and completeness of the data.
8. SI shall convey to State in advance all the mandatory data fields required for functioning of the proposed solution and which are not available in the legacy systems and are required to be obtained by State.
9. In the event State is unable to obtain all the mandatory fields as conveyed by SI, SI shall suggest the most suitable workaround to State. SI shall document the suggested workaround and sign-off will be obtained from State for the suggested workaround.
10. SI shall develop data entry programs / applications that may be required for the purpose of data migration in order to capture data available with / obtained by State in non – electronic format.
11. SI shall conduct the acceptance testing and verify the completeness and accuracy of the data migrated from the legacy systems to the proposed solution.
12. State may, at its will, verify the test results provided by SI.

Data Digitization

In addition to the data migration SI would also digitize the historical data (covering the last 10 years). The historical data to be digitized would include crime (case/incident) data, criminals' data, the data from the 7 IIF and relevant historical information parameters/data used to generate registers and reports. The unit of data digitization shall be one case file. Each case file shall consist of information pertaining to all 7 IIFs, information parameters relevant to generate specific registers from that case file and information parameters relevant to generate specific reports from that particular case file. The SPMC has to categorize the case files and associated manual registers and reports as a single unit to arrive at the number of records for each category.

SNo	Name of the Record (A)	No. of Records to be digitized (B)
1		
2		

<< The SPMC shall provide more details about Data digitization (Data entry of manual/physical registers into digital format) based on the PIM report assessment with respect to volume of data, (total number of records)>>

<< The SPMC to clearly provide the total number of records to be digitized, scanned and migrated in a table format>>

<< SPMC to specify the unit of data digitization (number of case files and associated records and registers) and prepare a detailed table for data digitization and migration requirements>>

4.10 Migration of CIPA and CCIS Police Stations / Higher Offices to CCTNS

The SI is also responsible for migrating the Police Stations and Higher Offices currently operational on CIPA and CCIS to CCTNS as part of the CCTNS implementation in the State/UT. SI shall validate the data in the CIPA systems and migrate the data to CCTNS. In addition, the State/UT may also decide to cover other applications currently being used under this data migration and integration effort if felt necessary.

<<SPMC shall provide the detailed list of Police Stations / Higher Offices running CIPA / CCIS along with the data to be migrated>>

4.11 Capacity Building

<<SPMC shall assist the State/UT in the following for implementation of Capacity Building part of the Bundle of Services. :>>

Identification of Trainers (Internal)

The State/UT Nodal Agency shall identify qualified Trainers with relevant IT experience and training competency within each District Mission Team and State Mission Team who will be directly trained by the System Integrator and will be responsible for interfacing with the System Integrator for all the Capacity Building Initiatives. These Trainers will be responsible for implementing the Capacity Building interventions beyond the scope of the System Integrator.

Identification of Trainers (Police Training Colleges)

The State / UT Nodal Agency shall identify the Trainers within each of the Police Training Colleges in the State / UT who will be directly trained by the System Integrator. These trainers will be responsible for including training on CCTNS within the training college curriculum and impart the training on CCTNS to the new recruits and current personnel (refresher training) at the Police Training Colleges.

Identification of Trainees

Based on the nature of their responsibilities and their requirements from CCTNS, police staff can be classified into the following categories for training purposes:

- *Group I: Identify the key senior officers (ADGP, IG, DIG) responsible for Crime, Law and Order, who are directly impacted by the CCTNS with respect to receiving/analyzing the reports through CCTNS.*
    - *Role-based training will be carried out for these officers at suitable location in the State / UT Headquarters by the System Integrator*
- *Group II: Identify the key officers (IG, DIG, SP, DCP, ACP) in charge of a zone/range/district/sub-division who are directly impacted by the CCTNS with respect to reviewing the police station performance through CCTNS, reviewing the reports generated by the system, carrying out the required analysis using CCTNS and providing the necessary guidance to the officers at the cutting edge.*
    - *Role-based training will be carried out for these officers at suitable location in the State / UT Headquarters and respective Districts/Commissionerates (if any) by the System Integrator*
- *Group III: Identify the key officers (SHO, SI, ASI,) in the Police Stations and Higher Offices who will use CCTNS for police station management, filing the necessary investigation forms, and utilize the basic and advance search features of CCTNS to facilitate their investigation process.*
    - *In addition to the computer awareness training, role-based training will be carried out for these officers at District Training Centers in the respective Districts/Commissionerates (if any) by the System Integrator*
    - *Refresher training can be carried out by the internal trainers subsequent to the System Integrator trainings*
- *Group IV: Identify at least 3-4 key officers/constables (Station Writers, Court Duty, Head Constables, Constables,) in each of the Police Stations and Higher Offices who will use CCTNS for capturing the data/investigation forms, generating the reports and utilize the*

basic and advance search features of CCTNS to service the general service requests and aid in investigation process.

- *In addition to the computer awareness training, role-based training will be carried out for the identified officers at District Training Centers in the respective Districts/Commissionerates (if any) by the System Integrator*
- *Refresher training, subsequent training to the remaining officers/constables in the Police Station and Higher Offices can be carried out by the internal trainers subsequent to the System Integrator trainings*

- *Group V: Identify 2 constables for each Circle Office that can provide the basic computer operation support to the police stations within the Circle.*
  - *Technical training will be carried out for the identified constables at District Training Centers in the respective Districts/Commissionerates (if any) by the System Integrator*

<<In case the Basic IT awareness of the Personnel is completed before the SI is on board, the same can be removed from the list of trainings to be carried out by the SI.>>

The main challenges to be addressed effectively by the SI are the geographically dispersed trainee base, wide variability in education and computer proficiency and minimal availability of time. The SI holds the responsibility for creation of a detailed and effective training strategy, user groups and classifications, training plan and guidelines, detailed training material, training program designed their delivery to the target groups.

The SI holds the responsibility for creation of training material, designing the training programs and their delivery to the target group. The State / UT SI shall be responsible for the following activities as part of the End User and Train the Trainer Training:

Develop Overall Training Plan

SI shall be responsible for finalizing a detailed Training Plan for the program in consultation with ***State / UT's Nodal Agency*** covering the training strategy, environment, training need analysis and role based training curriculum. SI shall own the overall Training plan working closely with the ***State / UT's Nodal Agency's*** Training team. SI shall coordinate overall training effort.

Develop District-Wise Training Schedule and Curriculum

SI shall develop and manage the District-Wise training schedule in consultation with ***State / UT's Nodal Agency***, aligned with the overall implementation roadmap of the project and coordinate the same with all parties involved. Training schedule shall be developed by solution and shall be optimized to reduce business impact and effective utilization of Training infrastructure and capacities. The training curriculum for the CCTNS training program should be organized by modules and these should be used to develop the training materials. The training curriculum outlines the mode of delivery, module structure and outline, duration and target audience. These sessions should be conducted such that the users of the application/modules are trained by the time the application "goes-live" in the District with possibly no more than a week's gap between completion of training and going live of modules. Continuous reporting (MIS) and assessment

should be an integral function of training. SI shall also iidentify the languages to be used by the end-user for entering data and ensuring multi-language training to the end users as per requirement.

Develop Training Material

Based on their needs and the objectives of CCTNS, training programs could be organized under the following themes:

1. Basic IT skills and use of computers to creating awareness about the benefits of ICT and basic computer skills
2. Role-based training on the CCTNS application – Basic and Advanced. This training should be in a role based, benchmarked and standardized format, multi-lingual and lead to learning completion and assessment. It should also allow for self-learning and retraining. Training would include mechanism for demonstration using audio/video/simulated/demo practice exercises and evaluation of trainees.
3. "Train the Trainer" programs, where members of the police staff would be trained to enable them to conduct further training programs, thus helping build up scalability in the training program and also reducing the dependency on external vendors for training.
4. System Administrator training: a few members of the police staff with high aptitude would be trained to act as system administrators and troubleshooters for CCTNS.
5. Customization of the Training Manuals, User Manuals, Operational and Maintenance Manuals provided along with the CCTNS CAS Software
6. Design and development of the Training Manuals, User Manuals, Operational and Maintenance Manuals for the modules developed at the State / UT level.

In cases where the training material may be made available by MHA/NCRB, it is the SI's responsibility to ensure the relevance of the material to the State/UT, customize if necessary and own up the delivery and effectiveness.

SI shall ensure that the training content meets all the objectives of the training course. The material shall be developed in English, Hindi and vernacular language. SI shall also develop the training material for delivery through Computer Based Training, Instructor Led Training, Online User Material/Help Manuals and Job Aids.

SI shall provide detailed training material providing step-by-step approach in soft and hard copies to all police stations and offices for reference.

Deliver Training to End Users

SI shall deliver training to the end users utilizing the infrastructure at the District Training Centers. Role-based training for the Senior Officers will be carried out for at suitable location in the State / UT Headquarters by the System Integrator.

SI shall also impart simulated training on the actual CAS (State) with some real life like database. The SI should create case studies and simulation modules that would be as close to the real life scenario as possible. The objective of conducting such trainings would be to give first had view of benefits of using CAS system. Such specialized training should also be able to provide the participant a clear comparison between the old way of crime and criminal investigation against the post CCTNS scenario. This training needs to be conducted by the SI at the very end when all the other trainings are successfully completed. This training may seem similar to role play training mentioned in the section above however, in this simulated training, the SI would ensure that the IO's are provided an environment that would be exactly similar at a Police Station post CAS (State) implementation.

Most of the training would be an Instructor-Led Training (ILT) conducted by trained and qualified instructors in a classroom setting. To maintain consistency across CCTNS trainings, standard templates should be used for each component of a module.

An ILT course will have the following components:

- Course Presentation (PowerPoint)
- Instruction Démonstrations (CAS - Application training environnent)
- Hands-on Exercices (CAS - Application training environnent)
- Application Simulations: Miniature version of CAS Application with dummy data providing exposure to the IOs to a real life scenario post implementation of CAS
- Job Aids (if required)
- Course Evaluations (Inquisition)

In addition to the ILT, for the modules that may be more appropriate to be conducted through a Computer Based Training (CBT), a CBT should be developed for them. CBT should involve training delivered through computers with self instructions, screenshots, simulated process walk-through and self assessment modules.

Select set of police staff with high aptitude group and/or relevant prior training, are to be imparted with the training/skills to act as system administrators and also as troubleshooters with basic systems maintenance tasks including hardware and network.

Deliver Training to Trainers (Internal and Trainers from the Training Colleges)

SI shall help ***State / UT's Nodal Agency*** in assessing and selecting the internal trainers as well as the trainers at training colleges who can conduct the end user training subsequent to the training by the SI. SI shall coordinate the 'Train the Trainer' session for the identified trainers to ensure that they have the capability to deliver efficient training.

In addition to the training delivered to the end-users, the trainers should also be trained on effectively facilitate and deliver training to end users. Also, it is advisable to always run pilots for any training program before deployment. This training will hence serve as the pilot and as a training session for trainers as well. In addition the end-user training sessions, ToT training will consist of three segments:

1. The first segment will be set of workshops covering effective presentation skills and coaching techniques and discussing the benefits and structure of the trainer model.

2. The second segment will be the formal CCTNS training which will consist of all modules of CCTNS relevant for their role.
3. The third segment will be a teach-back session where trained trainers will present course content and receive feedback regarding content, flow, and presentation techniques. This will also include a feedback session where trainers can provide feedback on the training materials, flow, comprehension level, and accuracy.

Training Effectiveness Evaluation

SI shall evaluate the effectiveness of all end users trainings using electronic or manual surveys. SI shall be responsible for analyzing the feedback and arrange for conducting refresher training, wherever needed.

State / UT will periodically monitor the training effectiveness through the performance metrics and Service levels and the SI shall comply with the same.

SI shall help the State with complete Change Management exercise needed to make this project a success. In fact Change Management will have to subsume 'training' as a key enabler for change. Following outlines the responsibilities of SI with respect to designing and implementation of change management plan for the Project.

The State Nodal Agency shall form various stakeholder groups to address the Change Management Initiative. Stakeholders are all those who need to be considered in achieving project goals and whose participation and support are crucial to its success. A key individual stakeholder or stakeholder group is a person or group of people with significant involvement and/or interest in the success of the project. Stakeholder analysis identifies all primary and secondary stakeholders who have an interest in the issues with which the CCTNS project is concerned. The stakeholder groups will be the set of core users (Change Agents) who will directly participate in the awareness and communication initiatives, workshops, and provide feedback to the District and State Mission Teams.

Change management

Stakeholder groups can be categorized into below categories, based on their influence and role in managing the change and making it successful:

- *Group I: Identify the key senior officers (ADGP, IG, DIG) responsible for Crime, Law and Order, who are directly impacted by the CCTNS with respect to receiving/analyzing the reports through CCTNS.*
- *Group II: Identify a few of the key officers (IG, DIG, DCP, ACP, SP) in charge of a zone/range/district/sub-division who are directly impacted by the CCTNS with respect to reviewing the police station performance through CCTNS, reviewing the reports generated by the system, carrying out the required analysis using CCTNS and providing the necessary guidance to the officers at the cutting edge.*
- *Group III: Identify a few of the key officers (SHO, SI, ASI,…) in the Police Stations and Higher Offices who will use CCTNS for police station management, filing the necessary investigation forms, and utilize the basic and advance search features of CCTNS to facilitate their investigation process.*

- *Group IV: Identify a few of the key officers/constables (Station Writers, Court Duty, Head Constables,…) in the Police Stations and Higher Offices who will use CCTNS for capturing the data/investigation forms, generating the reports and utilize the basic and advance search features of CCTNS to service the general service requests and aid in investigation process.*

Communication and Awareness

Communication & Awareness campaigns will be conducted throughout the duration of the implementation of the CCTNS project across the State/ UT at Project, Program level as well as for General awareness. SI shall work with the identified internal change agents (identified from the District and State Mission Teams) for all the Communication and Awareness Programs. SI shall utilize existing channels of communication and at the same time use innovative methods of communication for effectiveness. SI should ensure that the communication messages are consistent, continuous and easy to understand and wherever possible in **vernacular medium** using all available channels. SI shall align communication content, timing and delivery to the deployment phases/plan of each solution.

S. No	Activities	Details	Frequency
1	Develop detailed communication plan	• SI shall prepare a detailed communication plan for the program in line with the implementation timelines of each solution • SI shall ensure that all the impacted audience is covered in the communication plan and the most appropriate mode of communication is being used to deliver the messages to the target audience	Once
2	Develop Communication Content	• SI shall be responsible for developing the content for communication material in English, Hindi and vernacular language. • SI shall ensure that the communication is simple, continuous and consistent.	Recurring Activity over the entire duration of the SI
3	Deliver Communication Events	• Prior to implementing the plan, the SI shall obtain the necessary sign-offs from State on the Communication Strategy & plan and make necessary changes as recommended by State. • SI shall determine who needs to approve communications prior to dissemination, who is responsible for distributing the message, and who is responsible for	Recurring Activity (once a month) over the entire duration of the SI

S. No	Activities	Details	Frequency
		ensuring that those accountable for specific elements of the plan follow through on their responsibilities. • SI shall organize the communication events or interventions for the target audience. • SI shall ensure consistency between messages delivered via different interventions, since the engagement of a key individual stakeholder or stakeholder group is an integrated effort, aiming at the same objective.	

Change Management Workshops

SI shall conduct Change Management workshops build appreciation of change management and develop change leadership across the stakeholder groups. SI shall design the necessary content (reading material, presentations) in English, Hindi, and Local Language (if different) for the Change Management Workshops. SI shall conduct at least three Change Management Workshops (minimum of one-day) in the State Headquarters and at least one Change Management Workshop (minimum of one-day) all of the Districts (at the District Headquarters) covering at least 3 officers/constables (SHO, SI/ASI/HC, and Station Writer) from each police station in the district.

The SI is required to conduct the Change Management Workshops for all the identified Police personnel in a phased manner in line with the overall implementation plan. These workshops shall be conducted at the locations provided by the State. The workshop content & material shall be designed with specific focus on the requirements of the personnel. SI shall conduct workshops for each group of personnel in sync with the training plan and as part of the training module. SI is required to provide the necessary material for the workshops including presentations, training material etc in both soft and hard copy formats.

SI shall also associate and train the identified internal change agents (identified from the District and State Mission Teams) during these workshops so that subsequent workshops can be conducted by the internal change agents.

<<SPMC shall develop a suitable monitoring mechanism for this purpose>>

<<SPMC shall provide any additional requirements for specialized training such as hardware, network and any infrastructure at data centre and maintenance>>

<< SPMC to specify scope of Change management exercises as mentioned above as a part of the " Sensitization of Benefits to IT" component of Capacity building Services to be provided by SI.>>

4.12 Handholding Support

The System Integrator will provide one qualified and trained person per police station / higher office for a period of 6 months or one qualified and trained person per two police stations for a period of 1 year to handhold the staff in the police station / higher office and ensure that the staffs in that police station / higher offices are able to use CCTNS on their own by the end of the handholding period. Handholding support would be required only after the successful commissioning of Core application and the necessary infrastructure and completion of capacity building and change management initiatives in respective police stations / Higher Offices.

<<SPMC to provide a table to capture details on the engagement of handholding personnel and their resource deployment across various Police units in the State/UT>>

<<The SPMC to provide details of resource scheduling of handholding personnel across the State>>

<< SPMC also to provide code of conduct and rules for engagement of Handholding personnel for specified period by SI>>

4.13 Requirement on Adherence to Standards

CCTNS system must be designed following open standards, to the extent feasible and in line with overall system requirements set out in this RFP, in order to provide for good inter-operability with multiple platforms and avoid any technology or technology provider lock-in.

Compliance with Industry Standards

In addition to above, the proposed solution has to be based on and compliant with industry standards (their latest versions as on date) wherever applicable. This will apply to all the aspects of solution including but not limited to design, development, security, installation, and testing. There are many standards that are indicated throughout this volume as well as summarized below. However the list below is just for reference and is not to be treated as exhaustive.

Portal development	W3C specifications
Information access/transfer protocols	SOAP, HTTP/HTTPS
Interoperability	Web Services, Open standards
Photograph	JPEG (minimum resolution of 640 x 480 pixels)
Scanned documents	TIFF (Resolution of 600 X 600 dpi)
Biometric framework	BioAPI 2.0 (ISO/IEC 19784-1:2005) specification
Finger print scanning	IAFIS specifications
Digital signature	RSA standards
Document encryption	PKCS specifications
Information Security	CCTNS system to be ISO 27001 certified
Operational integrity & security management	CCTNS system to be ISO 17799 compliant
IT Infrastructure management	ITIL / EITM specifications
Service Management	ISO 20000 specifications
Project Documentation	IEEE/ISO specifications for documentation

The SI shall adhere to the standards published by the Department of Information Technology, Government of India.

4.14 Support to Acceptance Testing, Audit and Certification

The primary goal of Acceptance Testing, Audit & Certification is to ensure that the system meets requirements, standards, and specifications as set out in this RFP and as needed to achieve the desired outcomes. The basic approach for this will be ensuring that the following are associated with clear and quantifiable metrics for accountability:

1. Functional requirements
2. Test cases and Requirements Mapping
3. Infrastructure Compliance Review
4. Availability of Services in the defined locations
5. Performance and Scalability
6. Security / Digital Signatures
7. Manageability and Interoperability
8. SLA Reporting System
9. Project Documentation
10. Data Quality Review

As part of Acceptance testing, audit and certification, performed through a third party agency, State/ UT shall review 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 defined requirements, interoperability, scalability, availability and compliance with all the technical and functional requirements of the RFP and the agreement. Here it is important to mention that there may be two agencies selected by State, one for audit & certification of security and control aspect of the system and the other for audit & certification of overall application software.

State/ UT will establish appropriate processes for notifying the SI of any deviations from defined requirements at the earliest instance after noticing the same to enable the SI to take corrective action. Such an involvement of the Acceptance Testing & Certification agencies, nominated by State/ UT, will not, however, absolve the operator of the fundamental responsibility of designing, developing, installing, testing and commissioning the various components of the project to deliver the services in perfect conformity with the SLAs.

Following discusses the acceptance criteria to be adopted for system as mentioned above:

1. Functional Requirements Review

The system developed/customized by SI shall be reviewed and verified by the agency against the Functional Requirements signed-off between State/ UT and SI. Any gaps, identified as a severe or critical in nature, shall be addressed by SI immediately prior to Go-live of the system. One of the key inputs for this testing shall be the traceability matrix to be developed by the SI from system. Apart from Traceability Matrix, agency may develop its own testing plans for validation of compliance of system against the defined requirements. The acceptance testing w.r.t. the functional requirements shall be performed by both independent third party agency (external audit) as well as the select internal department users (i.e. User Acceptance Testing).

2. Infrastructure Compliance Review

Third party agency shall perform the Infrastructure Compliance Review to verify the conformity of the Infrastructure supplied by the SI against the requirements and specifications provided in the RFP and/or as proposed in the proposal submitted by SI. Compliance review shall not absolve SI from ensuring that proposed infrastructure meets the SLA requirements.

3. Security Review

The software developed/customized for system shall be audited by the agency from a security & controls perspective. Such audit shall also include the IT infrastructure and network deployed for system. Following are the broad activities to be performed by the Agency as part of Security Review. The security review shall subject the system for the following activities:

a. Audit of Network, Server and Application security mechanisms
b. Assessment of authentication mechanism provided in the application /components/ modules
c. Assessment of data encryption mechanisms implemented for the solution
d. Assessment of data access privileges, retention periods and archival mechanisms
e. Server and Application security features incorporated etc

4. Performance

Performance is another key requirement for system and agency shall review the performance of the deployed solution against certain key parameters defined in SLA described in this RFP and/or agreement between State / UT and SI. Such parameters include request-response time, work-flow processing time, concurrent sessions supported by the system, Time for recovery from failure, Disaster Recovery drill etc. The performance review also includes verification of scalability provisioned in the system for catering to the requirements of application volume growth in future.

5. Availability

The system should be designed to remove all single point failures. Appropriate redundancy shall be built into all the critical components to provide the ability to recover from failures. The agency shall perform various tests including network, server, security, DC/DR fail-over tests to verify the availability of the services in case of component/location failures. The agency shall also verify the availability of services to all the users in the defined locations.

6. Manageability Review

The agency shall verify the manageability of the system and its supporting infrastructure deployed using the Enterprise Management System (EMS) proposed by the SI. The manageability requirements such as remote monitoring, administration, configuration, inventory management, fault identification etc. shall have to be tested out.

7. SLA Reporting System

SI shall design, implement/customize the Enterprise Management System (EMS) and shall develop any additional tools required to monitor the performance indicators listed under SLA prescribed in this RFP. The Acceptance Testing & Certification agency shall verify the accuracy and completeness of the information captured by the SLA monitoring system implemented by the SI and shall certify the same. The EMS deployed for system, based on SLAs, shall be configured to calculate the monthly transaction-based payout by STATE/UT / UTState to SI.

8. Project Documentation

The Agency shall review the project documents developed by SI including requirements, design, source code, installation, training and administration manuals, version control etc. Any issues/gaps identified by the Agency, in any of the above areas, shall be addressed to the complete satisfaction of State / UT.

9. Data Quality

The Agency shall perform the Data Quality Assessment for the Data digitized/ migrated by SI to the system. The errors/gaps identified during the Data Quality Assessment shall be addressed by SI before moving the data into production environment, which is a key mile stone for Go-live of the solution.

<< SI shall only provide requisite support and coordinate with the State/UT Department for Audit, User acceptance and Certification>>

4.15 Scope of Services during Post-Implementation Phase

The SI shall be responsible for the over all management of the system including the application and entire related IT Infrastructure. The details of the post implementation support services are provided as an Annexure to this RFP. SI shall develop / procure and deploy an EMS tool that monitors / manages the entire enterprise wide application, infrastructure and network related components.

SI shall provide the Operations and Maintenance Services for period of <<5>> years following the deployment and "Go-Live" of the solution in the State / UT**. In case each District is declared as "Go-Live" at different instances during the project roll-out, the Operations and Maintenance Services for the District will start following the deployment and "Go-Live" of the solution in the District and SI shall continue to provide the Operations and Maintenance Support for a period of <<5>> years following the deployment and "Go-Live" of the solution in the last District.**

5 Implementation and Roll-Out Plan

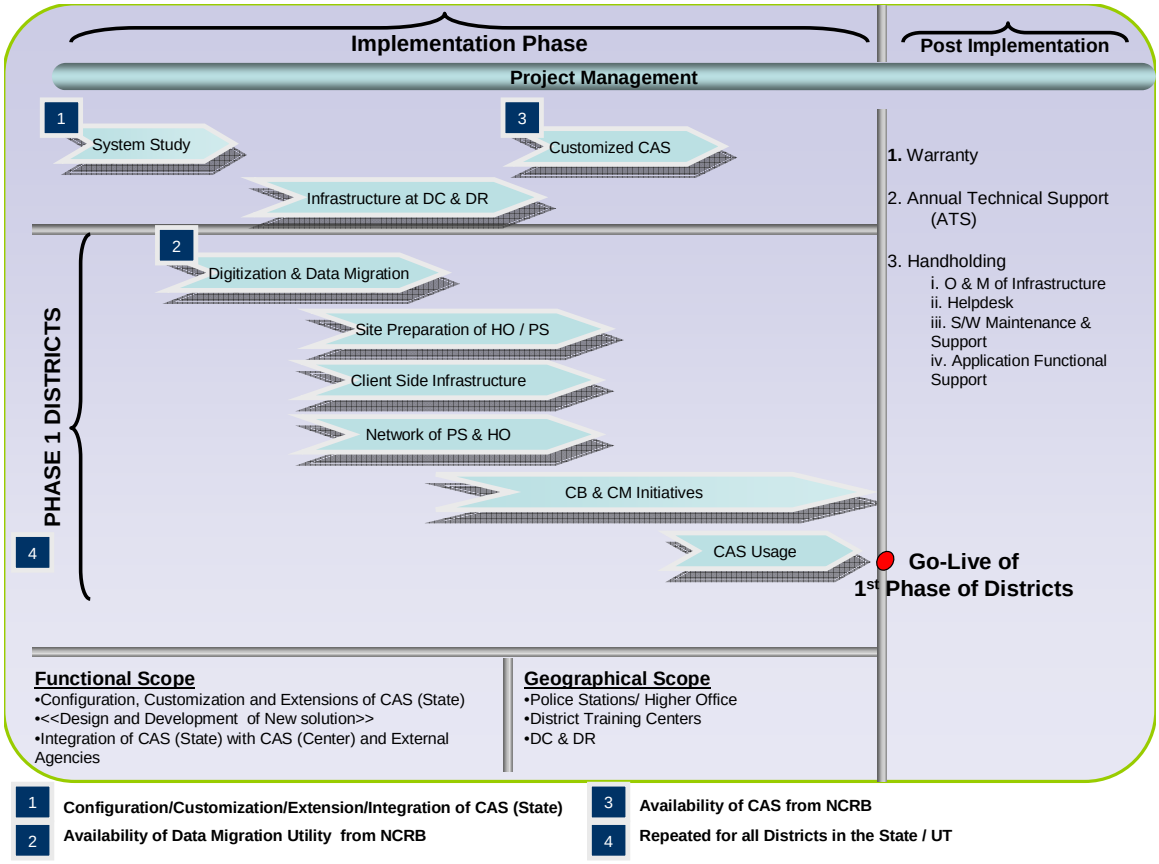
<<The State/ UT needs to provide the implementation and roll-out plan for the solution. SPMC in coordination with the State/UT to define the overall timelines for implementation and roll-out as per PIM report assessment)>> It is suggested that the solution be piloted in a few police stations in one or two districts/Commissionerates (if any) and the feedback incorporated before rolling out across the State / UT. The rollout plan shall be defined date-wise, location-wise, module-wise and training completion and change management completion wise. A detailed rollout checklist should be maintained for migrating application to production as well as for location readiness.

SI shall prepare a detailed roll-out plan for each of the Districts in the Phase and get the same approved by the State/UT. SI is also responsible for conducting workshops for the key officers (State Mission Team, District Mission Team, and District Core Team) of the Districts / State for presenting the District-Wise roll-out plan and get the approval from the District Teams before getting the final approval of the State Nodal Officer. The SI shall also provide the necessary assistance for the key officers (State Mission Team, District Mission Team, and District Core Team) of the Districts / State during the design and implementation of CCTNS in the State / UT.

One of the important factors that would determine the success of the CCTNS implementation in the State / UT is the continuous availability of domain experts to the implementation team. SI shall put together a team of domain experts with a minimum of 10 years of experience in the State/UT Police Department who will work on this project on a full time basis during the entire duration of the project.

List of Indicative Deliverables:

1. Overall Project Plan
2. CAS Configuration / Customization / Extension
    a. Requirements Traceability Matrix
    b. Refined Functional Requirements Specification
    c. Systems Requirement Specification
    d. Design Document (High Level Design and Low Level Design)
    e. Test Plans
    f. CAS Configuration / Customization / Extension Document
    g. Change / Reference Document documenting changes to the base version of CAS (State)
3. Network Connectivity
    a. Network Architecture
    b. Network diagrams (LAN and WAN) for PS / HO to State DC / DRC
    c. Network diagrams for connectivity between State DC / DRC to NCRB DC / DRC



4. Data Migration Strategy and Methodology including Detailed Data Migration Plan
5. Change Management and Capacity Building
    a. Overall Change Management Plan
    b. Content for Change Management including Awareness and Communications Program
    c. Overall Capacity Building Plan and District-wise Training Schedule and Curriculum
    d. Training Material
6. District-wise Roll-out / Implementation Plans

Service Levels

This section describes the service levels to be established for the Services offered by the SI to State / UT. The SI shall monitor and maintain the stated service levels to provide quality service to State / UT. The Service levels are provided in Annexure-III of this RFP.

ANNEXURE I: Details of Technology Stacks - CAS (State) and CAS (Center)

CAS (State) will be developed in two distinct technology stacks by the SDA at the Center.

The Technical Details for CAS (State) Solution Stack 1 and Stack2, CAS (State) Offline solution, CAS (Centre) Solution are provided in subsequent tables:

CAS (State) Solution - Stack 1

	Proposed Solution by Software Development Agency	Version and Year of Release	Original Supplier	Description (include major features/ services only)	Support Provided By
Web server	Sun Java System Web Server 7.0	7.0	SUN	HTTP Server	SUN
Application Server	Glassfish Application Server	3.0	SUN	J2EE Application Server	SUN
Database	MySQL	5.1	SUN	DB Store	SUN
Operating System	Solaris	10	SUN	Operating System	SUN
Others					
Reporting Engine	Jasper Reports	3.7	Jasper	Reporting Services	
Email/Messaging	Q-Mail	1.4	Qmail Community	E-Mail Solution	
Search Engine	Search: Unstructured data: using openCMS search features Structured Data MySQL & Custom application interface	N/a	N/a	N/a	N/a
Portal Server	Glassfish Application Server	3.0	SUN	J2EE Application Server	SUN

	Proposed Solution by Software Development Agency	Version and Year of Release	Original Supplier	Description (include major features/ services only)	Support Provided By
Workflow Engine	jBPM	4.0	JBoss	Workflow engine	
Rules Engine	Custom Built	N/a	N/a	N/a	N/a
Directory Services	Sun Directory Services	7.0	SUN	LDAP	SUN
DMS/CMS	openCMS	7.5.1	OpenCMS	Content Management System	
Security	Physical Security, Network Sercurity, DB Encryption (MySQL), DB Access Controls, Role Based Access Control (Custom Developed), LDAP (Sun Directory Services),	N/a	N/a	N/a	N/a
Identity Management	OpenSSO	7.0	SUN	LDAP	SUN
Audit	log4j, Custom Built application audit	N/a	N/a	N/a	N/a
ETL	Custom Built	N/a	N/a	N/a	N/a

CAS (State) Solution - Stack 2

	Proposed Solution by Software Development Agency	Version and Year of Release	Original Supplier	Description (include major features/ services only)	Support Provided By
Webserver	IIS	6	Microsoft	Web & App Server	Microsoft
Application Server	IIS	6	Microsoft	Web & App Server	Microsoft
Database	SQL Server 2008	2008	Microsoft	DB Store	Microsoft
Operating System	Windows Server 2008	2008	Microsoft	Operating System	Microsoft
Others					Microsoft
Reporting Engine	SQL Server Reporting Services	2008	Microsoft	Reporting Services	Microsoft
Email/Messaging	Q-Mail	1.4	Qmail Community	E-Mail Solution	
Search Engine	Search: Unstructured data: using openCMS search features Structured Data: SQL DB Search Engine & Custom application interface	N/a	N/a	N/a	N/a
Portal Server	IIS	6	Microsoft	Web & App Server	Microsoft
Workflow Engine	Windows Workflow Foundation	N/a	N/a	N/a	N/a
Rules Engine	Custom Built	N/a	N/a	N/a	N/a
Directory Services	Microsoft Active Directory	2008	Microsoft	LDAP	Microsoft
DMS/CMS	Windows SharePoint Services	n/a	n/a	n/a	Microsoft

	Proposed Solution by Software Development Agency	Version and Year of Release	Original Supplier	Description (include major features/ services only)	Support Provided By
Security	Physical Security, Network Sercurity, DB Encryption (MySQL), DB Access Controls, Role Based Access Control (Custom Developed), LDAP (Sun Directory Services),	N/a	N/a	N/a	N/a
Identity Management	Microsoft Active Directory	2008	Microsoft	LDAP	Microsoft
Audit	IIS Log, Custom Built	N/a	N/a	N/a	N/a
ETL	SQL Server ETL	2008	Microsoft	ETL	Microsoft

CAS (State) Offline Solution

The below list is indicative only	Proposed Solution by Software Development Agency	Version and Year of Release	Original Supplier	Description (include major features/ services only)	Support Provided By
Synchronization Solution	Custom Built	N/a	N/a	N/a	N/a
Application Container	Apache Tomcat	6.0	Apache Foundation	J2EE Application Container	
Database	MySQL / SQL Express	5.1/2008	SUN / Microsoft	DB Store	SUN / Microsoft

CAS (Center) Solution

The below list is indicative only	Proposed Solution by Software Development Agency	Version and Year of Release	Original Supplier	Description (include major features/ services only)	Support Provided By
Webserver	Sun Java System Web Server 7.0	7.0	SUN	HTTP Server	SUN
Application Server	Glassfish Application Server	3.0	SUN	J2EE Application Server	SUN
Database	Sybase IQ Enterprise	15.1	Sybase	ETL	Sybase
Operating System	Solaris				
Others					
Reporting Engine	Jasper Reports	3.7	Jasper	Reporting Services	
Search Engine	Search: Unstructured data: using Alfresco search features Structured Data: Sybase DB Search Engine & Custom application interface	N/a	N/a	N/a	N/a
Portal Server	Glassfish Application Server	7.0	SUN	HTTP Server	SUN
Workflow Engine	jBPM	4.0	JBoss	Workflow engine	
Rules Engine	Custom Built	N/a	N/a	N/a	N/a
Directory Services	Sun Directory Services	7.0	SUN	LDAP	SUN
DMS/CMS	Alfresco				
Email/Messaging	N/A				

The below list is indicative only	Proposed Solution by Software Development Agency	Version and Year of Release	Original Supplier	Description (include major features/ services only)	Support Provided By
Security	Physical Security, Network Sercurity, DB Encryption (MySQL), DB Access Controls, Role Based Access Control (Custom Developed), LDAP (Sun Directory Services),	N/a	N/a	N/a	N/a
Identity Management	Open SSO	7.0	SUN	LDAP	SUN
Audit	log4j, Custom Built	N/a	N/a	N/a	N/a
ETL + Data Quality	Sybase ETL	15.1	Sybase	ETL	Sybase

ANNEXURE II : Post Implémentation Support Services

As part of the post implementation services, the SI shall provide support for the software, hardware, and other infrastructure provided as part of this RFP. SI shall provide <<five (5)>> years of comprehensive AMC that includes

1. Warranty support
2. Annual Technical Support (ATS)
3. Handholding Services
    a. Operations and maintenance services for the server and related infrastructure supplied and commissioned by the SI for the application at the Data Center and Disaster Recovery Center.
    b. Central Helpdesk from the State / UT designated premises.
    c. Support for the end users at each of the locations including deployment of one competent person at each police station for a period of six months to handhold the staff after the Core application and the necessary infrastructure are successfully commissioned in the police stations.
    d. Software maintenance and support services.
    e. Application functional support services

The services shall be rendered onsite from the State/UT designated premises. To provide the support for the police stations, circle offices, sub-divisional offices, district headquarters / Commissionerates, ranges, zones, State/UT police headquarters and other locations across the State / UT where the software, hardware, and other infrastructure will be rolled out, SI is expected to provide experienced and skilled personnel at each location. The SI shall develop a work plan for the knowledge sharing as per scope defined in this RFP for use in future phases of the project.

As part of the warranty services SI shall provide:

1. SI shall provide a comprehensive warranty and on-site free service warranty for 5 years from the date of Go Live.
2. SI shall obtain the five year product warranty and five year onsite free service warranty on all licensed software, computer hardware and peripherals, networking equipments and other equipment.
3. SI shall provide the comprehensive manufacturer's warranty in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. covered by the RFP. SI must warrant all hardware, equipment, accessories, spare parts, software etc. procured and implemented as per this RFP against any manufacturing defects during the warranty period.
4. SI shall provide the performance warranty in respect of performance of the installed hardware and software to meet the performance requirements and service levels in the RFP.
5. SI is responsible for sizing and procuring the necessary hardware and software licenses as per the performance requirements provided in the RFP. During the warranty period SI shall

replace or augment or procure higher-level new equipment or additional licenses at no additional cost to the State / UT in case the procured hardware or software is not adequate to meet the service levels.

6. Mean Time between Failures (MTBF) If during contract period, any equipment has a hardware failure on four or more occasions in a period of less than three months or six times in a period of less than twelve months, it shall be replaced by equivalent or higher-level new equipment by the SI at no cost to State/ UT. However, if the new equipment supplied is priced lower than the price at which the original item was supplied, the differential cost should be refunded to State / UT. For any delay in making available the replacement and repaired equipments for inspection, delivery of equipments or for commissioning of the systems or for acceptance tests / checks on per site basis, State / UT reserve the right to charge a penalty.
7. During the warranty period SI shall maintain the systems and repair / replace at the installed site, at no charge to State / UT, all defective components that are brought to the SI's notice.
8. The SI shall as far as possible repair the equipment at site.
9. In case any hard disk drive of any server, SAN, or client machine is replaced during warranty / AMC the unserviceable HDD will be property of State / UT and will not be returned to SI.
10. Warranty should not become void, if State / UT buys, any other supplemental hardware from a third party and installs it within these machines under intimation to the SI. However, the warranty will not apply to such supplemental hardware items installed.
11. The SI shall carry out Preventive Maintenance (PM), including cleaning of interior and exterior, of all hardware and testing for virus, if any, and should maintain proper records at each site for such PM. Failure to carry out such PM will be a breach of warranty and the warranty period will be extended by the period of delay in PM.
12. SI shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.
13. The SI shall ensure that the warranty complies with the agreed Technical Standards, Security Requirements, Operating Procedures, and Recovery Procedures.
14. SI shall have to stock and provide adequate onsite and offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met.
15. Any component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA).
16. The SI shall develop and maintain an inventory database to include the registered hardware warranties.

As part of the ATS services SI shall provide:

1. SI shall maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements and maintenance.
2. If the Operating System or additional copies of Operating System are required to be installed / reinstalled / de-installed, the same should be done as part of ATS.
3. SI should carry out any requisite adjustments / changes in the configuration for implementing different versions of Application Software.

4. Updates/Upgrades/New releases/New versions. The SI shall provide from time to time the Updates/Upgrades/New releases/New versions of the software and operating systems as required. The SI should provide free upgrades, updates & patches of the software and tools to State / UT as and when released by OEM.
5. SI shall provide patches to the licensed software including the software, operating system, databases and other applications.
6. Software License Management. The SI shall provide for software license management and control. SI shall maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements, and maintenance.
7. SI shall provide complete manufacturer's technical support for all the licensed software problems and/or questions, technical guidance, defect and non-defect related issues. SI shall provide a single-point-of-contact for software support and provide licensed software support including but not limited to problem tracking, problem source identification, problem impact (severity) determination, bypass and recovery support, problem resolution, and management reporting.
8. The manufacturer's technical support shall at a minimum include online technical support and telephone support during the State / UT's business hours (Business hours in State / UT will be from 0830 hours to 2030 hours on all days (Mon-Sun)) with access for State / UT and SI to the manufacturer's technical support staff to provide a maximum of 4 hour response turnaround time. There should not be any limits on the number of incidents reported to the manufacturer. State / UT shall have access to the online support and tools provided by the manufacturer. State / UT shall also have 24x7 access to a variety of technical resources including the manufacturer's knowledge base with complete collections of technical articles.

As part of the Handholding services to provide Operations and maintenance support for the server and related infrastructure supplied and commissioned by the SI for the application at the Data Center and Disaster Recovery Center SI shall provide:

1. The scope of the services for overall IT infrastructure management as per ITIL framework shall include 365x24x7 on site Monitoring, Maintenance and Management of the server and related infrastructure supplied and commissioned by the SI for the application at the Data Center and Disaster Recovery Center. The business hours in State / UT will be from 0830 hours to 2030 hours on all days (Mon-Sun). SI will plan these services accordingly. The SI shall provide the MIS reports for all the devices installed in the Data Center and Disaster Recovery Center in format and media as mutually agreed with the State / UT on a monthly basis. Whenever required by State / UT, SI should be able to provide additional reports in a pre-specified format. The indicative services as part of this support are as below:
    (a) System Administration, Maintenance & Management Services
    (b) Application Monitoring Services
    (c) Network Management Services
    (d) Backend Services (Mail, messaging, etc)
    (e) Storage Administration and Management Services
    (f) IT Security Administration Services and Services for ISO 27001 and ISO 20000 compliance

(g) Backup and Restore Services

As part of the Handholding services to provide Centralized Helpdesk and Support for end users at each location SI shall provide:

1. The service will be provided in the local language of the State / UT.
2. The help desk service that will serve as a single point of contact for all ICT related incidents and service requests. The service will provide a Single Point of Contact (SPOC) and also resolution of incidents. State / UT requires the SI to provide Help Desk services to track and route requests for service and to assist end users in answering questions and resolving problems related to the software application, network, Data Center, Disaster Recovery Center, Client side infrastructure, and operating systems at all locations. It becomes the central collection point for contact and control of the problem, change, and service management processes. This includes both incident management and service request management.
3. SI shall provide a second level of support for application and technical support at police stations, circle offices, sub-divisional offices, district headquarters / Commissionerates (if any), range offices, zonal offices, state / UT police headquarters and other locations across the State / UT where the software, hardware, and other infrastructure will be rolled out.
4. For all the services of State / UT within the scope of this RFP, SI shall provide the following integrated customer support and help.
5. Establish 16X6 Help Desk facility for reporting issues/ problems with the software, hardware and other infrastructure.
6. SI shall maintain and support to all client side infrastructure including hardware, networking components, and other peripherals.
7. SI shall provide maintenance of Hardware, including preventive, scheduled and predictive Hardware support, as well as repair and / or replacement activity after a problem has occurred.
8. SI shall track and report observed Mean Time Between Failures (MTBF) for Hardware.
9. SI shall provide functional support on the application components to the end users.
10. SI shall also provide system administration, maintenance and management services, LAN management services, and IT security administration services.

As part of the Handholding services to provide software maintenance and support services SI shall provide:

1. The Software Maintenance and Support Services shall be provided for all software procured and implemented by the SI. The SI shall render both on-site and off-site maintenance and support services to State / UT to all the designated locations. The Maintenance and Support Services will cover, all product upgrades, modifications, and enhancements.
2. Updates/Upgrades/New releases/New versions. The SI will implement from time to time the Updates/Upgrades/New releases/New versions of the software and operating systems as required after necessary approvals from State / UT about the same.
3. Tuning of application, databases, third party software's and any other components provided as part of the solution to optimize the performance.

4. The SI shall apply regular patches to the licensed software including the operating system and databases as released by the OEMs.
5. Software Distribution. SI shall formulate a distribution plan prior to rollout and distribute/install the configured and tested software as per the plan.
6. Software License Management. The SI shall provide for software license management and control. SI shall maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements, and maintenance. SI should perform periodic audits to measure license compliance against the number of valid End User software licenses consistent with the terms and conditions of site license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions and report to State / UT on any exceptions to SI terms and conditions, to the extent such exceptions are discovered.
7. The SI shall undertake regular preventive maintenance of the licensed software.

As part of the Handholding services to provide application functional support services SI shall provide:

1. The Application Functional Support Services shall be provided for all software procured and implemented by the SI. The SI shall render both on-site maintenance and support services to State / UT from the development center in State / UT.
2. Enhancements and defect fixes. SI shall incorporate technological changes, and provide enhancements as per the requests made by State / UT. SI shall perform minor changes, bug fixes, error resolutions and minor enhancements that are incidental to proper and complete working of the application.
3. Routine functional changes that include user and access management, creating new report formats, and configuration of reports.
8. SI shall provide user support in case of technical difficulties in use of the software, answering procedural questions, providing recovery and backup information, and any other requirement that may be incidental/ancillary to the complete usage of the application.
9. The SI shall migrate all current functionality to the new / enhanced version at no additional cost to State / UT and any future upgrades, modifications or enhancements.
10. The SI shall perform user ID and group management services.
11. The SI shall maintain access controls to protect and limit access to the authorized End Users of the State / UT.
12. The services shall include administrative support for user registration, creating and maintaining user profiles, granting user access and authorization, providing ongoing user password support, announcing and providing networking services for users and providing administrative support for print, file, directory and e-mail servers.

Exit Management and Transition – Capacity Building at State/UT

After the exit of the SI, State/UT shall take up the management of CAS (State). Therefore before the exit of the SDA, State/UT must be strengthened and capacity must be developed for State/UT to manage CAS. The SI must plan the capacity building initiative to enable State/UT manage CAS, and will collaborate with State/UT to implement the plan.

The SI shall create a detailed plan for Capacity Building (CB) required at State/UT to manage CAS and a Transition Plan (implemented over a minimum period of three months) to affect the handover to State/UT; and implement the same in collaboration with State/UT before the completion of their engagement.

ANNEXURE III: Service Levels

The above list of Service levels is indicative. The State / UT should add more service levels / modify the above service levels as per their requirements.

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

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 state / UT.

(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 state / UT 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 state / UT 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.

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 state / UT. The SI however recognizes the fact that the state / UT 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 state / UT or an agency designated by them, then the state / UT 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 state / UT suggested format and a review shall be conducted based on this report. A monthly Availability and Performance Report shall be provided to the state / UT 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 state / UT upon review and signoff by both SI and the state / UT. 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 state / UT 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 state / UT and will be performed by the state / UT or the state / UT 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 state / UT on a monthly basis. The tool should also be capable of generating SLA reports for a half-year. The state / UT 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 state / UT decides after taking the advice of the SI and other agencies. All the changes would be made by the state / UT 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 state / UT 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 state / UT 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. Capacity Building

Service Level Description	Measurement
Capacity Building	At least 80% of the trainees within the training program should give a rating of satisfactory or above. Severity of Violation: High This service level will be monitored and measured on a per District basis through feedback survey to be provided to each attendee within the program. 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	Error rate in a batch should be less than 5%. Severity of Violation: Medium This service level will be measured on a monthly basis for each Police Station / Higher Office. If the data migration / digitization service level in a police station / higher office falls below the minimum service level, it will be treated as

Service Level Description	**Measurement**
	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		
1.	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
2.	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	State / UT may conduct independent audit to verify that the data center is as per the specifications.
3.	Capacity building	At least 80% of the training audience should give a rating of satisfactory or above	Less than 80% and more than 60% attendees find the training satisfactory	Rs. 15,000 / training session	Less than 60% of the attendees find the training satisfactory	Rs. 25,000 per training session	Feedback survey to be provided to each attendee	The feedback of the attendees must be taken after every training session and this feedback should be leveraged for improving the

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		
								capacity building program

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		
4.	Data Digitization	Error rate in a batch during verification should be less than 5%	Error rate between 5% - 10%	Rs. 5,000 / batch and correction of records	Error rate of over 10%.	Rs. 10,000 / batch and the entire batch to be re-done	Error rate in a batch during verification	Error rate is measured by percentage of the records with corrections marked by designated officials
5.	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	
6.	***The above list of Service levels is indicative. The State / UT should add more service levels / modify the above service levels as per their requirements***							

<<The above framework for Service levels including penalties is indicative. The SPMC can add more service levels for measuring the performance of the services delivered by SI>>

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.

<< Based on the above framework and in consultation with the State/UT, SPMC to define the penalties and the severity of violation>>

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 state / UT'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 state / UT'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 state / UT'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 state / UT'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
Infrastructure Availability	Availability of production CAS systems shall be at least 99% Severity of Violation: High

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>
<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 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 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

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</td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>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 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></table></td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>
<table>
<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 99.9%

Severity of Violation: High

This service level will be monitored on a monthly basis.</td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>
<table>
<tr><td>Availability over the six-month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>< 99.9% & >= 99.5%</td><td>1</td></tr>
<tr><td>< 99.5% & >= 99%</td><td>2</td></tr>
<tr><td>< 99%</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.

Severity of Violation: High

The list of critical business functions and peak usage hours will be identified by the state / UT during the Supply and System Integration Phase.</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>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. <u>Client Site Infrastructure Systems</u>

(a) **<u>Critical Client Site Systems</u>**. 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%

Service Level Description	Measurement
	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 Incident**. The incident has an immediate impact on the state / UT'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 state / UT'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 state / UT and SI.

(d) The scheduled operation time for the client site systems shall be the business hours of the state / UT.

(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 state / UT. 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 state / UT'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 state / UT'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 state / UT'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 state / UT 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 for each such month to the overall violations for this service level.</td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td></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. Network Uptime:

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 state / UT'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 state / UT'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 state / UT'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 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. Performance over the six- | Violations for calculation of

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>
<table>
<tr><td>month period</td><td>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>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><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>98% of the non SI supported incidents shall be routed to the appropriate service provider within 30 minutes.

Severity of Violation: Medium

This service level will be monitored on a monthly basis.</td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>
<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 for any incident of this nature shall not exceed 48 hours.</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>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-month period falls below 60%, one (1) additional violation will be added</td></tr>
</table>

Service Level Description	Measurement
	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 state / UT. 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.

Service Level Description	Measurement

<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. <u>Credits for Successful Application Uptake</u>

The below tables gives details of the credits that can gain by the SI for successful uptake of the application in the State/UT. The credits will not be calculated for the first 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": 1. Number of key transactions carried through internet (ex:

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>
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 Charge Sheets 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:

(v) 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.

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

i. 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.
ii. 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).

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

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

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

(x) 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

(xi) 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

(xii) 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

(xiii) 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 state / UT shall have the right to terminate the contract.

ANNEXURE IV : Governance Structure (State/UT Level)

The following governance committees, recommended by DIT shall review progress, implementation, and rollout, shall monitor utilization of funds and issue Policy Directions/Guidelines for CCTNS project at the State level.

- State Apex Committee
- State Empowered Committee
- State Mission Team
- District Mission Team

The committees are to be formed as per the guidelines below. It is requested that after the states form all teams for implementation, they inform the details to MHA/NCRB.

State Apex Committee

This committee will be headed by the Chief Secretary and will be responsible for following:

- Review progress of project
- Monitor utilization of funds
- Issue of Policy Directions
- Issue of Guidelines etc.

The suggested composition of **State Apex Committee** is as following:

Members	**Composition Suggested**
Member 1 (Chairperson)	Chief Secretary
Member 2 (Co-Chair)	Principal Home Secretary
Member 3	Secretary Finance
Member 4	IT Secretary
Member 5	Head of SCRB
Member 6	Representative of NIC
Member 7	Representative of GOI, MHA
Member 8 (Convener)	Nodal Officer (CCTNS Project)
Member 9	Any other member co-opted from the field of IT, Telecom, etc.

Frequency of Meeting: Once in a quarter

State Empowered Committee

This Committee will be headed by the DGP and will be responsible for following:

- Allocation of funds
- Approval of BPR (Business Process Reengineering) proposals.
- Sanction for various project components, as may be specified, including the Hardware/Software procurement.
- Approval of various functionalities to be covered in the Project.
- Review progress of the Project.
- Ensure proper Training arrangements.
- Ensure deployment of appropriate handholding personnel.
- Other important policy and procedural issues.
- Guidance to State/District Mission Teams.

The suggested Composition of State Empowered Committee is as following:

Members	Composition Suggested
Member 1 (Chairperson)	**DGP**
Member 2 (Co-Chair)	**Head of SCRB**
Member 3	**Representative of NCRB**
Member 4	**Representative of Home Department at State level**
Member 5	**Representative of Finance at State level**
Member 6	**Director e-governance or representative of IT Department**
Member 7	**NIC representative at State Level**
Member 8	**Representative of State Implementation agency**
Member 9 Nodal Officer as Convener	**ADGP/IG level office as nominated by DGP**
The Committee may co-opt any other member whenever, felt necessary.	

Frequency of Meeting: Once a month

State / UT Mission Team

The State/UT Mission Team will be headed by the Nodal Officer for CCTNS Project/Head of SCRB, whoever is senior. The State/UT Mission Team will be responsible for following:

- Operational responsibility for the Project.
- Formulating Project Proposals.
- Getting sanction of GOI for various projects.
- Hardware rollout and commissioning
- Co-ordination with various agencies.
- Resolution of all software related issues, including customization.
- Resolution of all other issues hindering the Project Progress.
- Any other decision to ensure speedy implementation of the project.
- Assist the State Apex and Empowered Committees

The suggested composition of State Mission Team is as following:

Members	**Composition Suggested**
Member 1 (Mission Leader)	**Nodal Officer**
Member 2	**Head of SCRB**
Member 3	**Head of Implementing Agency**
Member 4	**State Informatics Officer (SIO), NIC**
Nodal Officer/ Head of SCRB, whoever is senior will be the Mission Leader	

Frequency of meeting: Once a month

District Mission Team

The **District Mission Team** will be headed by the SSP/SP of the respective district and will perform the following functions:

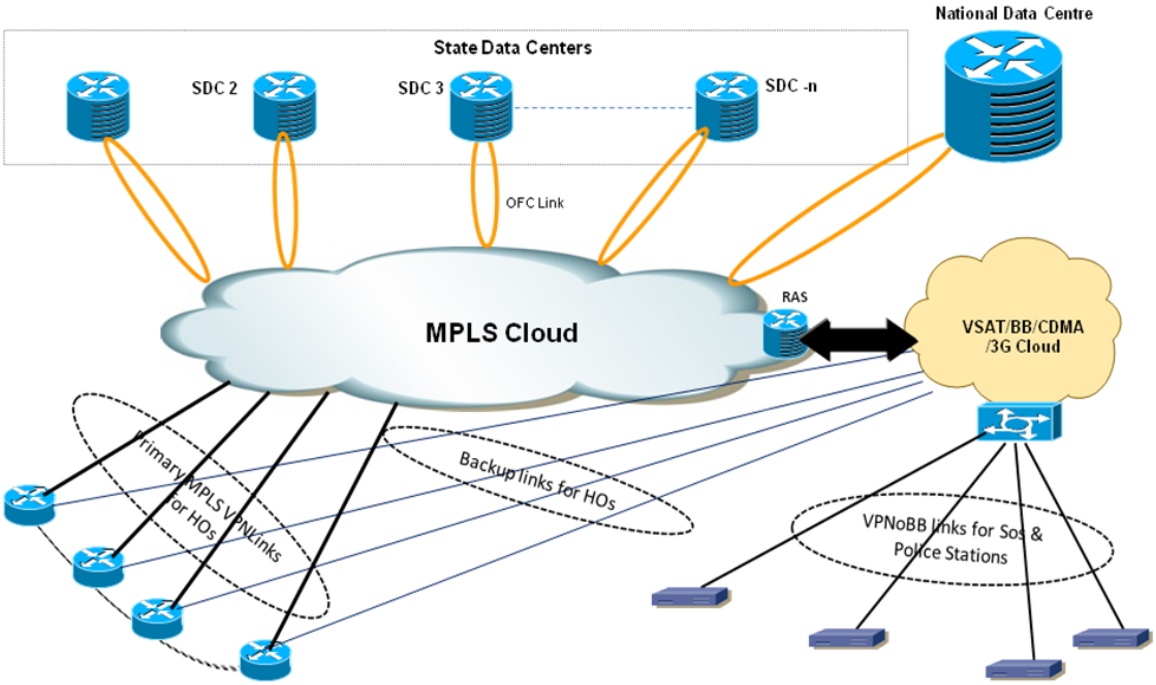
- Prepare District Project Proposal.
- Ensure proper Rollout of the Project in each selected Police Station.
- Ensure hardware and software installation, and operationalization of the Project.
- Training of all police personnel in the District.
- Site preparation and availability of all utilities.
- Ensure separate account keeping for the Project.
- Appointment and proper utilization of handholding personnel.

The suggested composition of **District Mission Team** will have the following members**:**

Members	**Composition Suggested**
Member1 (Chairperson)	**SSP/SP of the District**
Member 2 (Convener) Convener	**One officer of DCRB**
Member 3	**DIO of the NIC District Centre**
Member 4	**One officer from District Police having computer knowledge**

Frequency of meeting: Once a month

ANNEXURE V: Network Connectivity Solution



- It has been decided that connectivity for all the police stations and higher offices will be provided by BSNL.
- MPLS network to connect 2,000 higher offices and the remaining 18,000 sites to be connected through VPN on Broadband.
- SWAN will be the backup network wherever available
- The network will ultimately graduate to MPLS for all sites with SWAN as backup
- SLA of 99% uptime would be provided for MPLS connectivity. SLA for the sites connected through VPN on Broadband will be 97%

Annexure VI: Indicative Technical Specifications

Minimum Technical Specifications Requirement at State/UT Data Center & Disaster Recovery Site

1. Enterprise Management and Monitoring Solution (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 Nodes 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. 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

3. 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

4. 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 (Intel / AMD 64) – 2 nos. (min)

- 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
- At least 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.

5. Storage and Backup Solution

SAN Switches – 2 nos.

- 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 – 1 no.

- **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 (SPMC to assess as per State requirement) 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 - 1

Tape drives

- Minimum 2 latest generation LTO drives. The State can size for more as per their 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 ……. and should be a 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 – 2 nos.

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.

6. Desktops

a. High end Desktop

Intel® Core™ i5-650/ i5-750 Processor (4M Cache, 3.20 GHz) or above, RAM 4GB.

b. Low end Desktop

Intel® Core™2 Duo Processor E4400 (2M Cache, 2.00 GHz, 800 MHz FSB) or above, RAM 2GB. The system to support browser based application via IE/Mozilla

<< All the above technical specifications are indicative. The SPMC shall provide specifications based on the PIM report assessment in line with MHA guidelines. SPMC shall also provide specifications in the RFP to enable the SI to provide hardware/IT infrastructure items of latest specifications available in the market. SPMC should ensure that specifications to be provided shall not lead to the supply of end of life cycle or outdated products>>

<<SPMC shall also propose suitable models of deployment architecture at the Police Station/Higher office level in line with budgetary considerations and the PIM report assessment in consultation with State/UT. SPMC with approval of the State/UT may explore such options for deployment solutions and propose the same for implementation of hardware and IT infrastructure components. >>

<< SPMC to provide a detailed Bill of Materials Table for all the hardware and infrastructure items for enabling SI to respond with relevant information in the bid process>>