E-GOVERNANCE

MISSION MODE PROJECT (MMP)

CRIME & CRIMINAL TRACKING NETWORK AND SYSTEMS (CCTNS)

DRAFT MODEL RFP TEMPLATE FOR STATE – SYSTEM INTEGRATOR

IMPLEMENTATION OF CCTNS IN <<STATE / UT>>

VOLUME – I: FUNCTIONAL AND TECHNICAL SPECIFICATIONS

(Draft v2.0, 23rd August 2010)

MINISTRY OF HOME AFFAIRS
GOVERNMENT OF INDIA

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

TABLE OF CONTENTS

1. INTRODUCTION

1.1. PROJECT BACKGROUND

Availability of relevant and Timely information is of utmost necessity 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 the two GOI-led initiatives.

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 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.

1.3.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 citizen's interface to provide basic services to citizens.

1.4.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

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

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. Please refer to Annexure 3), managing (from a high level) and monitoring the program. 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.

1.5. GOALS OF THIS REQUEST FOR PROPOSAL (RFP)

The primary goal of this RFP is to serve as a framework or a model for the 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

Vision: To transform the police force into a knowledge-based force and improve the delivery of citizen-centric services through enhancing the efficiency and effectiveness of the police stations by creating a platform for sharing crime and criminal information across the police stations in the country.

The overall objective of the MMP is based on enhancing the operational efficiency and effectiveness of the police force in delivering the services.

The broad objectives of the project are as follows:

a) Improve Service Delivery to the Public

Citizens should be able to access police services through multiple, transparent, and easily accessible channels 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.

b) 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.

c) 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.

d) 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

- Non-Government/Private sector organizations

2.4. DESIRED OUTCOMES FROM VARIOUS STAKEHOLDERS

The following are the expected benefits envisaged from successful implementation of the MMP:

Benefits to Citizens

i) Multiple channels to access services from police
ii) Simplified process for registering and tracking incidents, petitions and FIRs
iii) Simplified process for accessing general services such as requests for certificates, verifications, and permissions
iv) Simplified process for registering grievances against police
v) Simplified process for tracking the progress of the case during trials
vi) Simplified access to view/report unclaimed/recovered vehicles and property
vii) Improved relationship management for victims and witnesses
viii) Faster and assured response from police to any emergency calls for assistance

Benefits to Police Department

i) Enhanced tools for investigation
ii) Centralized crime and criminal information repository along with the criminal images and fingerprints with advanced search capabilities
iii) Enhanced ability to analyze crime patterns, modus operandi
iv) Enhanced ability to analyze accidents and other road incidents
v) Faster turnaround time for the analysis results (crime and traffic) to reach the officers on the field
vi) Reduced workload of the police station back-office activities such as preparation of regular and ad-hoc reports and station records management
vii) Enhanced tools to optimize resource allocation for patrols, emergency response, petition enquiries, and other general duties

viii) A collaborative knowledge-oriented environment where knowledge is shared across the different regions and units

ix) Better coordination and communication with external stakeholders through implementation of electronic information exchange systems

Benefits to Ministry of Home Affairs (NCRB)

i) Standardized means of capturing the crime and criminal data across the police stations in the country

ii) Faster and easier access to crime and criminal information across the country in a manner amenable for trend and pattern analysis

iii) Enhanced ability to detect crime patterns and modus operandi across the states and communicate to the state police departments for aiding in crime prevention

iv) The ability to respond faster and with greater accuracy to inquiries from the parliament, citizens and citizens groups; and to RTI queries.

Benefits to External Departments (example: Jails, Courts, Passports Office, Transport Department, and Hospitals)

i) Seamless integration with police systems for better citizen service delivery and improved law enforcement

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 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 list of addresses, designations and contact details of key officials shall be provided as a annexure to this RFP.

<< SPMC to provide the above annexure >>

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 a 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 at the various client sites (Police Stations, Circle 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 to add the relevant annexure pertaining to the client site infrastructure >>

3.6. Existing Capacity Building Infrastructure (District Training Centers and Police Training Colleges)

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 >>

4. 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 Core application Software (CAS) is expected to be ready by ***<Month 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).

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).

4.1. CAS (CENTER)

CAS (Centre): CAS (Centre) would cater to the functionality that is required at the GOI level (by MHA and 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.

4.2.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. 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, 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
- 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.
- 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

4.3. 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 under the supervision of National Informatics Centre (NIC). 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) and CAS (State) would be managed by NCRB under the guidance of NIC, DIT and MHA.

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.

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.

4.4. Overview of Services for CAS (State)

i. 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.

ii. Petition Management Service

The service shall enable the police personnel to register and process the different kinds of general service petitions and complaints.

iii. 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.

iv. 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.

v. 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.

vi. 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.

vii. 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.

viii. 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.

ix. Police Email and Messaging Service

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

x. 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.

xi. 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.

xii. 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.

xiii. 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.

xiv. 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.

xv. User Feedback Tracking and Resolution Service

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

xvi. Activity Log Tracking and Audit Service

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

xvii. 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

4.5. Overview of Services for CAS (Center)

i. 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.

ii. 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.

iii. 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.

iv. *Talaash* Service

The service will enable the user to search for missing persons across a central/ national database.

v. 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 across the national database.

vi. 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.

vii. Publication Service

This functionality will help the NCRB to publish the periodic crime reviews to the NCRB portal.

viii. 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.

ix. 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.

4.6. 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 is provided as an Annexure to this RFP.

4.7. 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 Management Services for CAS (State) and CAS (Center)
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.
- Routine functional changes.
- 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.

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.

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/artefacts (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.
- *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. In addition, the SDA shall assist the State SIs in customizing CAS (State) to support local language interface and ensure the development of interface in local languages.
- 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.

5. SCOPE OF THE PROJECT

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

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

<< SPMC to provide the above annexure >>

5.2. 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.

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), eforms applications (of State portals), Transport Department, Courts, Jails, Hospitals, Universities, Telephone Service Providers, and other external government departments (indicative only) to facilitate electronic exchange of information.

<< SPMC shall prepare the list of state MMPs (Targetted Public Distribution System, State portal, SSDG,) that needs to be integrated with the CCTNS >>

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.

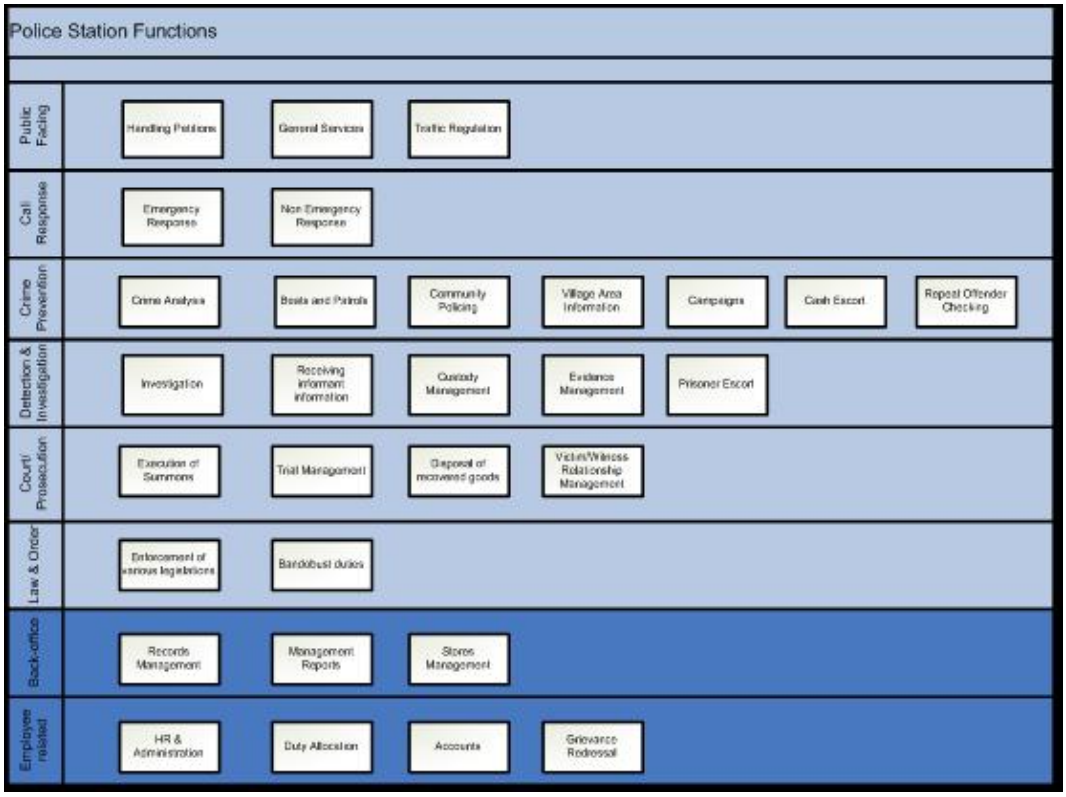
Brief Description of Police Station Process

<< The SPMC may add the additional functions as per State specific requirements along with the below mentioned Police Station, Traffic Management and Emergency response management functions. >>

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

Traffic Management

Traffic Police handle a variety of functions with an aim to ensure smooth flow of traffic and reduce traffic incidents that result in injuries or loss of life or damage to property. The key functions in Traffic are categorized under the three E's, - engineering, education, and enforcement. In addition to the three E's of traffic, police have a key responsibility of performing timely analysis of past traffic incidents in order to design strategies for road design changes, additional road signage, awareness campaigns, target audience, and identification of junctions and frequent violations for enforcement. Citizen-facing and analysis functions were selected for detailed study in order to focus the roadmap study on functions where IT enablement can lead to enhanced citizen-service delivery and higher efficiency gains rather than incremental ones.

Emergency Response Management

The control room of the police department serves as the focal point in the initiation and response of resources to the immediate citizen need for service. The primary function of the emergency response wing of the police department is to respond to

citizen calls for assistance. It is critical that the department responds to calls for assistance in the shortest possible time, with the appropriate resources and with the most accurate information available in order to meet the public safety. In order to achieve a minimum turnaround time from the time the call is received to the time an emergency responder is sent for service, the control room personnel should be provided with easy interfaces to capture the caller information and access to caller details, incident location and the nearest available emergency responder. Efficient and timely responses to emergency calls are critical in building up the confidence of public in the police department. Information systems can play a major role in improving the efficiency and the effectiveness of the functioning of the control room and field units while responding to emergencies. There are multiple stakeholders in an emergency response scenario, right from the caller or victim making the call to report the incident to the call receivers and dispatchers manning the control room to the emergency responders visiting the caller at his/her location. While the patrol officers may be the first responders, the police station takes charge of the incident after the first response for further enquiry and investigation.

6. SCOPE OF SERVICES DURING IMPLEMENTATION PHASE

The scope of the "bundled services" to be offered by the SI includes the following:

- Project planning and management
- 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.
- Infrastructure at the District Training Centers including computers, networking components, projectors and UPS.
- Site preparation at the Client site locations (police stations, circle offices, Commissionerates, Range offices, Zones, SCRB, SDPOs, Disctrict HQ and State HQ), Training Centers and Data Center.
- IT Infrastructure at the Client site locations (police stations, circle offices, Commissionerates, Range offices, Zones, SCRB, SDPOs, Disctrict HQ and State HQ).
- Network connectivity
- IT infrastructure at the Data Center and Disaster Recovery Center including the necessary hardware, software and other networking components.
- Data migration and Digitization of Historical Data
- Migration of CIPA and CCIS Police Stations / Higher Offices to CCTNS
- Change Management
- Capacity building
- Handholding Support
- 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 State Nodal Offcer's 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.

6.1. 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. Establish and measure resource assignments and responsibilities
c. Construct a project plan schedule including milestones
d. Measure project deadlines, budget figures, and performance objectives
e. Communicate the project plan to stakeholders with meaningful reports
f. Provide facility for detecting problems and inconsistencies in the plan
g. 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;
h. Progress reports on a fortnightly basis
i. 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;
j. Project quality assurance reports

k. 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 in the State and approved by the Committee on the advise 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 advise 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. 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.

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 modelling 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 artefacts 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 artefacts), 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.

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

System Study, Design, Application Development and Integration

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. 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 including 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 and validation of the data required for the configuration of the CAS (State) shall be the responsibility of 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 have 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 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.

6.3. Infrastructure at the District Training Centers

The SI is expected to setup the district training centers at each District Headquarters and Police Commissionerates. The premises will be provided by the STATE but all the infrastructure such as projectors, computers, networking components, UPS required to run the training lab shall be provided by the SI.

<<This applies only in the States / Districts where such training centers have not been setup>>

6.4. 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.

6.5. 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. 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)
3. Installation, Testing and Commissioning of UPS, DG-Set
4. Physical Installation of Desktops, Printer, Scanner, /MFD, Switch- Connecting peripherals, devices, Plugging in
5. Operating System Installation and Configuration
6. Installation of Antivirus and other support software if any
7. Configuring the security at the desktops, switch and broadband connection routers
8. Network and browser Configuration
9. Test accessibility and functionality of CCTNS application from the desktops
10. Ensuring all the systems required are supplied, installed, configured, tested and commissioned and declaring the site to be operational.

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. >>

6.6. Network Connectivity for Police Stations, Higher Offices, and District Training Centers

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.

6.7. 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), additional 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).

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 to 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.

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..>>

6.8. DATA MIGRATION & DATA DIGITIZATION

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. Though STATE 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 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. 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 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, … (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 as proposed
7. Get final sign off from State Nodal Officer 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.
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.

6.9. 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. SI shall validate the data in the CIPA systems and migrate the data to CCTNS.

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

6.10. CHANGE MANAGEMENT

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.

It is to be noted that State has adopted a holistic approach for implementation of Project to ensure that planned objectives are met. Change Management initiative, to be designed & implemented by SI, shall focus on addressing key aspects of Project including building awareness in Police personnel on benefits of new system, changes (if any) to their current roles & responsibilities, addressing the employee's concerns & apprehensions w.r.t. implementation of new system and benefits that are planned for the employees.

It is required that if SI doesn't operate in the Change Management, Communication and Training domain then he collaborates with/ hires services of a specialist agency who will be responsible for complete Change Management, Awareness and Communication implementation and monitoring, on the lines suggested below.

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 a 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.

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.*

It is to be noted that SI is required to incorporate the cost of all resources required for design, execution and management of Change Management Plan for project, in its overall project cost.

Stakeholder Analysis / Impact Assessment

The SI shall perform the impact assessment, in light of new system, to identify the changes to the current functioning, organization structure, roles & responsibilities, current capacities (training to the existing resources or deployment of additional resources) etc. In this context, the SI is required to perform a baseline assessment of the communication requirements of various stakeholders to understand what stakeholders currently know about the initiative; what they need and want to know; how they prefer to receive information about the project. The SI shall steer the communication efforts, for both internal & external stakeholders, for the project and State will provide necessary support and guidance to SI for the same.

A detailed study needs to be carried out to understand the impact on each of the stakeholder and the influence that they can exercise on their respective areas of control, for making CCTNS successful. System Integrator (SI) shall ensure that the all stakeholders are aligned to the program and their concerns are documented and addressed. This activity would ensure that the Communications and Awareness Plan is in sync with the overall project's deployment schedule and to develop and deliver effective stakeholder interventions to individual stakeholders and stakeholder groups.

The stakeholders are distributed across the State/ UT and the SI should ensure that innovative and effective methods are used to conduct the Stakeholder Management activity which should cover the following but is not limited to points mentioned in the table below.

The SI would be responsible for the following activities:

S. No	Requirements	Details	Frequency
1.	Stakeholder	• SI shall be responsible for	

S. No	Requirements	Details	Frequency
	Analysis	interviewing stakeholders, analyzing data and recommending action plan to address concerns related to the CCTNS project. • Finalize questions to understand stakeholder concerns, what success means for them, influence on project, what is the impact of the program on the stakeholder etc • SI shall be responsible for refreshing the stakeholder engagement plan in consultation with the State's Nodal Agency, whenever the project scope or the program implementation timelines undergo a change.	One time activity Given the number of stakeholders, SI will use innovative ways to interview/interact with Stakeholders including, Phone/VC/Face to face/Focused Group etc so as to reduce costs of interaction.
2.	Develop Stakeholder Engagement Content	• SI shall develop content – discussion scripts, presentations or videos to explain the objectives of the program, what is in it for them and their people, what the benefits are.	Recurring activity over the entire duration of the SI

Other Requirements:

- SI shall cover all the identified stakeholders and stakeholder groups identified in all the higher offices, State Headquarters, District Headquarters, SCRB, DCRB and Police Stations.
- SI will recommend additional Stakeholder or Stakeholder Groups – Internal and External who need to be covered under this activity.
- SI shall also cover the extended teams and should not limit to the direct identified stakeholders

- SI shall come up with innovative ways of stakeholder engagement in addition to the video conferencing, one on one meeting and teleconference
- SI shall ensure that the stakeholder engagement activity is a continuous activity and buy-in and commitment of the stakeholders are key drivers for the success of this project
- SI shall make recommendations to best manage this process
- SI shall also develop Job Aids, an important component of sustaining the change by ensuring that there is enough support material available to maintain the performance of the transformed workforce. A job aid is a repository for information, processes, or perspectives that is external to the individual and that supports work and activity by directing, guiding, and enlightening performance. Since job aids are external to the individual and would be applicable to those set of activities which are complex and difficult to memorize. For example, in the beginning stage, searching of records in the CAS might require a Job Aid. However, as the time progresses and user becomes more thorough and comfortable with the new system Job Aids for such activities may no longer be required. Also, for more complex activities such as generating a MIS report from the system might require a Job Aid for a much longer duration. These Job Aids must be revised on periodic basis.

Assess change readiness

The SI shall perform an assessment, based on the Impact Assessment, to identify to what extent the State is currently equipped for the change, what are the key potential blockers and enablers within the structure, processes and staff for implementing the changes.

The Change Readiness Assessment should be used to determine the changes, requirements, concerns, type and level of resistance and expectations emerging as a result of the CCTNS program. The analysis should be performed for the whole State/ UT, for each of the identified stakeholders impacted by CCTNS.

Assessing change readiness will help the change team to:

- Pinpoint where risks are likely to occur
- Clarify issues associated with CCTNS
- Identify potential responses to change

- Identify and target where change activities are most needed

Change Readiness Survey shall involve collecting information about affected groups within the organization to determine how ready they are to accept and assimilate forthcoming changes. **At least four Change Readiness Surveys** are recommended during the project to measure if the project is on track and is aligned to the intended end state objectives (This may change as per the size of the target police personnel).

SI shall conduct 4 Cycles of Change Readiness Survey:

- 1st Cycle shall measure readiness to change
- 2nd & 3rd Cycle shall measure progress of change
- 4th Cycle shall measure the State/ UT police department's acceptance to change, potentially on the job.

S. No	Activities	Details	Frequency
1.	Develop Change Readiness Survey approach	• SI shall be responsible for developing the objectives, scope, and process for change measurement • SI shall also finalize the target audience, timelines, method of change measurement	One time activity
2.	Develop and Configure Change Measurement Survey/ Instrument	• SI shall develop or configure an appropriate change measurement instrument that is convenient for audience and easy to assimilate for CM Team • SI shall configure the change measurement instrument based on the requirements of the project	Recurring Activity (at least four times in two years)
3.	Select Sample Audience and	• SI shall select the sample for the survey and should ensure that the targeted audience is a fair mix representing all State Offices,	One time activity followed by review of sample audience for each subsequent

S. No	Activities	Details	Frequency
	Administer the survey	solutions and all levels of the organization. • SI shall be responsible for administering the survey- paper based or electronic, as the case may be.	cycle
4.	Analyze reports and devise corrective action plan	• Analyze the result of the survey and generate survey reports (Higher Office-wise, State Headquarters - wise, District Headquarters - wise and Police Station-wise) to be shared with respective leadership team. • Identify the key patterns that emerge out of the survey for all groups of stakeholders	Once for each survey
5.	Share the result with the leadership and refresh change management plan	• SI shall share the results of each survey with audience identified by ***State's Nodal Agency*** and validate the corrective action plan with their inputs. • SI shall refresh the Change Management Plan with new interventions in consultation with ***State's Nodal Agency's*** Change Management Plan	Once for each survey

Other Requirements:

- Change Readiness Survey should be deployed at significant milestone along the project implementation timelines but not limited to four in number, considering different go-lives in the project implementation plan

- SI should conduct at least four change readiness surveys- First survey shall be a baseline survey and should be deployed at the beginning of Track-2. Second survey should be conducted after 3-4 months of the first survey. Third survey should be completed at least a month before the go-live. Fourth survey should be conducted after the CAS (State) go-live.
- Proper mechanism for survey validation and verification should be devised. The survey result shall not be considered as valid if the participant audience is less than 60% of the target audience.
- SI should ensure that the sample selected for the change readiness survey is a fair mix representing all solutions, State Offices and levels of the organization. SI shall utilize both computer based and paper based method of survey deployment
- SI should ensure that the change measurement report gives insight to the leadership team if the change is on track or off-track and the corrective action plan for desired result. Report should bring forth results for higher offices, State Headquarters, District Headquarters, SCRB, DCRB and Police Stations.
- Change management plan should be revisited and revised based on the survey results and corresponding corrective actions in consultation with ***State's Nodal Agency's*** Change Management Team

Develop the change management plan

The SI shall design a road map to achieve/implement all the change management initiatives, which are essential for success of the project. The plan shall be more than an implementation plan; and shall contain change milestones based on the change vision, benefits milestones, benefits tracking mechanisms, actions to build commitment and actions to ensure business continuity. The plan shall also define change governance – including appropriate decision making and review structures.

Implementation of Change Management Plan

SI shall take lead in assisting State in implementing the change and State in turn shall provide all the necessary support for successful implementation of the change management plan developed by the SI. The SI shall be responsible for all the costs involved in design and implementation of the change management plan for Project.

The SI shall proactively work with State to address the project needs and gain buy-in and involvement of all the stakeholders in achieving the change. During the whole exercise, stakeholders' awareness, understanding and commitment to new ways of working should be raised. Stakeholders should also be encouraged, where appropriate, to contribute to or participate in the project to engender a joint sense of ownership.

Communication and Awareness

Communication and Awareness aims at engaging officers of the police force in two way interactive communications about the changes so that all individuals in the State/ UT's police department understand the target vision and strategy for moving forward. The purpose of communication plan is to educate and involve all audience groups to build understanding and ownership of the CCTNS Project. The communication plan also ensures that the CCTNS project provides relevant, accurate, consistent and timely project information to relevant stakeholders to promote and gain support for CCTNS Project. This plan provides a framework to manage and coordinate the wide variety of communications that take place during the project covering who will receive the communications, how the communications will be delivered, what information will be communicated, who communicates, and the frequency of the communications.

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.

S. No	Activities	Details	Frequency
1.	Develop and Validate detailed communication plan	• SI shall facilitate an exploration of specific objectives; i.e., who must understand what, by when, and why with respect to the project, to ensure successful uptake of the project. • SI shall prepare a detailed communication plan for the program	Once

S. No	Activities	Details	Frequency
		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 • These key audiences are not the only ones who will receive information, but their demographics will shape the strategy in terms of message and vehicle selection.	
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 ensuring that those accountable for specific elements of the plan follow through on their	Recurring Activity (once a month) over the entire duration of the SI

S. No	Activities	Details	Frequency
		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.	
4.	Measure Effectiveness of Communication and Update Change Management Plan	• After implementing the communications program, SI shall seek feedback on and measure the impact of the communications program. • SI shall evaluate the effectiveness of the communication by electronic or paper based survey or focused group discussion and develop an action plan to improve the effectiveness of communication • SI shall refresh the Change Management Plan in consultation with ***State's Nodal Agency's*** Change Management Plan • Through feedback, SI shall assess which messages have been delivered most clearly; which vehicles are most effective; and whether the appropriate target audiences have been identified. Based on such assessment, SI shall update the	Once in Six Months

S. No	Activities	Details	Frequency
		communication strategy & plan and shall ensure that objectives of communication program are ensured, which further should lead to successful uptake of system.	

Other Requirements:

- 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
- The SI shall conduct Communications & Awareness Campaigns for each Technology Solution offered in CAS (State) being implemented through various means – Print, Electronic, Face to Face, Audio/Visual etc.
- SI shall align communication content, timing and delivery to the deployment phases/plan of each solution.

Change Management Workshops

SI shall conduct Change Management workshops build appreciation of change management and develop change leadership across the stakeholder groups. SI shall define the requirements based on the detailed analysis and 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.

6.11. CAPACITY BUILDING

<<SPMC shall assist the State in the following:>>

Identification of Trainers (Internal)

The State Nodal Agency shall identify at least four 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 Nodal Agency shall identify the Trainers within each of the Police Training Colleges in the State 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 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 Headquarters and respective Districts/Commissionerates 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 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 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 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 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'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'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'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 identify the languages to be used by the end-user for entering data and ensuring multi-language training to the end users as per requirement.

Learning Management System and Training Portal

Developing a Learning Management System and Training Portal for providing access to all training content online including documents, demo, audio, video, simulation and practice, assessment, self-learning and context sensitive help and monitoring, support and reporting

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 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, 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 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 specialised 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)
- Instructor Demonstrations (CAS - Application training environment)
- Hands-on Exercises (CAS - Application training environment)
- 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'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.

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

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

6.12. 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.

6.13. 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 summarised 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 19784-1:200 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 & secur 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.

6.14. 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 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 s/w.

STATE 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, 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 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 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 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.

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.

7. 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 a 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.

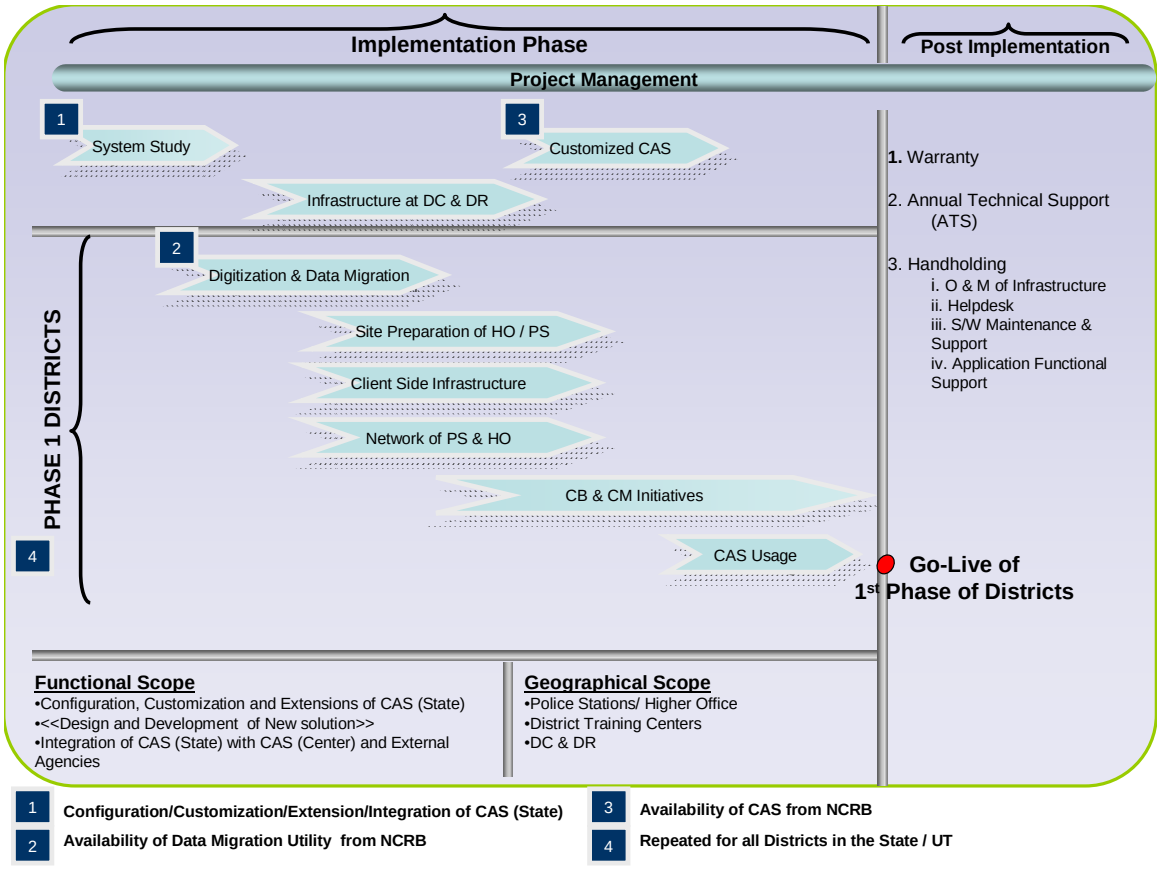
SI shall provide the Operations and Maintenance Services for a period of <<5>> years following the deployment and "Go-Live" of the solution in the State**. In case each District is declared as "Go-Live" at different instances during the project roll-out, the Operations and Maintenance Services for the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

8. IMPLEMENTATION AND ROLL-OUT PLAN

<<The STATE needs to provide the implementation and roll-out plan for the solution.>> It is suggested that the solution be piloted in a few police stations in one or two districts/commissionerates and the feedback incorporated before rolling out across the STATE. 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. SI is also responsible for conducting workshops for the key officers (State Mission Team, District Mission Team, 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, District Core Team) of the Districts / State during the design and implementation of CCTNS in the State.

One of the important factors that would determine the success of the CCTNS implementation in the State is the continuous availability of domain experts to the implementation team. SI shall put together a team of at least five (5) domain experts with a minimum of 10 years of experience in the State 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

7. SERVICE LEVELS

This section describes the service levels to be established for the Services offered by the SI to STATE. The SI shall monitor and maintain the stated service levels to provide quality service to STATE. The SLA are provided as an Annexure to this RFP.

ANNEXURE :

DETAILS OF THE TECHNOLOGY STACKS FOR 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
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	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: Unstructure data: using openCMS search features Structured Data	N/a	N/a	N/a	N/a

	Proposed Solution by Software Development Agency	Version and Year of Release	Original Supplier	Description (include major features/ services only)	Support Provided By
	Mysql & Custom application interface				
Portal Server	Glassfish Application Server	3.0	SUN	J2EE Application 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	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 Manageme	OpenSSO	7.0	SUN	LDAP	SUN

	Proposed Solution by Software Development Agency	Version and Year of Release	Original Supplier	Description (include major features/ services only)	Support Provided By
nt					
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: Unstructure 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

	Proposed Solution by Software Development Agency	Version and Year of Release	Original Supplier	Description (include major features/ services only)	Support Provided By
Directory Services	Microsoft Active Directory	2008	Microsoft	LDAP	Microsoft
DMS/CMS	Windows Sharepoint Services	n/a	n/a	n/a	Microsoft
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: Unstructure 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

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
DMS/CMS	Alfresco				
Email/Messaging	N/A				
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 : POST IMPLEMENTATION 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 designated premises.
    c. Software maintenance and support services.
    d. Application functional support services

The services shall be rendered onsite from the State designated premises. To provide the support for the police stations, circle offices, sub-divisional offices, district headquarters / commissionerates, ranges, zones, state police headquarters and other locations across the STATE 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 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. 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. 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 reserves 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, 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 and will not be returned to SI.
10. Warranty should not become void, if STATE 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 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's business hours (Business hours in STATE will be from 0830 hours to 2030 hours on all days (Mon-Sun)) with access for STATE 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 shall have access to the online support and tools provided by the manufacturer. STATE 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 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 on a monthly basis. Whenever required by STATE, 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.
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 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, range offices, zonal offices, state police headquarters and other locations across the STATE where the software, hardware, and other infrastructure will be rolled out.
4. For all the services of STATE 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 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 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 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 from the development center in STATE.
2. Enhancements and defect fixes. SI shall incorporate technological changes, and provide enhancements as per the requests made by STATE. 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 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 authorised End Users of the STATE.
12. The services shall include administrative support for user registration, creating and maintaining user profiles, granting user access and authorisation, providing ongoing user password support, announcing and providing networking services

for users and providing administrative support for print, file, directory and e-mail servers.

ANNEXURE : 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.

(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 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.

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 is 0.1% of respective payment-period payment to the SI.

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

Post Implementation Phase SLAs

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

(a) **Production CAS Systems**. The failure or disruption has a direct impact on the 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.

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

Severity of Violation: High

<table>
<tr><th>Availability over the six-month period</th><th>Violations for calculation of penalty</th></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>
</td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>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><th>Availability over the six-month period</th><th>Violations for calculation of penalty</th></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

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

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>
<table>
<tr><th>Number of instances over the six month period</th><th>Violations for calculation of penalty</th></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><th>Number of instances over the six month period</th><th>Violations for calculation of penalty</th></tr>
<tr><td>>0 & <=3</td><td>1</td></tr>
<tr><td>> 3</td><td>2</td></tr>
</table>

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

Severity of Violation: High

Each occurrence where the peak memory utilization of any server crosses 70% (with the exception of batch processing) and stays above 70% for time more than 30 minutes will be treated as one (1) instance.
<table>
<tr><th>Number of instances over the six month period</th><th>Violations for calculation of penalty</th></tr>
<tr><td>>0 & <=3</td><td>1</td></tr>
<tr><td>> 3</td><td>2</td></tr>
</table>
</td></tr>
</table>

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

<table><tr><th>Availability over the six-month period</th><th>Violations for calculation of penalty</th></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><th>Availability over the six-month period</th><th>Violations for calculation of penalty</th></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</td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>The list of critical business functions and peak usage hours will be identified by the state / UT during the Supply and System Integration Phase.

This service level will be monitored on a monthly basis.

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

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

2. Client Site Infrastructure Systems

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

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

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

Service Level Description	Measurement
Client Site Systems Availability	Availability of the critical client site infrastructure components at all the implementation sites shall be at least 99% Severity of Violation: High This service level will be measured on a monthly basis for each implementation site. If the availability in a month for an implementation site falls

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

3. Handholding Support: Client Site Support

(a) **Level 1 Incidents**. The incident has an immediate impact on the 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 officesthat 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.

Service Level Description	Measurement
Client Site Support Performance	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

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>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><th>Average number of instances per month</th><th>Violations for calculation of penalty</th></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

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><th>Average number of instances per month</th><th>Violations for calculation of penalty</th></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)</td></tr>
</table>

Service Level Description	Measurement
	Severity of Violation: High Each instance of non-meeting this service level will be treated as one (1) violation.

4. Handholding Support: Application Support

(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><th>Performance over the six-month period</th><th>Violations for calculation of penalty</th></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>
</td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>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>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><th>Performance over the six-month period</th><th>Violations for calculation of penalty</th></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><th>Performance over the six-month period</th><th>Violations for calculation of penalty</th></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>
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>Application Support Performance</td><td>Up to date of the documentation of the design, modifications, enhancements, and defect-fixes in the half-yearly period.

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

Service Level Description	Measurement
	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 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.

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td>Helpdesk Performance</td><td>98% of the calls shall be answered within 45 seconds.

Severity of Violation: High

This service level will be monitored on a monthly basis.

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

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

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

Severity of Violation: High

This service level will be monitored on a monthly basis.

<table><tr><td>Performance over the six-month period</td><td>Violations for calculation of penalty</td></tr><tr><td>< 80% & >= 70%</td><td>1</td></tr><tr><td>< 70% & >= 60%</td><td>2</td></tr><tr><td>< 60%</td><td>3</td></tr></table>
In addition to the above, if the service level in any month in the six-month period falls below 60%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Helpdesk Performance</td><td>80% of the Level 2 calls shall be resolved within 6 hours from call received / logged which ever is earlier. The maximum resolution time for any incident of this nature shall not exceed 48 hours.

Severity of Violation: High

This service level will be monitored on a monthly basis.

<table><tr><td>Performance over the six-month period</td><td>Violations for calculation of penalty</td></tr><tr><td>< 80% & >= 70%</td><td>1</td></tr></table></td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>
<table>
<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 for each such month to the overall violations for this service level.</td></tr>
<tr><td>Datacenter Support Performance</td><td>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.</td></tr>
<tr><td>Datacenter Support Performance</td><td>Up to date of the documentation of the design, modifications, enhancements, and fixes.

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

Service Level Description	Measurement
	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
Availability and Performance Report	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.

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

8. Credits for Successful Application Uptake

The below tables gives details of the credits that can gained by the SI for successful uptake of the application in the State. The credits will not be calculated for the first reporting period.

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

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

The following table applies for each of the above parameters:

<table><tr><th>% increase over the measurement in the last reporting period</th><th>Credits</th></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 is two (2) % of respective half yearly payment to the SI.

(viii) Penalties 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.