E-Governance

Mission Mode Project (MMP)

Crime & Criminal Tracking Network and Systems (CCTNS)

Model RFP for States

(Draft)

सत्यमेव जयते

Ministry of Home Affairs
Government of India

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.*

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 by these monitoring agencies and also to be shared by states.

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 effective policing at all levels and especially at the Police Station level through adoption of principles of e-Governance, and 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 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.

2.3 CCTNS Implementation Framework

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

The role of the Centre (MHA and NCRB) focuses primarily around planning, providing the core application software (to be configured, customized, enhanced and deployed in States), 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 (or a maximum of two) System Integrators (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.

2.4 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(s) 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 or consortia of companies 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 and Citizen groups
- Police Personnel at the Cutting Edge (Station House Officers, Investigation Officers, Station Writers, Constables)
- Senior Officers in the State Police Force
- Ministry of Home Affairs
- External Departments such as Jails, Courts, Passports Office, Transport Department, and Hospitals

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 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) Greater access to traffic police for registering traffic complaints

ix) Ability to view and pay pending traffic challans from multiple access points

x) 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

x) Advanced tools for traffic regulation and enforcement

Benefits to Police Personnel

i) Balanced performance evaluation metrics and framework

ii) Simplified process for registering grievances within the department

iii) Simplified process for personnel's administrative services such as leave, pay-roll, loans, and bill claims

iv) Integrated view of the service record that presents the performance feedback and training needs.

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

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 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.

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
7. Current data available in the system and whether the data can be used during data migration

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

3.3 Existing Data Center Infrastructure

State shall furnish the details about the existing Data Center Infrastructure that will be provided to the SI for the commissioning the IT infrastructure that will be used to deploy the application. The proposed location 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 a Annexure to this RFP.

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 shouild be provided in this section.

The detailed information pertaining to the WAN Infrastructure shall be provided to the SI as a Annexure to this RFP.

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 a Annexure to this RFP.

4. Scope of the Project

4.1 Geographical Scope

The STATE shall specify the locations across which the application will be rolled out and the SI will provide the handholding support. While all the police stations, circle offices, and other such locations will be covered for the implementation, the section on the implementation and roll-out plan should specify how the SI is expected to phase out the implementation.

4.2 Functional Scope

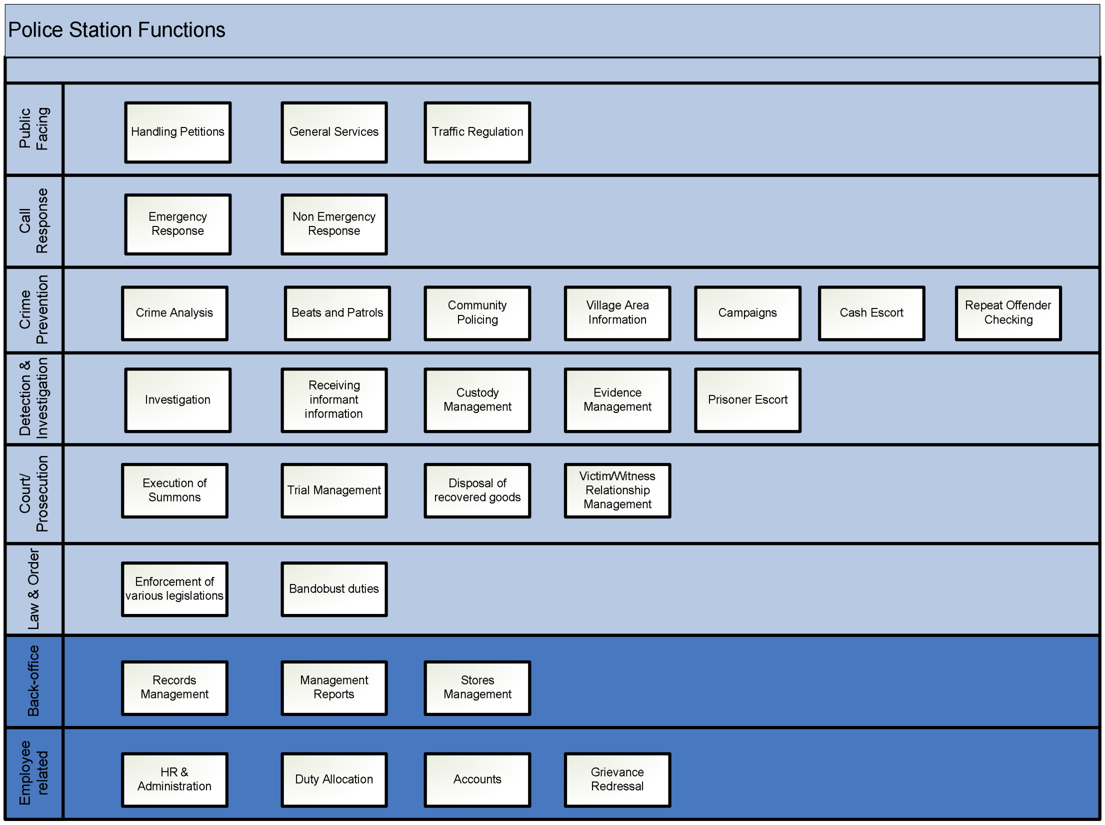
The functional scope primarily covers the functions and activities at the Police Station.

Police Station

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.



Police Station Functions

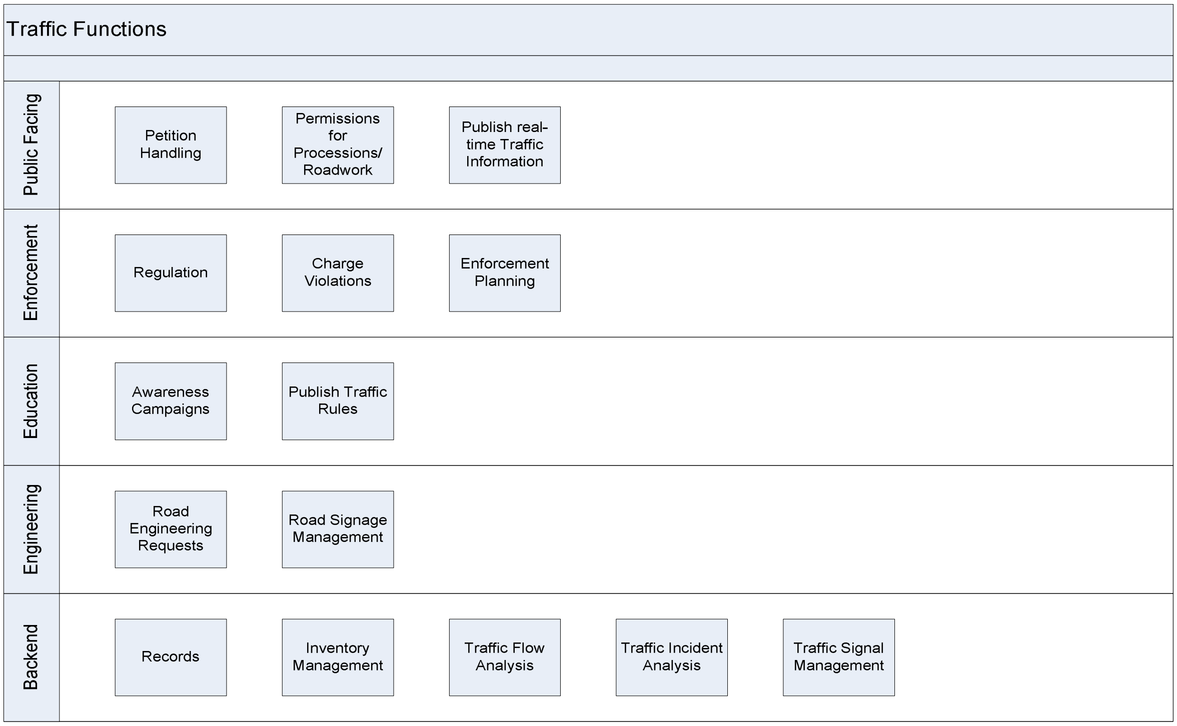
Public Facing	Handling Petitions	General Services	Traffic Regulation				
Call Response	Emergency Response	Non Emergency Response					
Crime Prevention	Crime Analysis	Beats and Patrols	Community Policing	Village Area Information	Campaigns	Cash Escort	Repeat Offender Checking
Detection & Investigation	Investigation	Receiving informant information	Custody Management	Evidence Management	Prisoner Escort		
Court/ Prosecution	Execution of Summons	Trial Management	Disposal of recovered goods	Victim/Witness Relationship Management			
Law & Order	Enforcement of various legislations	Bandobust duties					
Back-office	Records Management	Management Reports	Stores Management				
Employee related	HR & Administration	Duty Allocation	Accounts	Grievance Redressal			

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.

The various functions of the traffic police have been mapped in the diagram below:



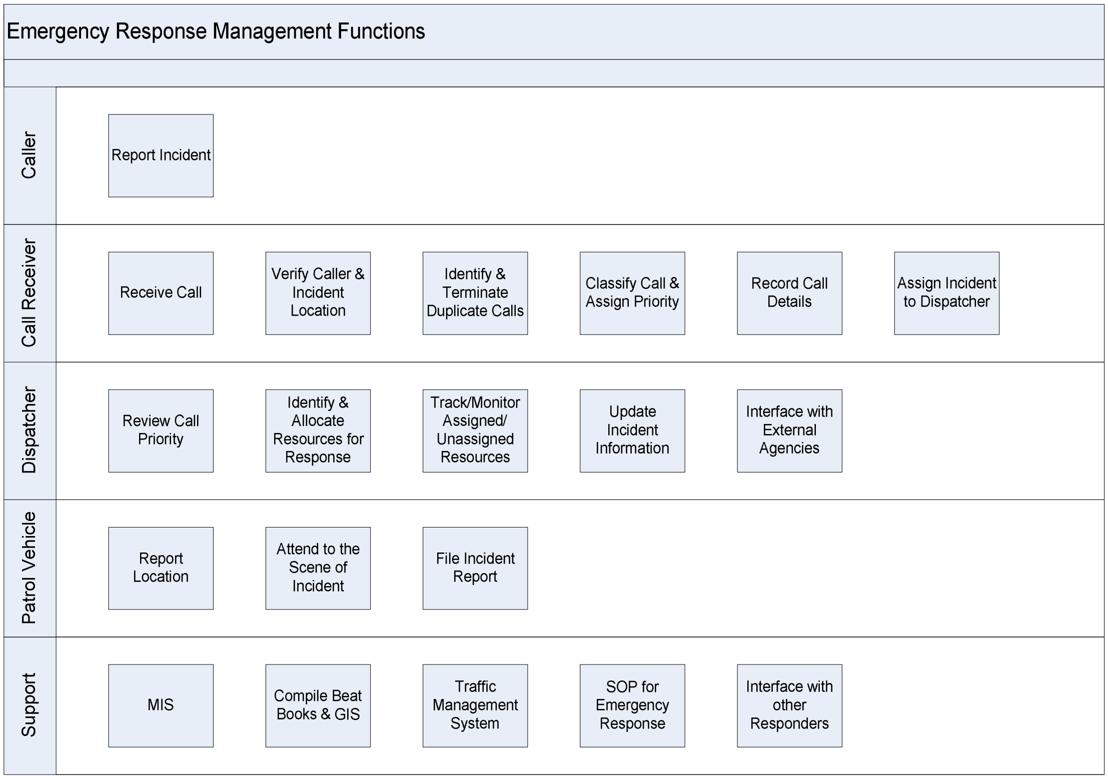
Traffic Functions					
Public Facing	Petition Handling	Permissions for Processions/ Roadwork	Publish real-time Traffic Information		
Enforcement	Regulation	Charge Violations	Enforcement Planning		
Education	Awareness Campaigns	Publish Traffic Rules			
Engineering	Road Engineering Requests	Road Signage Management			
Backend	Records	Inventory Management	Traffic Flow Analysis	Traffic Incident Analysis	Traffic Signal Management

Traffic Related Functions in a Police Station

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.

The figure below illustrates the activities/functions that are a part of emergency response management:


Emergency Response Management Functions
Caller
Report Incident
Call Receiver
Receive Call
Verify Caller & Incident Location
Identify & Terminate Duplicate Calls
Classify Call & Assign Priority
Record Call Details
Assign Incident to Dispatcher
Dispatcher
Review Call Priority
Identify & Allocate Resources for Response
Track/Monitor Assigned/ Unassigned Resources
Update Incident Information
Interface with External Agencies
Patrol Vehicle
Report Location
Attend to the Scene of Incident
File Incident Report
Support
MIS
Compile Beat Books & GIS
Traffic Management System
SOP for Emergency Response
Interface with other Responders

Emergency Response Management Functions

5. Scope of Services

5.1 Project Management and Control

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 Project Director, 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 Project Director and/or actions to be taken by the Project Director 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

5.2 System Study, Design, Application Development and Integration

The SI shall carry out a detailed systems study to prepare the System Requirements Specifications (SRS) incorporating the functional specifications and standards provided by the NCRB and the state-specific requirements. The SRS preparation shall take into account the BPR recommendations suggested by the NCRB.

1. Conduct of System Study at selected locations.
2. Preparation of System Requirements Specifications (SRS).
3. Preparation of the Solution Design
4. Solution Development and/or Customization as required
5. Development of reports
6. Formulation of test plans
7. Testing of the configured solution

5.3 Functional Modules of the Solution

The following are the suite of proposed solutions / modules for the Police Department:

1. Registration, Investigation, and Prosecution Solutions
   a. Case Management System
   b. Criminal Information System
   c. Information Registers

    d. Trial Management System
    e. Summons and Warrants Management System
    f. Automatic Fingerprint Identification System

2. Law and Order Solutions
3. Crime Prevention Solutions
    a. Crime Analysis Tools
    b. Jail Information System
    c. Beats Management System
4. Traffic Solutions
5. Emergency Response Management Solutions
6. Reporting Solutions
7. HRMS Solutions
    a. Personnel Management
    b. Leave, TA, and other personnel related solutions
    c. Duty Allocation System
    d. Employee Grievance Management System
8. Collaboration Solutions
    a. Police Messaging System
    b. Email
    c. Bulletin Board
    d. Case Knowledge Bank
    e. News Groups
9. Citizen and External Interfacing Solutions
    a. Citizen Portal
    b. Citizen Grievance Redressal System
    c. Police Service Center System
    d. External Interfacing Systems to interface with Transport Department, Courts, Jails, Hospitals, Universities, Telephone Service Providers, and other external government departments to facilitate electronic exchange of information

The detailed functional requirements for the key process areas of Registration, Investigation, and Prosecution are provided as Annexure to this RFP. The suggested technical architecture and standards are provided as Annexure to this RFP. The non-functional requirements for the solution are provided as a separate Annexure to this RFP.

5.4 IT Infrastructure at the data center and Disaster Recovery Center

The STATE will provide the Data Center premises for both Primary Data Center and Disaster Recovery Center for hosting the solution. 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 are sized adequately and redundancy is built into the architecture required meet the service levels mentioned in the RFP.

SI shall be responsible for sourcing, supplying and deploying server hardware and solution specific software; developing and installing solution. SI shall provide a Bill of Material/ Bill of Quantity that specifies all the hardware, software and any additional networking components of solution, both for Primary Data Center and Disaster Recovery Data Center, in detail so as to facilitate sizing of common Data Center infrastructure such as Racks, Power and Cooling, Bandwidth among other components.

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

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

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 Center can be avoided.

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

5.5 Network Connectivity

The SI shall provide the last mile connectivity to the Police Station wherever required. The STATE shall use SWAN for the connectivity to the Data Center where feasible. In cases where SWAN is not available, the STATE shall procure the connectivity from a service provider and the SI is expected to setup the last mile connectivity to the client site.

5.6 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.

5.7 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 provided under the Geographical Scope Section. SI shall procure the CCTNS infrastructure required at the locations statewide.

At each such location the following shall be carried out.

1. Supply of the hardware, software, networking equipments, UPS, DG set to the location as per the requirements
2. Ensure adequate power points in adequate numbers with proper electric-earthling
3. Redundant Network Connectivity - Ensuring last mile connectivity and testing. (At some locations SWAN may be available. SI shall ensure there is redundancy in the connection)
4. Installation and Testing of UPS, DG-Set

5. Physical Installation of Desktops, Printer, Scanner, /MFD, Switch- Connecting peripherals, devices, Plugging in
6. Operating System Installation and Configuration
7. Installation of Antivirus and other support software if any
8. Configuring the security at the desktops, switch and broadband connection routers
9. Network and browser Configuration
10. Test accessibility and functionality of CCTNS application from the desktops
11. 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

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

The infrastructure at required at these locations include-

1. Connectivity
2. Desktops/PCs
3. Network Switch/LAN
4. Printer + Scanner/MFD
5. UPS
6. DG Set
7. Furniture

Details of quantities and additional guidance about the capacity of the above are given as Annexure to this RFP.

5.8 Site Preparation

The SI is expected to prepare the client sites for setting up the necessary client site infrastructure.

5.9 Capacity Building

SI shall design and implement a requisite plan for Capacity Building for various levels of police personnel in the STATE such that the direct users and other stakeholders of CCTNS are empowered to optimally use CCTNS and enhance outcomes in crime investigation, criminals tracking and other core police functions; and also ensure a smooth functioning of CCTNS.

In line with the strategy of "bundling of services" for the implementation of CCTNS, the Capacity Building initiatives should be closely aligned with the stage of implementation of the project. The "Go-live" milestones of the project implementation plan for each District should also ensure that requisite capacity is available among the users for sustained operation of the system.

A critical part of the Capacity Building initiative would be the training program. The overall capacity building is envisaged to have a multi-tiered approach:

- Sensitization and Basic Awareness for IT systems - broad level
- Orientation for the particular application (s) and what it does
- Role/process specific training programs

a. Creating awareness and sensitization regarding the benefits of ICT

i. This part of the training focuses on the awareness of the general benefits of IT systems such as automation of routine and redundant tasks or moving from the paper-based records management to a more sophisticated electronic records system that can alleviate the efforts to create reports for senior management.

b. Basic Computer awareness training

i. Fundamentals of computer usage should focus on the basics of using the computer, keyboard, and mouse in order to make the users feel comfortable with the computer.

ii. Email and Office suite training should be imparted to all the users in the department.

iii. Training on analytical functions of the computers such as spreadsheets and such worksheet applications should be imparted to the users to actually derive the benefits of analyzing the data.

c. Role based training on application software

i. The training should focus on the users getting comfortable to use the deployed CCTNS solutions.

d. Specialized training on system administration and maintenance

i. For a select set of high-aptitude group, training should be imparted on basic troubleshooting, hardware and network maintenance for sustained functioning of the program and continued success of the CCTNS initiative.

Broad guidelines for the Capacity Building plan have been provided as Annexure to this RFP. These guidelines include the following:

1. Broad outline of capacity building areas and skills to be imparted
2. Segments of Police Staff to which different types of training needs to be provided
3. Number of personnel to be trained
4. Training calendar and frequency of training required for different types of training
5. Suitable Mode of communication for conducting the training such as multimedia, written content, instruction mode etc.
6. Details of Training Infrastructure available for conducting the training programs such as Police Training Centres and other Government, Institutional or Academic training centres.
7. Requirements for specialized training such as hardware, network and data centre maintenance
8. Train-the-trainer program details
9. Metrics for measuring the success of the training programs

In accordance with the guidelines provided, the SI is expected to provide the following services for Capacity Building:

1. Conducting the training sessions for Sensitization and Basic IT Awareness as per recommended guidelines
2. Conducting the training sessions specific to the application. These sessions should be conducted such that the users of the application are trained by the time the application "goes-live" in the District.
3. Identifying the specific roles required for the application, mapping the roles to users of the application and conducting the role-specific training sessions for the applications.
4. Conducting specialized training sessions for select group of individuals that would form Core teams for each District so that the group is equipped with basic information about all aspects of the software application, basic troubleshooting for networking, hardware, peripherals and system commands.
5. Conduct training sessions for identified "trainers" within the department and provide requisite training material to them for conducting the trainings.
6. Providing hard copies of the training material to all police stations and offices for reference
7. Developing a Learning Management System for providing access to all online training content
8. Customization of the Training Manuals, User Manuals, Operational and Maintenance Manuals provided along with the CCTNS CAS Software
9. Design and development of the Training Manuals, User Manuals, Operational and Maintenance Manuals for the modules developed at the State level.
10. Gathering feedback from participants and instructors on the training sessions related to content, mode of instruction, readiness levels of participants, attendance etc.
11. Conducting audits to evaluate effective usage by users of application and identify corrective action plan

5.10 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.

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 (SI to finalize the actual number of sessions in consultation with the STATE) in sync with the training plan and as part of the training module. SI can utilize the District Training Centers that will be setup as part of this project but is required to provide the necessary material for the workshops including presentations, training material etc in both soft and hard copy formats. Following outlines key activities/approach to be adopted by SI for designing & execution of change management plan for project.

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, Communication and Training implementation and monitoring, on the lines suggested below:

1. 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.

2. 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.
3. Design the change management approach – The SI shall perform an analysis and provide advice on the optimal way of getting STATE from where it is now to where it needs to be, for successful implementation of system and to mitigate all the project risks. This will include the approach to change. What are the time frames and when are benefits expected to accrue?
4. Develop the change plan – The SI shall design a road map to achieve/implement all the changes, 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.
5. Define change governance – including appropriate decision making and review structures
6. Assist in implementation of Change Management Plan – SI shall take lead in assisting STATE in implementing the change and STATTE 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.
7. 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.

The communication strategy should be aimed at addressing the information needs, awareness building in the internal stakeholders of the project through appropriate mechanisms. Following outlines the requirements for this piece of work for SI and approach to be adopted for implementation of Communication strategy for project.

1. *Conduct a Baseline Communications Assessment*

The police personnel are key strategic elements for the successful uptake of the Project. 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.

2. *Develop and Validate the Communications Strategy*

   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. Utilizing data from the baseline assessment as well as individual knowledge of stakeholders, the SI will reach consensus on target and influencer audiences – segmented, prioritized, and addressable. 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.

3. *Develop and Validate the Communications Plan*

   From the foundation of the communications strategy (objective, audiences, and messages), SI shall work with STATE to build a plan in terms of vehicles, timing, sequence, accountability, and measurement. Examples of vehicles may include: presentations, newsletters, videos, brochures, Internet and Intranet sites, email messages, telephone hotlines, publicity in media etc.

4. *Implement the Communications Program*

   Implementing the communications plan will involve following up with the individuals responsible – and accountable – for specific communications vehicles. 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 responsibilities. If needed, SI shall deliver communications training to groups of individuals responsible for communicating key messages to target audiences.

5. *Measure the Results of the Communications Program*

After implementing the communications program, SI shall seek feedback on and measure the impact of the communications program. SI may adopt various feedback mechanisms: event-based, periodic, or performance-related, depending on types of communications vehicles implemented. Obtaining this feedback is critical in order to ensure that messages are being received via the most efficient means possible, and with the desired effect.

6. *Adjust the Communications Program*

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 communication strategy & plan and shall ensure that objectives of communication program are ensured, which further should lead to successful uptake of system.

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

5.11 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 methodology, 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. Provide checklists from the migrated data to Project Director for verification, including number of records, validations (where possible), other controls / hash totals. Highlight errors, abnormalities and deviations.
4. Incorporate corrections as proposed
5. Get final sign off from Project Director for migrated / digitized data
6. At the end of migration, all the data for old cases and registers must be available in the new system

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 SP will be required to devise his own detailed methodology and get it approved by Project Director.

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.

5.12 Requirement on Adherence to Standards

Preference for Open 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.

Workflow design	WFMC standards
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 19784-1:20 specification

Finger print scanning	IAFIS specifications
Digital signature	RSA standards
Document encryption	PKCS specifications
Information Security	CCTNS system to be ISO 27001 certified
Operational integrity & security management	CCTNS system to be ISO 17799 compliant
PFC Operations	All PFC's to be ISO 9001 certified
IT Infrastructure management	ITIL / EITM specifications
Service Management	ISO 20000 specifications
Project Documentation	IEEE/ISO specifications for documentation

5.13 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. Infrastructure Compliance Review
3. Availability of Services in the defined locations
4. Performance
5. Security
6. Manageability
7. SLA Reporting System
8. Project Documentation
9. 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.

5.14 Post Implementation Support

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.

6. 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.

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 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 STATE or an agency designated by them, then STATE will have the right to take appropriate disciplinary actions including termination of the contract.

A Service Level violation will occur if the SI fails to meet Minimum Service Levels, as measured on a quarterly 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 suggested format and a review shall be conducted based on this report. A monthly Availability and Performance Report shall be provided to the STATE 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 upon review and signoff by both SI and STATE. 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. 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 STATE and will be performed by STATE or STATE appointed third party agencies.

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 STATE on a monthly basis. The tool should also be capable of generating SLA reports for a half-year. STATE will audit the tool and the scripts on a regular basis.

The 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 depots/ user units and the developments of technology practices globally. The SLAs may be reviewed on an annual/bi-annual basis as STATE decides after taking the advice of the SI and other agencies. All the changes would be made by STATE in consultation with the SI. The changes made should not result in undue financial advantage to the SI.

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 Annexure to this RFP. 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. STATE and SI.

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 STATE 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.

Service Level Category: Application Uptake

Service Level Metrics

1. Level of adoption of the system among the police personnel
2. Number of successful service requests to search and retrieve information that can aid investigations and servicing the general service requests from the central crime and criminal information repository
3. Turnaround time for providing the feedback to the field officers from the Chief Office and crime records bureau on the identified crime trends and patterns
4. Ease and turn-around time for preparing regular and ad-hoc reports on crime and criminal data in responding to requests from Chief Office, NCRB, and Parliamentary questions

Service Level Category: Data Center IT Infrastructure

Service Level Metrics

1. Availability of the IT infrastructure
2. Data Loss in the event of the failure of the Primary Data Center
3. Recovery time in the event of the failure of the Primary Data Center
4. Performance of the IT infrastructure with respect to utilization of CPU, I/O, and memory
5. Application Availability
6. Application Performance within the Data Center
7. Application Performance simulated for a low bandwidth connectivity to the Data Center
8. Replacement of the Data Center IT infrastructure in case of repeated failures of the equipment
9. Status of the documentation of the configuration, modifications to the configuration carried out on the infrastructure.

Service Level Category: Client Side IT Infrastructure

Service Level Metrics

1. Availability of the Core Client Side IT infrastructure
2. Replacement of the client side IT infrastructure in case of repeated failures of the equipment

Service Level Category: Handholding Support

Service Level Metrics

1. Performance of the Client Side Handholding Support team with respect to resolution time for the incidents reported by the Police personnel.
2. Performance of the Application Support team with respect to the resolution time for the defects and/or enhancements reported in the application.
3. Status of the documentation of the design, modifications, and enhancements carried out on the application
4. Performance of the Centralized Helpdesk with respect to answering calls and providing first level support to the end users of the application

Service Level Category: Project Management and Reporting

Service Level Metrics

1. Performance of the SI with respect to submitting the monthly status and SLA compliance reports to the STATE

ANNEXURE: CLIENT SIDE IT INFRASTRUCTURE SPECIFICATIONS

The indicative specifications for the Client Side IT infrastructure components are provided below:

Desktops

Make	Make, Model, Part Number and details - Must be Specified and all the relevant product brochures and manuals must be submitted
CPU	Intel Pentium Core 2 Duo 2.8 GHz or latest Processor GHz
Memory	2 GB 667 MHz DDR2 RAM upgradeable upto 4 GB
Mother Board	Intel G43 or better on Intel Motherboard
Monitor	17" TFT Monitor
Display Controller	Intel Graphics integrated on motherboard and capable of 1024x768 resolution with 16 Million colours
Hard Disk	Minimum 250 GB , 7200 RPM SATA Hard Disk
Networking Features	10/100/1000 Network Card with remote booting facility, remote system installation, remote wake up
Ports	8 USB Ports (including 2 USB in the front), 1 Serial Port, 1 Parallel Port, 1 PS/2 KeyBoard and 1 PS/2 Mouse Port
Keyboard	104 Keys, heavy-duty bilingual keyboard, having key life of 20 million keystrokes or more (same make and colour as base PC)
Mouse	2 button optical scroll mouse with mouse pad
Power supply	230 watts and above ACPI compliant or more SMPS power supply, should be capable to support fully configured PC
Power Management	Energy star compliant for power saving
Operating System	Windows XP Professional or latest preloaded
Bundled software	Standard bundled software pertaining to the model offered should be included in offer (Must be specified in the offer)
MS Office	Preloaded with office 2007 with media
Anti-virus	Preloaded (licensed version of Antivirus with 5 years validity)

Laptops

Processor	Intel Pentium Core 2 Duo (minimum 1.8 GHz) or latest
Operating System(s)	Windows XP Professional or latest preloaded
Memory	2.0GB, DDR2 SDRAM, 1 DIMM
Internal Keyboard:	Internal English Keyboard
Monitors	15 inch or higher
Graphics	Integrated Graphics Media Accelerator

	950(minimum)
Hard Drive:	160GB Hard Drive, 9.5MM, 7200RPM
Touchpad	Standard Touchpad
AC Adapter:	90W A/C Adapter
Module Bay Device:	24X CD-RW/DVD w/ DVD player software
Wireless LAN (802.11)	802.11a/g Dual-band Mini Card
Battery:	9 Cell Primary Battery
Carrying Cases:	To be included
MS Office	Preloaded with office 2007 with media
Anti-virus	Preloaded (licensed version of Antivirus with 5 years validity)

Multifunction Devices

Basic Functionality	
Functions	Black-and-white printing, black-and-white copying, colour scanning, black-and-white faxing
Printing System	
Print speed	> 18 ppm
Memory	256 MB expandable to 512 MB
Print quality (black, normal quality)	Up to 1200 x 1200 dpi
Duplex print options	Automatic
Copy System	
Copy speed (black, draft quality, A4)	>18 ppm
Copy resolution (black graphics)	600 x 600 dpi
Copier resize	25 to 400%
Scan System	
Scan Type	Flatbed, ADF
Optical scanning resolution	Up to 600 dpi
Maximum scanning size	22.7 x 30.2 cm
Minimum scanning size	No minimum
Bit depth	30-bit
Color scanning	Yes
Scan file format	PDF, JPEG
Fax functionality	
Colour faxing	No
Auto-redialing	Yes
Paper Handling/Media	
Auto document feeder	Standard, 50 sheets

capacity	
paper trays	minimum 2 Nos
Media types supported	Paper , transparencies, labels, envelopes, card stock
Maximum input capacity (sheets)	>500
Standard media sizes	A4, A5, B5 (JIS), executive (JIS), 16K, envelopes
Recommended media weight	Tray 1: 60 to 200 g/m², Tray 2: 60 to 120 g/m², Tray 3: 60 to 120 g/m²,
Other technical information	
System Interface	1 USB (compatible with USB 2.0 specifications), 1 network port
Compatible operating systems	Windows XP Professional or latest
Power requirements	Input voltage 220 to 240 VAC (+/- 10%), 50/60 Hz (+/- 2 Hz),
Operating temperature range	10 to 30º C

UPS

160V-270V, 50Hz+/-5% Single Phase
220V +/- 8% on AVR Mode, 220V +/- 1% on Battery mode
1 KVA /2 KVA Line Interactive
0.7-0.8 Lagging to unity
>86%
Pure Sine Wave
Max 3ms
>70%
(a) Hot Standby configuration (b) Static By Pass Switch (c) Serial RS 232 Interface (d) Auto file shut down (e) Remote Indicator Panel (f) SNMP Web Management software
Overload /short, circuit protection at the output of UPS Prevent overheating and transfer the load to bypass line.
Minimum 30 mins.
<55 dB at 1 m radius
0-50 deg C, Storage Temperature – 45 Deg C, Humidity – 95% RH non-concerning
AC Mains , AC main higher/low inverter or mains inverter on battery, fault, overload, load on bypass, load level/battery level bar graph
Input Voltage/output voltage /output current/output frequency/DC Voltage
ISO 9001/14001, Safety Standard Certification as per IEC 950/ EN 50091-1, EMC/EMI Certification as per IEC 950/EN 50091-2

ANNEXURE: DATA CENTER IT INFRASTRUCTURE SPECIFICATIONS

The indicative specifications for the IT infrastructure components are provided below:

Web-Server

1. Web server shall host the Web-Tier of the application
2. CCTNS solution shall have 2 Web-Servers configured in load-balancing mode. The number of servers/nodes in Application Server-Farm and capacity and specification of the same shall take into consideration the capacity and performance needs of the CCTNS application
3. Should be scalable up to 4 processors if a traditional rack mount server is chosen for this tier; Initial number of processors populated shall depend on the capacity needs of the application. If blade server based server-farm is chosen as the deployment option each blade server will have a single processor.
4. Vendor should supply the processors which should be the latest in its segment on date of hardware delivery
5. Should have 4GB RAM
6. Hard drives with the best available RPM at the time of delivery; Capacity of these drives shall depend on the capacity requirements of CCTNS and standard configuration offerings from OEMs
7. Should have integrated RAID controller
8. Server should provide vertical scalability features in terms of both processors and memory
9. Vendor should provide the cost of upgrading server in terms of both processors and memory
10. Should have redundant NICS 1Gbps
11. Should have redundant power supply

Application Server

1. Application Servers shall host the CCTNS solution-business logic and therefore shall be scalable and deployed in high availability cluster mode
2. CCTNS solution shall have at least 2- Application servers configured in Active-Active mode
3. Each Application Server shall be of at least dual processors and of the current processor architecture generation
4. Should be scalable ate last up to 4 processors if a traditional rack mount server is chosen for this tier. Initial number of processors populated shall depend on the capacity needs of the application. If blade server based server-farm is chosen as the deployment option each blade server will have a single processor
5. Vendor should supply the processors which should be the latest in its segment on date of hardware delivery
6. Should have at least 4GB RAM
7. Hard drives with the best available RPM at the time of delivery; Capacity of these drives shall depend on the capacity requirements of CCTNS and standard configuration offerings from OEMs
8. Server should provide vertical scalability features in terms of both processors and memory
9. Vendor should provide the cost of upgrading server in terms of both processors and memory
10. Should have redundant NICS 1Gbps
11. Should have redundant power supply

Database Server

1. Database servers solution for CCTNS should be a high performing clusters and therefore shall be scalable

2. CCTNS solution shall have at least 2- Database servers configured in Active-Active mode
3. Each Application Server shall be of at least 4 processors and of the current processor architecture generation
4. Vendor should supply the processors which should be the latest in its segment on date of hardware delivery
5. Should have at least 4GB RAM installed expandable to 8GB
6. 2x500 GB SCSI/SATA hard drives with the best available RPM at the time of delivery
7. Server should provide upgrade scalability features in terms of both processors and memory
8. Vendor should provide the cost of upgrading server in terms of both processors and memory
9. Should have redundant NICS 1Gbps
10. Should have redundant power supply

Server farm Switches

1. The server farm switches for CCTNS solution shall provide the gigabit Ethernet inter-connectivity for various solution components
2. The solution should provide redundant chassis based switches with high availability mode across the 2 switches
3. Each switch should have Gigabit Ethernet Fiber ports with 24 ports with dual power supplies and cooling fans
4. Should provide switching fabric of at least 8Gbps capable of delivering wire speed performance on all ports
5. Should support RADIUS/TACAS and should be manageable via SNMP. Embedded Web Management, CLI and RMON
6. The switches should support dynamic online configuration

ANNEXURE: POST IMPLEMENTATION SUPPORT SERVICES

SI shall provide five (5) years of comprehensive AMC that includes warranty support, Annual Technical Support (ATS), and handholding support. 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 .The handholding services shall include:

1. 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.
2. Central Helpdesk from the STATE designated premises.
3. Support for the end users at each of the locations.
4. Software maintenance and support services.
5. 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.