Tender Document for Selection of System Integrator (SI) Under CCTNS Project

MADHYA PRADESH COMPUTERIZATION OF POLICE SOCIETY, BHOPAL

"MPCOPS"

TENDER No. MPCOPS/SCRB/PHQ/CCTNS/SI-RFP/167/11

DATE: 25-04-2011

Tender for Selection of

System Integrator

Under

Crime & Criminal Tracking Network and Systems- Second Call

Volume – I "Functional and Technical Specifications"

Issued by

MPCOPS State Crime Record Bureau, Police Head Quarters,

Jehangirabad, Bhopal (M.P.)

Received Rs.…… ……
Vide DD No…..……
Dated…….....……
Issued to M/s..…….....

Phone: 0755 – 244 3635, FAX: 0755 – 244 3634

E-mail: cctns_mpcops@mppolice.gov.in, Web: www.mppolice.gov.in

Table of Contents

1. INTRODUCTION

1.1. Project Background

Availability of relevant and Timely information is of utmost necessity in Police functioning, 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, it is proposed to implement CCTNS project in all the state police departments to have common minimum threshold in the use of IT, especially for **crime & criminals** related functions.

1.2. Back Ground of Police System 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 AFIS (in Madhya Pradesh), 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 Criminal 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 (SCRB), and District Crime Records Bureaus (DCRB) and to facilitate statistical analysis of crime and criminals related information with the States and monitoring agencies.

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

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

1.2.2. Common Integrated Police Application (CIPA)

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

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

CIPA is a stand-alone application developed to be installed in police stations and to support the crime investigation and prosecution functions. CIPA is a centrally managed application: an application core centrally developed and is installed in police station. Any state-specific customizations are evaluated and made on a need basis.

The core focus of the CIPA application is the automation of police station operations. Its core functionality includes the following modules:

(i) Registration Module

(ii) Investigation Module

(iii) Prosecution Module.

There is also a Reporting module that addresses basic reporting needs.

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

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

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

1.2.3. Crime and Criminal Tracking Network System (CCTNS)

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

CCTNS aims at creating a comprehensive and integrated system for enhancing the efficiency and effectiveness of policing at all levels and especially at the Police Station level through adoption of principles of e-Governance. CCTNS will operate through the creation of a nationwide networked infrastructure for evolution of IT-enabled state-of-the-art tracking system around "investigation of crime and detection of criminals" in real time, which is a critical requirement in the context of the present day internal security scenario.

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

1.3. CCTNS Implementation Framework

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

The role of the Centre (MHA and NCRB) focuses primarily around planning, providing the core application software (CAS) (to be configured, customized, enhanced and deployed in States. Please refer to "**Annexure – VII Scope of Services"**), managing (from a high level) and monitoring the program. States would drive the implementation at the state level and would continue to own the system after deployment.

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

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

1.3.1. Goals of This Request for Proposal (RFP)

The primary goal of this RFP is to select System Integrator (SI) through a competitive bidding process. This volume of RFP intends to bring out all the details with respect to solution and other requirements that are deemed necessary to share with the potential bidders. The goals of RFP are further elaborated below:

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

MPCOPS under the directions of State Apex Committee and State 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 MPCOPS reserves the right to reject any or all the bids without assigning any reason. The MPCOPS 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

This section covers overview of the project i.e. its necessity, vision, & objective, expected beneficiaries of the project.

2.1. Need for the Project

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

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

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

2.2. Vision and Objectives of Project

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

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

The broad objectives of the project are as follows:

a) Improve Service Delivery to the Public

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

b) Provide Enhanced Tools for Law & Order Maintenance, Investigation, Crime Prevention, & Traffic Management

Law & Order Maintenance, Investigation, Crime Prevention, and Traffic Management are core components of policing work. Information technology can both enable and improve the effectiveness and efficiency of the core activities of the police. Police should be provided with data amenable for easier and faster analysis in order to enable them to make better and informed decisions.

c) Increase Operational Efficiency

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

d) Create a platform for sharing crime & criminal information across the country

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

2.3. Stakeholders of Project

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

- Citizens/ Citizens groups
- MHA/NCRB/Others
- State Police department
- External Departments of the State
- Non-Government/Private sector organizations

2.4. Desired Outcomes from Various Stakeholders

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

Benefits to Citizens

a) Multiple channels to access services from police
b) Simplified process for registering and tracking incidents, petitions and FIRs
c) Simplified process for accessing general services such as requests for certificates, verifications, and permissions
d) Simplified process for registering grievances against police
e) Simplified process for tracking the progress of the case during trials

f) Simplified access to view/report unclaimed/recovered vehicles and property

g) Improved relationship management for victims and witnesses

h) Faster and assured response from police to any emergency calls for assistance

Benefits to Police Department

a) Enhanced tools for investigation

b) Centralized crime and criminal information repository along with the criminal images and fingerprints with advanced search capabilities

c) Enhanced ability to analyze crime patterns, modus operandi

d) Enhanced ability to analyze accidents and other road incidents

e) Faster turnaround time for the analysis results (crime and traffic) to reach the officers on the field

f) Reduced workload of the police station back-office activities such as preparation of regular and ad-hoc reports and station records management

g) Enhanced tools to optimize resource allocation for patrols, emergency response, petition enquiries, and other general duties

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

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

Benefits to Ministry of Home Affairs (NCRB)

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

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

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

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

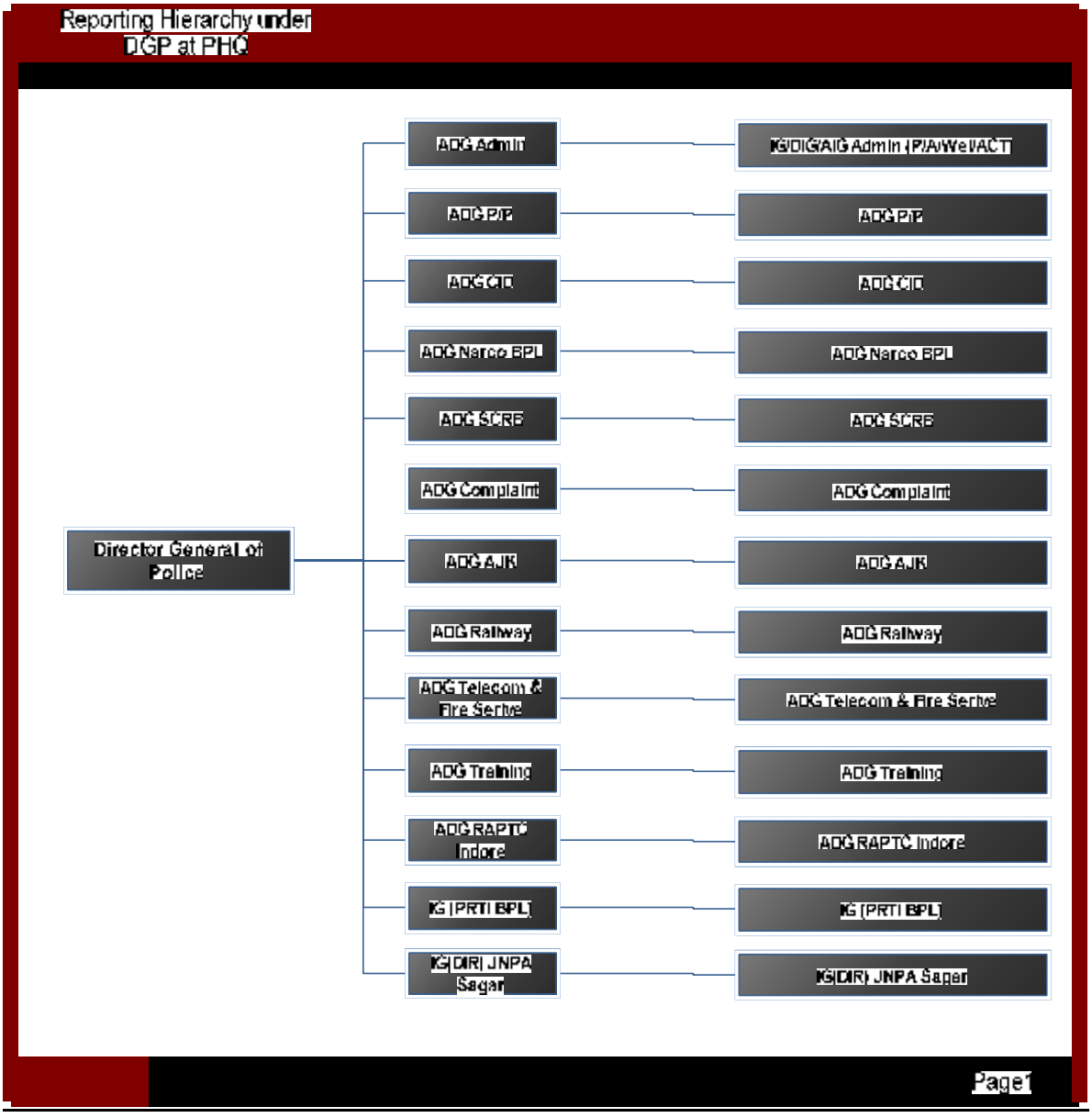
Benefits to External Departments (example: Jails, Courts, Passports Office, Transport Department, and Hospitals)

a. Seamless integration with police systems for better citizen service delivery and improved law enforcement

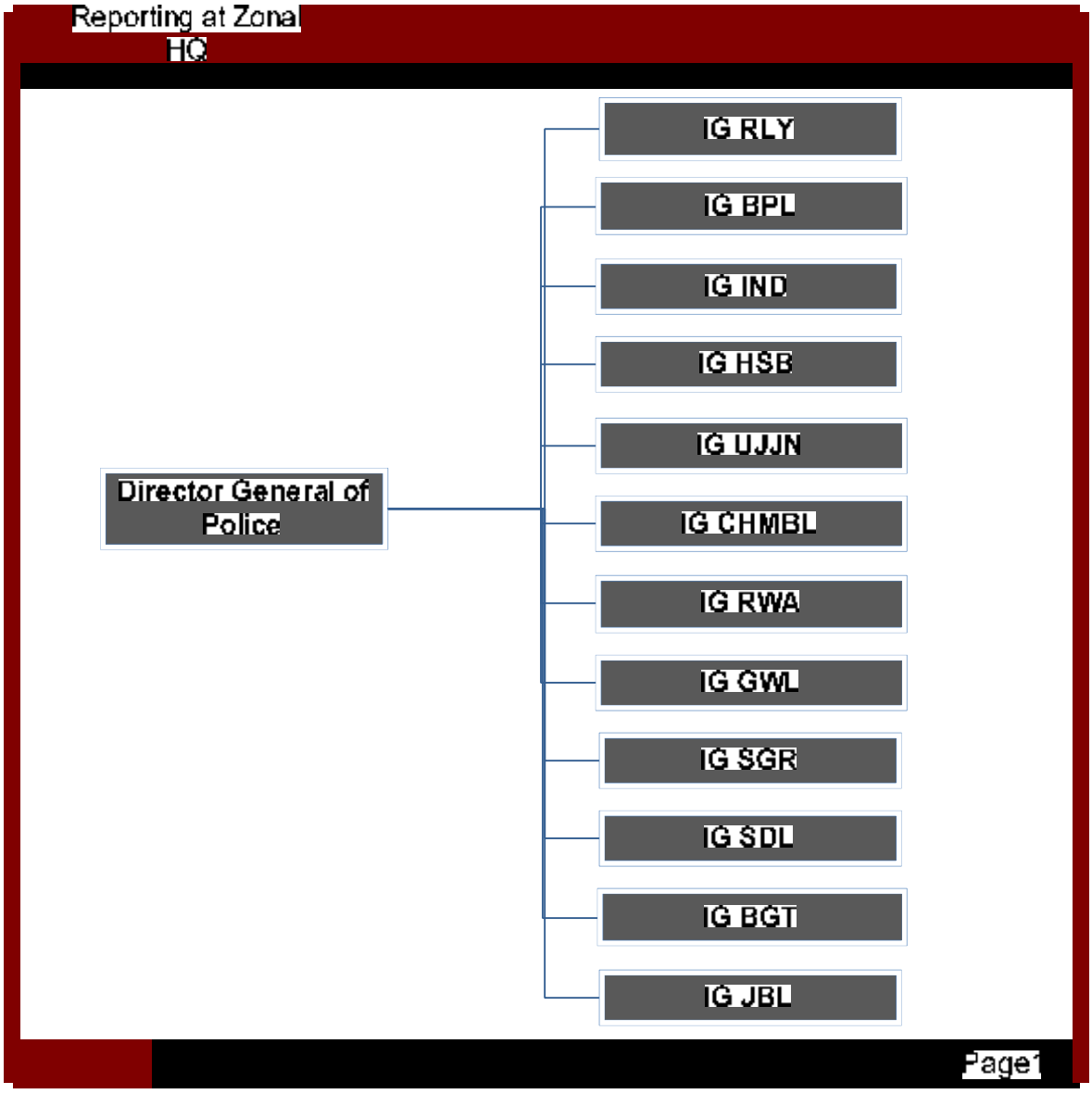
3. STATE POLICE DEPARTMENT

3.1. Organizational Structure

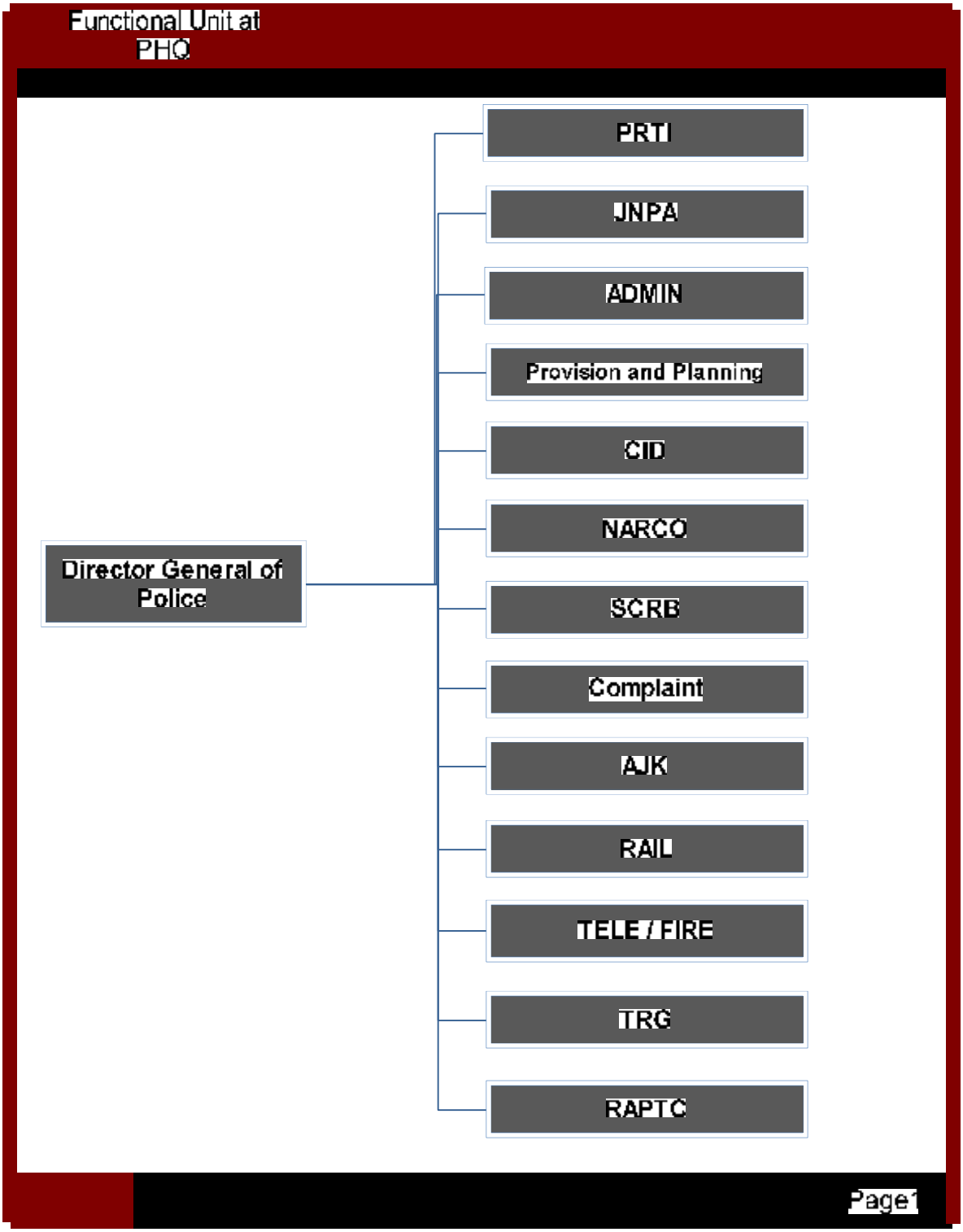
Pictorial notation of reporting hierarchy at PHQ under DGP



Pictorial notation of IG field under DGP



Pictorial notation of functional unit at PHQ



PHQ Branches functions at a Glance:

Administration:

The functions of this branch include administration, selection, recruitment/ promotions / disciplinary n legal case, accounts and welfare activities of Police Department.

Planning and Provision (P/P):

Planning section's work includes planning of Annual Budget Proposals / Supplementary Budget proposal / Revised Estimate / Re-appropriation and allotment of budget to Police Units and Branches. It also includes Sanction of all new post / Establishment of New Offices / Police Station and out posts / Training Institutions / Statistical data of sanction posts and establishment/ Recommendations of Central Finance Commission.

Provision section's work includes purchasing of Vehicles, Arms/ ammunition, various office equipments, furniture etc. under Modernisation of Police force Scheme and General Budget. This section also provides uniform & Kit, Stationery to different units of Police department. This unit also deals with PHQ press, Store section, M.T. pool etc.

Criminal Investigation Department (CID):

This department mainly works for verification of the state government cases. The coordination of the work of the CID with that of the district Police is entirely in the hands of the in-charge of that department. Superintendents would immediately report to him for any case of special difficulty, which baffles the local police, cases of professional or organised crime, counterfeit coining or note forgery. In-charge is to decide whether an officer of the Criminal Investigation Department should be deputed to assist the local police or whether the case should be taken out of the hands of the local police for investigation by CID.

Narcotics:

Main working of this department is to Prevent, investigate and control on Drug trafficking, Drug Abuse, Narco-Terrorism and Drug related Crime situation in Madhya Pradesh as well as to conduct studies and impart training in multifarious aspects of Narcotics crime, Demand Reduction and De-addition.

State Crime Record Bureau (SCRB):

SCRB gathers all statistical data about crime from all over the State and analyses the same. Carefully maintained data helps in furnishing a clue to the probable identity of the criminal. It keeps in constant touch with the National Crime Records Bureau and exchanges data. It has its own computer division. The SCRB is also working as a nodal agency for the work of computerization in Madhya Pradesh.

Complaint:

In this branch various complaints pertaining to police from all sources viz. President's Secretariat, Prime Minister's Office, Secretariat, Ministers, MP/ MLAs. National/ State Human Rights Commission, Women/ Minority Commission etc. are registered, enquired into and appropriate

action is taken. Complaint against any police officer of the Madhya Pradesh Police may also be lodged here. Status of the complaint may be checked at any time by the complaint ID number.

Anusuchit Jati Aaivam Kalyan Vibhag (AJK):

This department monitors crimes occurring against schedule caste and schedule tribes in the state. Each of the districts in the state has an AJK Police Station. All cases that are registered under Schedule caste and schedule tribe Act and Indian Criminal Law (Bhartiya Dand Vidhan) are analyzed by this department.

Railway:

Government Railway Police (GRP) needs information to take care of the crimes and complaints related to the railways. This Branch of the State Police with over 2100 Officers and other ranks is involved in the investigation, detection and prosecution of the offences concerning the railways within the State of M.P. and also coordinates with the GRP of the adjoining States and the Railway Protection Force. This Branch also prepares a detailed statement of the crime situation and important happening related to its field of functioning annually.

Fire Services:

Duties and Functions of this branch to save life and property from fire, To conduct rescue operations, to assist/evacuate people during natural calamities/disasters, such as, floods, earthquakes etc., To educate and create public awareness for fire prevention and fire fighting, To provide guidance to Hotels, Hospitals, Factories, Cinema Houses etc.

Telecommunication:

Telecom department is responsible for commissioning of Advance Radio Trunking System, integrated communication system like (VHF, EMAIL, and POLNET etc). It also keeps vigilance for Improvement in Training Standards and Level, Re-appropriation of police radio personals all over the state to meet the current challenges of law and order as well as to provide satisfactory and quick communication to take action against culprits, during VVIP visits, elections and natural disaster.

Training:

Work of this section is to provide training to police personnel in different domains and enhance their skill set so that they can perform their duties in synchronization with necessities of the present age. MP Police department has 10 training institute across the state i.e. 15th BN, 6th BN, APTC Indore, PRTS Indore, PTS Panchmari, PTS Indore, PTS Umaria, PTS Tigra, PTS Rewa, JNPA Sagar. Training is provided to the directly recruited Dy. SP and the Sub Inspectors / Subedars. Training of Pre-Promotion Courses for Inspectors and Sub Inspectors is also provided. The wing also conducts various in-service courses on Dept. Enquiries, Human Rights, Personal Skills, Development, Investigation, Economic Offences, Vertical Interaction Stress management etc.

RAPTC:

Purpose of establishment of RAPTC is uniformed training of directly recruited Platoon Commanders and SAF Constables and also to organize the special weapons and tactics course for SAF & DEF Personnel viz. Probationer: Dy.S.P, Subedars and Sub-Inspectors.

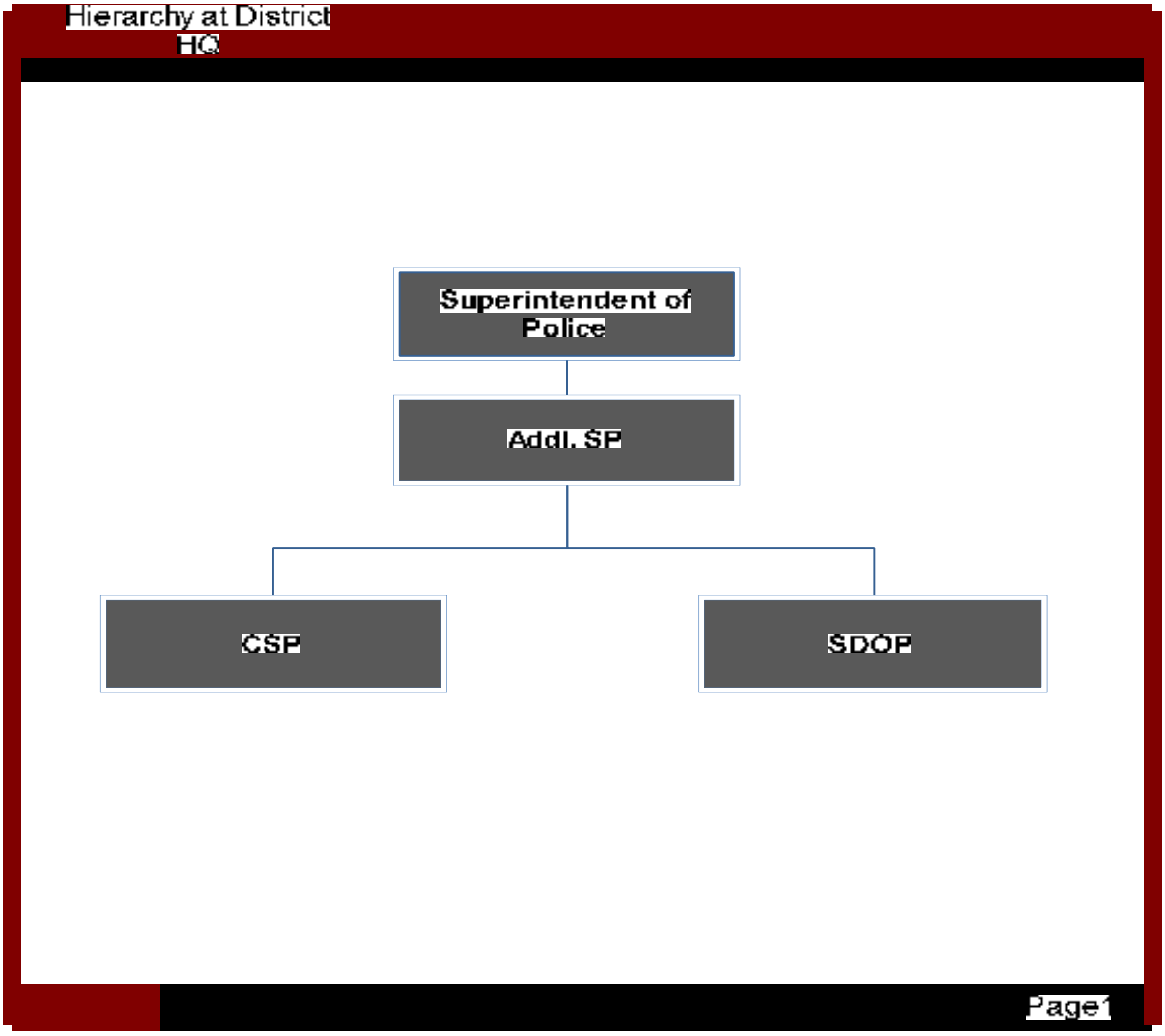
Police Training & Research Institute (PTRI):

PTRI Keeps track of Road Accidents in comparison to Registered Vehicles, Road Accidents in comparison to State Population, Road length vs. increase in accidents, Collects data for accidents from all the districts on a monthly basis, Compounding fees and challans, Details of Road Accidents due to transport of Hazardous substances, details of road safety fund that is managed by Provision and Planning Department and Accounts section.

JNPA:

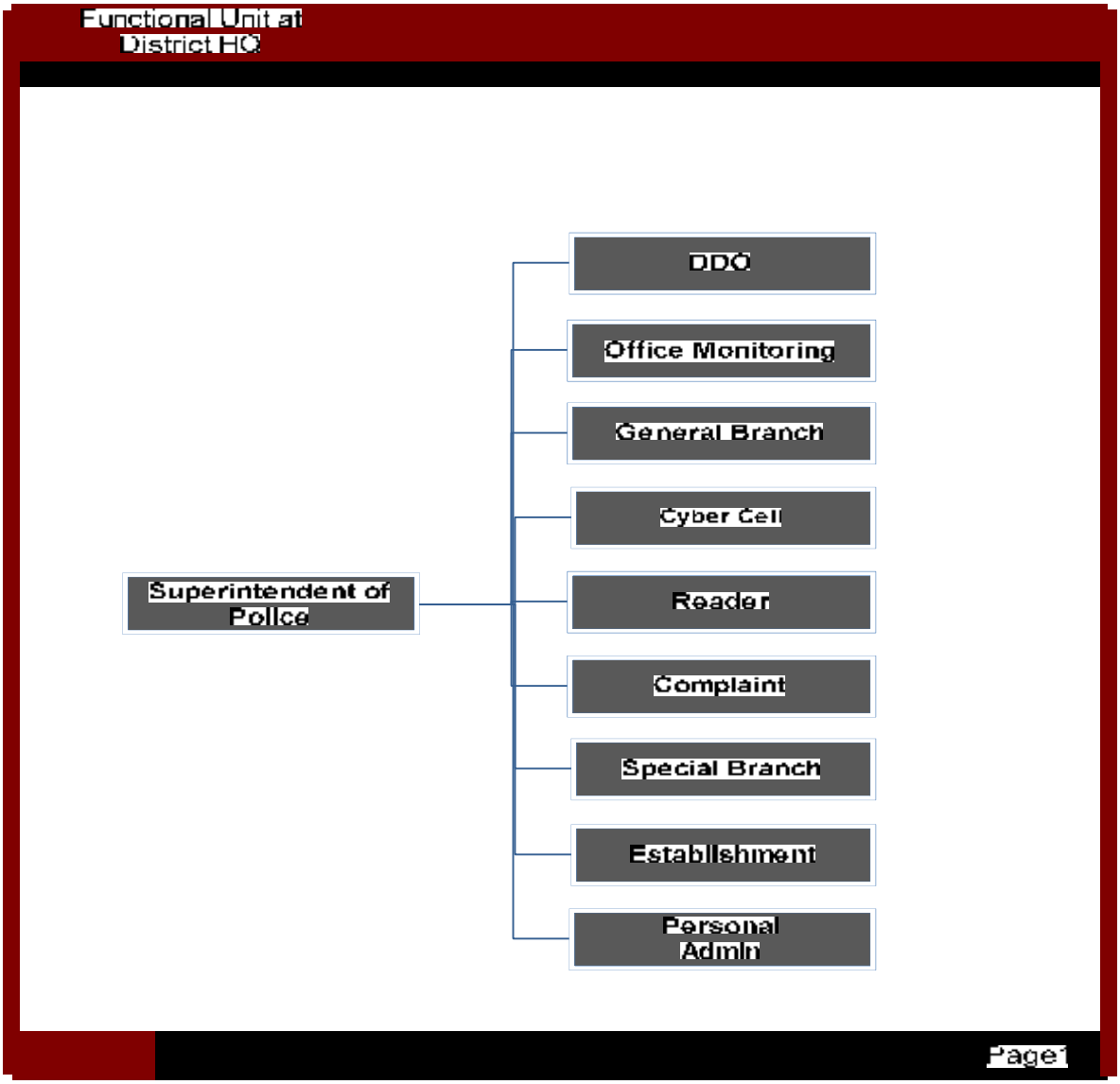
The Academy has also been the training ground for Home Guards, Jail Officers, Excise and Transport Officials, Public Prosecutors and Deputy Collectors, and other Executive Magistrates. Here emphasize has also been given to develop personality, emotional intelligence, requisite attitudes, character, leadership and to train intellect sufficiently, so that the trainees inculcate officer like qualities.

Pictorial notation of Hierarchy at DHQ



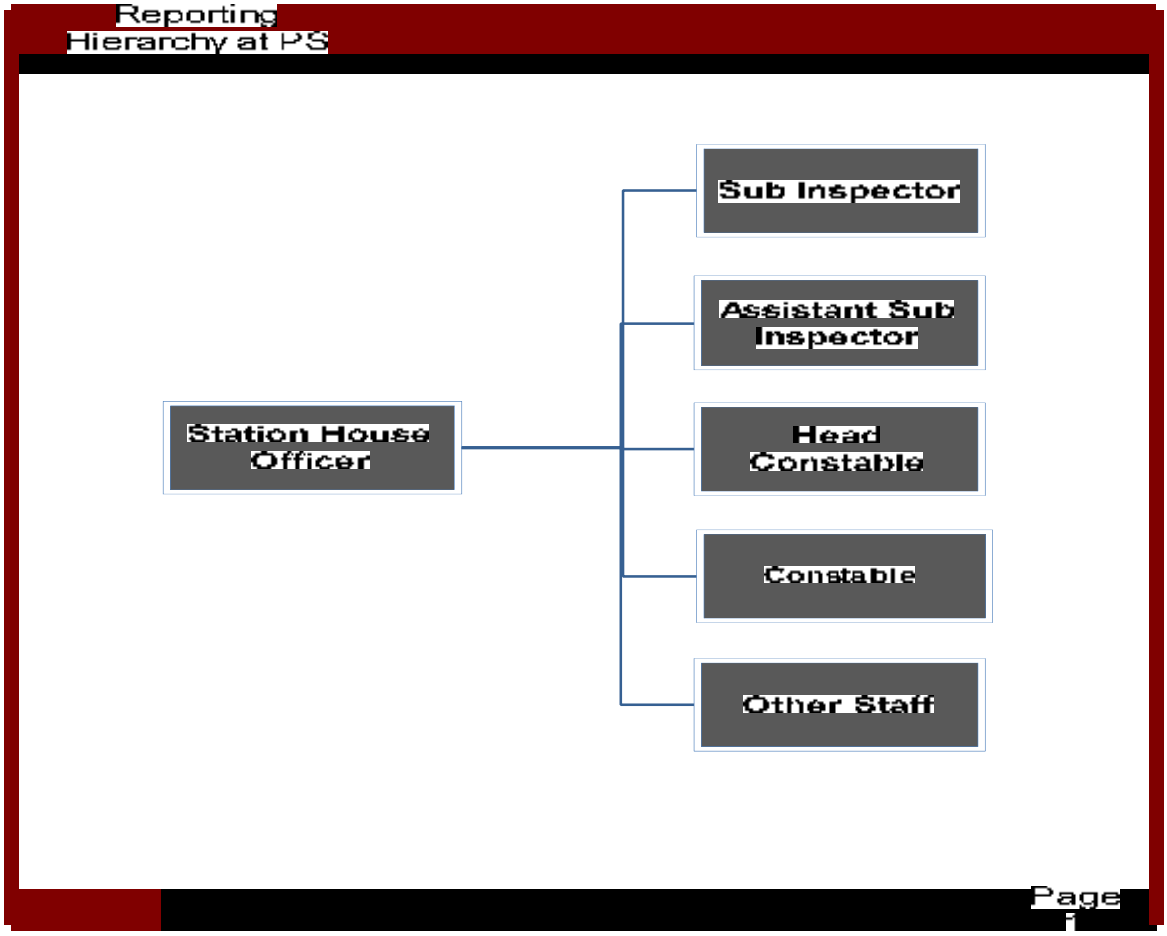
Superintendent office is a topmost office of police at District level, headed by IPS officer (i.e. Superintendent of Police). Madhya Pradesh has 53 offices of Superintendent of Police including 50 Districts and 3 Railway Districts. All the districts of MP have SP offices to maintain law & order and peace at district. These offices have multiple sections to support different areas.

Pictorial notation of Functional unit at DHQ



All these sections are performing functions for serving different areas like Reader Section initiates circulars for identifying reason of crime and its resolution, watch on crime's information, circulation & execution of warrant and summons to concerning police stations and other concerning officers which comes from Zone/ Range offices in case of severe crimes or else. Establishment section takes care of Transfers, postings, attachments, promotions. Special Branch keeps close watch on the activities of Spy's and Political Leaders, Jansunwai and VIP security also comes under their responsibility. General Branch takes care of fund related activities. Complaint branch taking care of the complaint which comes from citizens. Personal Administration section takes of Departmental enquiries etc. Cyber Cell provides technical support to the investigation agencies on cases. DDO takes care of activities related to funds and payroll. Office Monitoring Section takes care of summons/ warrant and crime statics. They are taking care arrived, executed, and pending summons/warrants. These summons and warrants send to concerning IGs.

Pictorial notation of Hierarchy at Police Station



The police station is headed by SHO. One or more outposts make a Police station Area. Police station has responsibilities like Prevention of crime, Detection of Crime, Investigation of cognizable offences, Conduct of supervisions, Protection of life and property, Maintenance of peace and order, Intelligence collection, Security management, Enforcement of legislations etc. The MHC (Moharrir. Head Constable) at the Police station maintains all the records of a Police station. Duty of all the Police personnel in that Police station is allocated by the MHC Like who is performing Patrolling in which areas, who is on which nakas duty etc.

The sentries at the Police station provide 24 hour security to the Police Station. Apart from maintaining the law and order in the area of jurisdiction, it also keeps a record of the major influential persons in the area, various political parties' information etc. The Police station also houses barracks & messes for providing boarding and lodging to the Police personnel. It also has a control room which maintains the communications between other Police station in the district and Madhya Pradesh Also has a stock room which is used to store all the materials seized.

3.2. Existing System

During AS-IS analysis, software applications have been identified those are being used by MP Police.

Existing Applications used by MP Police		
Motor Vehicle Coordination System		**MVCS**
1.	Project Description	MVCS supports police department on managing information of lost/stolen/recovered vehicles along with vehicles involved in crime. This facilitates police personnel on cross verification of vehicles across the country and equipped police to provide quick services to citizen.
2.	Category	Liable to Integrate with upcoming CAS Application.
3.	Technical Details	Windows based, Front End-VB, Back End-SQL
4.	Deployment Details (Geographical reach/no. of police station covered)	SCRB, Bhopal(MP)
5.	Issues/Challenges	NA
Common Integrated Police Application		**CIPA**
1.	Project Description	CIPA was considered as a major step towards computerization of police stations and developed to provide automated working on crime registration, Investigation, Prosecution, management of police station register's records. It provides customized reports on specific needs of Police stations.
2.	Category	Liable to Migrate into upcoming CAS Application.
3.	Technical Details	Operating System-Linux Front end- Java Backend- Postgres SQL
4.	Deployment Details (Geographical reach/no. of police station covered)	373 Police Station across the state.
5.	Issues/Challenges	It's a decentralized application; each police station manages their data separately. All the desired (State

		Specific) reports were not achieved in it. Instantaneous access on particular record of any location is not available for higher level. limited facilities for PS.
Crime and Criminal information System		**CCIS**
1.	Project Description	Application manages information about crime and criminal by digitizing 7 IIFs used for a case; of all the police stations across the state.
2.	Category	NA
3.	Technical Details	**Operating System**- Windows **Back End**- SQL **Front End**- VB
4.	Deployment Details (Geographical reach/no. of police station covered)	SP Offices field, SCRB, NCRB.
5.	Issues/Challenges	CCIS's data is incompetent and unreliable due to lack of interest of police officials while filling the data into the system.
MP Police Payroll System		
1.	Project Description	System provides automated way of salary calculation and generation of pay bills and different schedules along with pay slips. It's a complete payroll management system for MP Police Department.
2.	Category	Integration
3.	Technical Details	Windows based, FoxPro (Backend & Frontend), Decentralized
4.	Deployment Details (Geographical reach/no. of police station covered)	At Police Station Level
5.	Issues/Challenges	NA

Emailing System		
1.	Project Description	It's a complete email application and intended to get email facility for Police officers.
2.	Category	Integration
3.	Technical Details	Centralized Application
4.	Deployment Details (Geographical reach/no. of police station covered)	SCRB
5.	Issues/Challenges	NA
MP Police Web Portal		
1.	Project Description	MP Police Web portal is complete informative and service portal towards police personnel's, citizens, and government departments. Portal consisting all the information of initiatives towards Police personnel, Citizens, and government. Portal has email interface for police personnel, complaint logging facility and directives for citizens. Portal consist all the information of posted IPS and Non IPS cadre officials, circulations of tenders, Traffic education, welfare activities, citizen rights, duty of citizens etc.
2.	Category	Integration
3.	Technical Details	Windows based, Front End-Asp.net, Back End-SQL
4.	Deployment Details (Geographical reach/no. of police station covered)	Web Application accessible to all the police locations.
5.	Issues/Challenges	NA
Portrait Building		
1.	Project Description	Application has been designed by NCRB to acquire sketch of criminal or lost person so that department can track criminals or lost person according to the designed sketch.

2.	Category	Integration
3.	Technical Details	Windows based Application
4.	Deployment Details (Geographical reach/no. of police station covered)	Stand alone at DO and running at DO/HO
5.	Issues/Challenges	NA
Talaash		
1.	Project Description	To gather/ maintain/ circulate information of unidentified persons/dead bodies across the country as per the investigation need on cases of police department.
2.	Category	Integration
3.	Technical Details	Windows based application
4.	Deployment Details (Geographical reach/no. of police station covered)	SCRB, PHQ (Bhopal)
5.	Issues/Challenges	NA
Automated Finger Print Identification System		**AFIS**
1.	Project Description	To Acquire the accurate information of finger prints by matching current sample with the stored database, So that person can be easily identified by the system's result. System is being run in two levels and manages distributed database system i.e. database of finger prints are managed at district level as well as in central server at SCRB Bhopal. It has 30 PRI lines for data transmission so that at a single point of time 30 districts can send their data. Districts terminal are treated as remote query station when they are fetching information from the central server.
2.	Category	Integration
3.	Technical Details	**At Server End** - Oracle as RDBMS, OS- Linux. **At Client End** - Oracle as RDBMS, VB as Front End, OS-

		Windows.
4.	Deployment Details (Geographical reach/no. of police station covered)	Distributed system running at DO level.
5.	Issues/Challenges	NA
Automated Vehicle Locating System		**AVLS**
1.	Project Description	Automated vehicle locating system supports police control room to track the current position of police vehicle so that nearest vehicle can be made available to the suspected areas. This software communicate to the GPS devices connected to the police vehicles and trace their current location, on the basis of their location nearest vehicles are directed to the suspected areas.
2.	Category	Integration
3.	Technical Details	Backend- SQL Server
4.	Deployment Details (Geographical reach/no. of police station covered)	Bhopal, Indore
5.	Issues/Challenges	NA

3.3. Existing Data Center Physical Infrastructure

Currently State Data Center (SDC) is under construction at Bhopal and expected to be operational by June 2011. The implementation time lines of CCTNS at all Police Stations and DC/DR is September 2011.

If the SDC will not ready till the timelines of CCTNS implementation, MP Police Server room may be temporarily utilized for installation of DC equipments. After the completion of SDC all the DC equipment shall be moved to SDC.

3.4. Existing WAN Infrastructure

MP Police currently doesn't have its own wide area network. Currently MP State DIT is creating State Wide Area Network (SWAN) to provide network connectivity to all the government departments. As per the information obtained, till date it has 149 POPs (Point of Presence) operational across the state. SWAN can be considered as a one method of network connectivity for the CCTNS project.

Details of SWAN's Point of Presence across the state attached as an **Annexure: X Present Status of SWAN at State.**

3.5. Existing Client Side Infrastructure

MP Police has IT infrastructure under projects like modernization and CIPA etc.

457 Dual Core, 201 Laser Printers and 201 Scanners have been purchased by MP Police under CIPA project. Under Modernization plan 725 Dual Cores, 51 Laser Printers and 62 scanners have been purchased by MP Police. Detailed statistics of IT infrastructure details acquired by MP Police have been depicted in the table below:

Project Details	P III	P IV	Dual Core	Laser Printer	Scanner
HW Distributed Under CIPA Project			457	201	201
HW Distributed Under Modernization Plan	44	896	725	51	62
Total	44	896	1182	252	263

All the CIPA locations details have been provided in **Annexure XVII - CIPA Hardware Distribution (Phase wise).**

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

Madhya Pradesh Police department has 10 Training centers those can be used for CCTNS training purpose, they are: 15 BN Indore, 6th BN Jabalpur, APTC & PRTS Indore, PTS (Panchmari, Indore, Umaria, Tigra, Rewa), JNPA Sagar. Earlier 30 nodes 2 switches networking was done on these

training institutes and for aiming CCTNS project's personnel training program; later 24 node 2 switches networking has been done. Along with these 10 training institutes, 53 District offices, 7 Range offices have been equipped with network connectivity to provide training under CCTNS. At Range level 12 nodes 1 switch connectivity has been established. Furthermore at District level, earlier 12 nodes 1 switch networking was done and for CCTNS point of view another 11 nodes 1 switch networking has been done. Distribution of hardware at 10 Training center is 22 PC, 2 servers and peripherals like printer, UPS etc, at SP offices 10 PC, 1 server and peripherals like printer/UPS, at Range offices 10 PC, 1 server and peripherals like printer/UPS.

3.7. Core Application Software (CAS)

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

For Customization please refer **Annexure- VII Scope of Services.**

This section covers all the details of Core application software designed for center and state. This section focuses on the entire functional, nonfunctional, and technical requirement for implementing CAS.

3.7.1. Volume-I Scope of Services

Core application software has been provided by NCRB to all states/ UTs and it covers generic requirements. Core application software has been developed to be used at two levels i.e. center and state/UT. The functional architecture and technical architecture of the core application (state) and core application (center) has been provided in **Annexure- VII Scope of Services**:

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

3.8. CAS (Center):

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

Overview of Services for CAS (Center):

State-SCRB-NCRB Data Transfer and Management:

The service shall enable the NCRB to receive, transform, and collate the crime, criminal, and related data from States/UTs, to organize it suitably to serve NCRB requirements.

Crime and Criminal Reports:

The service shall enable authorized personnel to generate the reports and perform analysis on the central crime, criminals, and related data repository of the nation.

Crime and Criminal Records and Query Management:

The service shall enable the authorized personnel to view various registers and perform basic and advanced queries on the central crime, criminals, and related data repository of the nation.

Talaash Service:

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

Person of Interest:

The service will enable the user to search for persons of interest such as persons wanted on outstanding warrants, accused, charged habitual offenders, convicts, etc. across the national database.

Registered Vehicle and Vehicle of Interest Service:

The service will enable the user to search for registered vehicles and vehicles of interest such as, missing / stolen vehicles, abandoned / unclaimed vehicles, and vehicles involved in traffic incidents across the national database.

Publication Service:

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

NCRB Citizen Interface:

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

NCRB Interface for RTI:

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

3.9. CAS (State):

CAS (State) covers functionality that is central to the goals of CCTNS and is common to all States and UTs. It would focus primarily on functionality at police station with special emphasis on crime investigation and criminals' detection. The following are the main function blocks that would comprise CAS (State):

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

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

It is envisioned that CAS (State), once operational, will significantly enhance the outcomes in core police functions at Police Stations. It will do so primarily through its role- and event-orientation, that helps police personnel (playing different roles) in more effectively performing their core functions, and that relieves police personnel from repetitive tasks that claim much of their time while returning low or no value. In order for CAS (State) to achieve the above goals, it is envisaged to meet the following requirements:

- It will lay special emphasis on the functions at police stations with focus on usability and ease of use of the application.
- It will be designed to provide clear and tangible value to key roles at the Police Station: specifically the SHO (Station House Officer), the IO (Investigation Officer) and the Station Writer.
- It will be event-and role-driven.
- It will be content/forms-based, with customized forms based on requirements.
- It will be a flexible application, event and role-driven system where actions on a case can be taken as required without rigid sequence / workflows.
- It will eliminate the need for duplicate and redundant entry of data, and the need for repetitive, manual report preparation – this freeing valuable time and resources for the performance of core police functions.
- It will be intelligent and help police perform their roles by providing alerts, highlighting key action areas, etc.
- Ability to view and exchange information amongst Police Stations, between Police Stations and other Police formations and with external entities including citizens.
- Reporting and data requirements of higher offices must be met at the State Data Centre/SCRB

level and not percolate to the police station level.

- Central facilitation and coordination; but primarily driven and owned by States/UTs where States/UTs can configure and customize the CAS for their unique requirements without the intervention of the central entity.

Services in CAS (State)

Citizens Portal Service:

This service shall enable Citizens to request services from Police through online petitions and track status of registered petitions and requests online. Citizens requests/services include passport verification services, general service petitions such as No Objection Certificate (NOC) for job, NOC for vehicle theft, NOC for lost cell phone/passport, Licenses for arms, processions etc.

Petition Management Service:

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

Unclaimed/Abandon Property Register Service:

The service shall enable the police personnel to record and maintain unclaimed/abandoned property registers and match unclaimed/ abandoned property with property in lost/stolen registers.

Complaint and FIR Management Service:

The service shall enable the police personnel to register and process the complaints (FIR for cognizable complaints, Non-Cognizable Report for non-cognizable, Complaint Report for genera complaints, etc.) reported by the public.

PCR Call Interface and Management Service:

The service shall enable the police personnel to register and process the complaints as received through the Police Control Room through the Dial 100 emergency contact number.

Investigation Management Service:

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

Court and Jail Interface and Prosecution Management Service:

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

Crime and Criminal Records and Query Management Service:

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

Police Email and Messaging Service:

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

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

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

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

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

State-SCRB-NCRB Data Transfer and Management Service:

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

State CAS Administration and Configuration Management Service:

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

User Help and Assistance Service:

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

User Feedback Tracking and Resolution Service:

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

Activity Log Tracking and Audit Service:

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

User Access and Authorization Management Service:

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

3.10. DEVELOPMENT OF CCTNS CORE APPLICATION SOFTWARE (CAS)

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

CAS (State) would be built as a platform at NCRB addressing the core requirements of the Police Station to provide a basic framework to capture and process crime and criminal information at the police station while providing the MP Police with the flexibility to build their state specific applications around it and in addition to it. CAS (State) will be provided to States for deployment. A bulk of the functionality would be added at States/UTs discretion and would be added as extensions to the CAS (State) by the System Integrators (SI) chosen by the States/UTs.

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

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

3.11. TECHNOLOGY STACK FOR CAS (STATE)

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

4. ROLE OF SOFTWARE DEVELOPMENT AGENCY (SDA) IN SUPPORTING CAS

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

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

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

Each of these activities is detailed out below.

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

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

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

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

- Appropriate communication on change required has taken place.
- Proper approvals have been received from CAS Core Group/CTT/CPMU.

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

Technical Program Management of Implementation of CAS (State):

After successful certification, the SDA will hand over the certified CAS (State) to State through NCRB. While NCRB will facilitate the transfer, the successful transfer of CAS to State on time is SDA's responsibility. During the period of CAS Solution Design and Development and the Operations and Maintenance Phase following that, the SDA shall provide technical program management services in implementing CAS in State. Through the Technical Program Management,

the SDA shall extend all the necessary support to the State SI and ensure that the SI successfully configures, customizes, and deploys CAS (State) in State. The SDA's Technical Program Management responsibilities include but are not limited to:

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

- **Data Migration Utility:** The SDA shall develop a Data Migration Utility/application with all the formats and tools to load the data into the state databases. This will be provided to State will enable the State SIs to migrate data from legacy/paper based systems to the CAS databases.

- **Language Localization Support:** Proving interface in local languages is a key requirement of CAS (State). The SDA shall build CAS (State) with interfaces in English and Hindi; and also build CAS (State) in such a way that it can be configured for interfaces in other local languages at the State level by the State SIs. In addition, the SDA shall assist the State SIs in customizing CAS (State) to support local language interface and ensure the development of interface in local languages.

- Supporting the SI to ensure that the CAS (State) that is configured and customized by the SI in the State successfully passes the User Acceptance Testing (UAT) with below milestone.

  - Configuration of CAS (State)
  - Customization of CAS (State)
  - Data Migration of CAS (State) related data from the legacy systems and / or manual records to CAS (State)
  - Infrastructure Sizing related to CAS (State)
  - Commissioning and Deployment of CAS (State)
  - Infrastructure Environment Performance Turning related to CAS (State)
  - Maintenance of CAS (State)
  - Integration of CAS (State) with external agency solutions
  - Integration of CAS (State) with additional solutions being integrated by the SI at the State

- Seamless data exchange from CAS (State) to CAS (Centre)

- Troubleshooting, resolution and escalation with State SIs; and ownership of end-to-end data exchange between the CAS (State) and CAS (Centre) needs to ensure seamless and real-time data exchange.

SCOPE OF THE PROJECT

4.1 Geographical Scope:

It is proposed to roll out CCTNS in phases. Deployment of hardware, connectivity, CAS and other infrastructure across all police stations and at DC with rollout of CCTNS at all Polices stations would take Place in the first phase. In second phase Zone, Range, Districts, PCR, FSL, FPB, SCRB, PHQ, and DR site are required to be covered under the project. For the third phase SI has to rollout CCTNS at all the balance locations.

Police Locations at a Glance:

MPP Locations Detail		
S. No.	**Units/Offices**	**Total Numbers**
1.	Police Stations	948
2.	Traffic Police Stations	48
3.	Sub-Divisional Police Offices/Additional (SP)/DSP	288
4.	District Police Control Room (PCR)	50
5.	Districts	53
6.	Ranges	16
7.	Zones	12
8.	SCRB	1
9.	State Police Control Room (SSR)	1
10.	State Finger Print Bureau	1
11.	State Forensic Science Lab	1
12.	PHQ	1
Total :		**1420**

The core focus of each of the three phases is delineated below:

CCTNS First Milestone

Geographical Coverage:

During the primary priority of the project, rollout of all the police stations (CIPA & Non CIPA) & Data center must be covered and fully functional till September 2011, any police station should not be nonfunctional after this timeline. The Roll out would include installation and commissioning of application & hardware, connectivity, other Infrastructure and associated services (such as handholding, digitization etc.).

Details of all 996 police stations are covered in **Annexure XI Police Station (Non CIPA), Annexure XII Non CIPA Police Station**, that includes CIPA (Phase-I, II, III) and **Annexure XVIII Traffic Police Station**.

CCTNS Second Milestone

Geographical Coverage:

During Second Milestone of CCTNS, PHQ, SCRB, Zones, Ranges, Districts, SSR, FSL, FPB, District Police Control Room i.e. 136 Locations and Disaster Recovery Site must be covered for the installation and Commissioning of hardware, connectivity and other infrastructure and associated software & services. Second milestone must be achieved within 6 months after completion of first milestone.

CCTNS Third Milestone

Geographical Coverage:

During Third Milestone of CCTNS, Sub-Divisional Police Offices, Addl. SP/DSP i.e. 288 Locations shall be covered for the installation and Commissioning of hardware, connectivity and other infrastructure and associated services. Third milestone must be achieved within 6 months after successful completion of Second milestone.

CCTNS Forth Milestone:

Forth milestone is planned for the operation and maintenance of CCTNS project including updation for release of subsequent versions of CAS and the large enhancements initiated at the state level. Time period of Operation & Maintenance Phase is 5 (Five) Years from the date of Go-Live

As CCTNS would be rolled out under defined milestone across the state, maps for implementation support is attached as **Annexure II of annexure to Volume – I Geographical scope of CCTNS**.

Note:

The information pertaining to the number of police stations, circle offices, and other such units, the approximate number of personnel within each unit is attached as an Annexure - I of Annexure to Volume – I Police sanctioned strength.

Condition of Police stations in Madhya Pradesh varies. Some Police stations in Madhya Pradesh have their own building while there are some Police Stations that do not have their own building and thus have taken building on rent. SI would do site survey and identify appropriate room in Police stations for the installation of computer systems and other peripherals.

Functional Scope

Functional scope covers incorporates IT solutions along with the detailed functional requirements that will be covered under the project. It contains functional requirements at the different levels of the organizations covering police stations and higher offices. This section will also list the functionality that the state wants specifically for itself. It incorporates customization requirements of the core application developed and provided by the Centre to the State.

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

Details about interfaces that need to be developed on the existing systems to interface with CAS (State) have been provided in the functional scope provided as an Annexure VII Scope of Services to this RFP.

Details of existing systems have been incorporated in point 3.2 of this RFP.

CCTNS and other Mission Mode Projects:

The National e-Governance Plan (NeGP) of the Govt. of India aims to cooperate, collaborate and integrate information across different departments in the Centre, States and Local Government. Government systems are characterized by islands of legacy systems using heterogeneous platforms and technologies and spread across diverse geographical locations, in varying state of automation, make this task very challenging.

The NSDG (National e-Governance Service Delivery Gateway) is an integrated MMP under the National e-Governance Plan (NeGP), can simplify the above task by acting as a standards-based messaging switch and providing seamless interoperability and exchange of data across the departments. NSDG acting as a nerve center, would handle large number of transactions, and would help in tracking and time stamping all transactions of the Government.

The Gateway would provide major benefits to the departments such as Multiple Delivery Channels, Better Audit Management & Time Stamping, Web enabling of Legacy Applications, Interoperability, Departmental Workflow, Seamless availability of information , Centralized Management, Shared Services.

Crime and Criminal Tracking Network and Systems (CCTNS) is a Mission Mode Project (MMP) conceptualized and sponsored by the Ministry of Home Affairs (MHA), Govt. of India (GoI) towards enhancing outcomes in Crime Investigation and Criminals Tracking; and in enhancing the efficiency and effectiveness of Police departments in all States. It is proposed to achieve this through the adoption of the principles of e-Governance and creating a nationwide, networked infrastructure for supporting an ICT (Information and Communication Technologies) enabled state-of-the-art policing system.

CCTNS aims at creating a comprehensive and integrated system for enhancing the efficiency and effectiveness of policing at all levels and especially at the Police Station level through adoption of principles of e-Governance, 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 the real time, which is a critical requirement in the context of the present day internal security scenario.

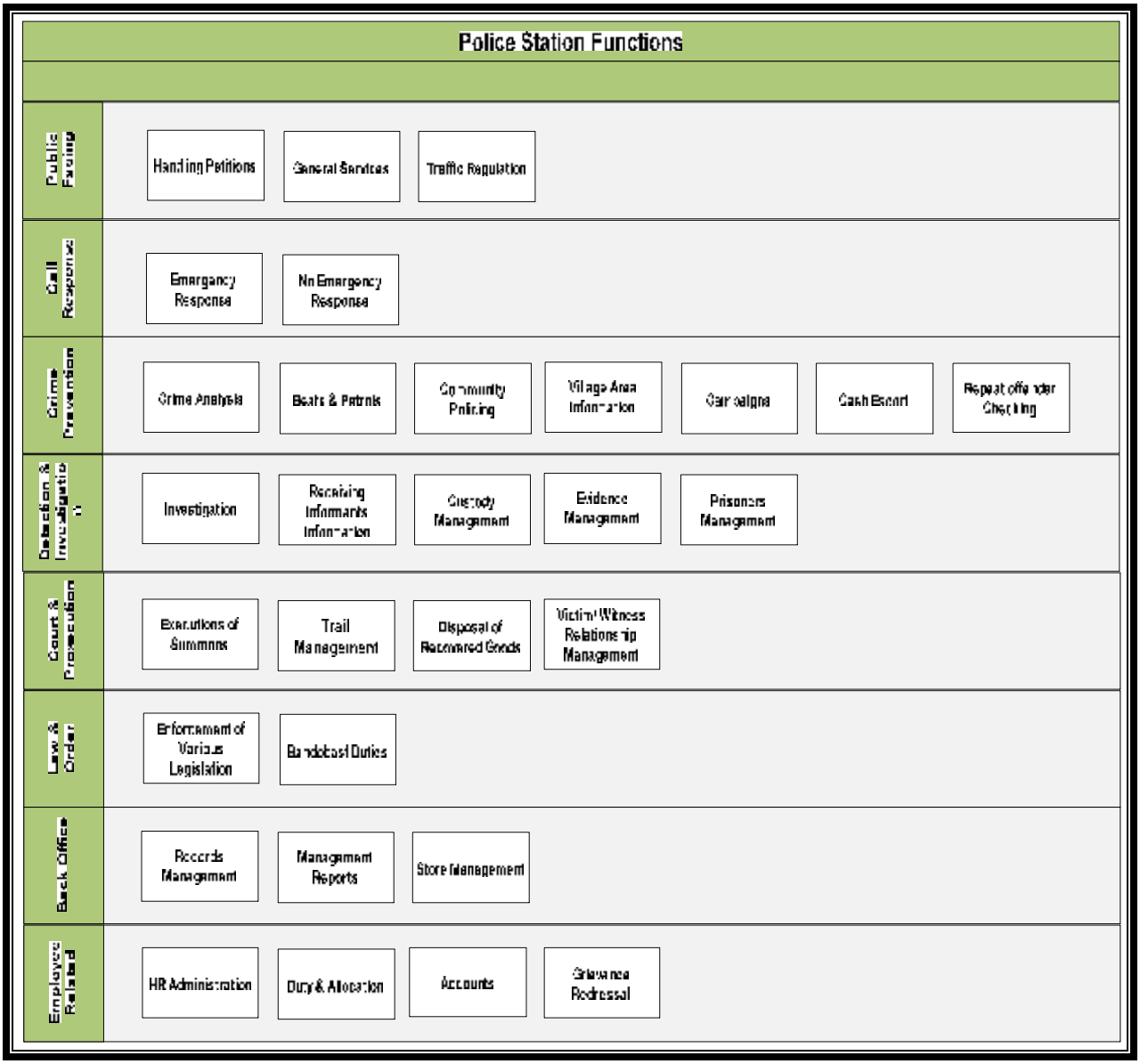
For increasing the efficacy of CCTNS it needs to be integrated with few other e-governance mission mode projects i.e. SWAN & SDC. SWAN may provide the basic network connectivity for CCTNS whereas State Data Center would be the heart of CCTNS where all information would get stored.

Brief Description of Police Station Process:

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.



4.2 Scope of Services during Implementation Phase

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

a) Project planning and management including system study and design.

b) Configuration Customization of CAS (State), Integration with CAS (Center) & Integration with Existing Identified Applications. Implementation of CAS at all locations mentioned in this RFP.

c) Supply, Installation, Testing and Commissioning of required Infrastructure at all locations.

d) Site preparation at the police locations including Data Center and DR site.

e) Service and Support for Wide Area Network connectivity.

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

g) Data migration and Digitization of Historical Data.

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

i) Capacity building

j) Handholding support

k) Support for third party acceptance testing, audit and certification.

l) Post Go-Live operation and maintenance support / services

In implementing the above, the SI shall strictly adhere to the standards set by the MPCOPS, MHA, NCRB. At all points in the execution of the project, key senior resources including the project manager must be based at MPCOPS, SCRB, PHQ, Bhopal.

The item above refers to project planning and management functions from the perspective of SI which should align with the overall project planning and management functions of the State executed through MPCOPS with the support of SPMU.

4.2.1 Project Planning and Management

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

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

a) Create an organized set of activities for the project.

b) Coordinate and collaborate with various stakeholders including the police departments, SPMU, CPMU, and SDA.

c) Establish and measure resource assignments and responsibilities.

d) Construct a project plan schedule including milestones.

e) Measure project deadlines and performance objectives.

f) Communicate the project plan to stakeholders with meaningful reports.

g) Provide facility for detecting problems and inconsistencies in the plan.

h) During the project implementation the SI shall report to the MPCOPS, on following items:

i. Results accomplished during the period;

ii. Cumulative deviations to date from schedule of progress on milestones as specified in this RFP read with the agreed and finalized Project Plan;

iii. Corrective actions to be taken to return to planned schedule of progress;

iv. Proposed revision to planned schedule provided such revision is necessitated by reasons beyond the control of the SI;

v. Other issues and outstanding problems, and actions proposed to be taken;

vi. Interventions which the SI expects to be made by the Project Director and / or actions to be taken by the Project Director before the next reporting period.

i) Progress reports on a monthly basis.

j) Interventions which the SI expects to be made by the MPCOPS and/or actions to be taken by the MPCOPS before the next reporting period;

k) Project quality assurance reports

l) Change control mechanism

m) As part of the project management activities, the SI shall also undertake:

i. Issue Management to identify and track the issues that need attention and resolution from the State.
ii. Scope Management to manage the scope and changes through a formal management and approval process
iii. Risk Management to identify and manage the risks that can hinder the project progress

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

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

Requirements Traceability Matrix:

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

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

Project Documentation:

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

Project documents include but are not limited to the following:

- Detailed Project Plan
- Updated/vetted FRS
- SRS document
- HLD documents (including but not limited to)
  - Application architecture documents
  - ER diagrams and other data modeling documents
  - Logical and physical database design
  - Data dictionary and data definitions
  - Application component design including component deployment views, control flows, etc.
- LLD documents (including but not limited to)
  - Application flows and logic including pseudo code

- GUI design (screen design, navigation, etc.)

- All Test Plans
- Requirements Traceability Matrix
- Change Management and Capacity Building Plans
- SLA and Performance Monitoring Plan
- Training and Knowledge Transfer Plans
- Issue Logs

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

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

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

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

Commission and Maintain Project Management, Configuration Management and Issue Tracker Tools at MPCOPS / SCRB

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

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

Issue Tracker: The SI shall employ a suitable and proven tool for tracking issues through the execution of the project. The SI shall install the Issue Tracking System at MPCOPS/SCRB's premises to enable State's users to access and use the same.

The SI shall commission the required infrastructure (software, hardware) for Project Management Tool, Configuration Management Tool and Issue Tracker tool and maintain the same through the duration of the project.

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

4.2.2 Configuration, Customization of CAS (state) and integration with CAS (center) & integration with existing identified applications

System Study, Design, Application Development, and Integration:

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

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

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

1) Conduct of System Study at selected locations i.e. Addl. SP office, SP office, Police Stations etc.

2) Preparation of System Requirements Specifications (SRS) for customization and different integration points with CAS (Center) and identified applications.

3) Preparation of CAS (State) implementation document with respect to Configuration, Customization and integration as per the requirement of state.

4) Preparation of the Solution Design

5) Solution Development and/or Customization and/or Configuration and/or Extension as required

6) Development of reports

7) Formulation of test plans and test cases for additional functionalities and different integrations including CAS (Center)

8) Change/Reference document include all the changes or deviations from the base version of the CAS(State)

9) Testing of the configured solution (CAS) and additional functionalities.

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

Creation of Test Plans:

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

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

High Level Design (HLD):

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

Detailed (Low Level) Design (LLD):

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

Customization and Unit Testing:

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

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

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

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

Configuration of CAS (State):

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

1) Customization for Local Language Interfaces and Support.
2) Configuring users.
3) Configuring Police Stations / Higher Offices.
4) Configuration of the User Interface (UI) as required by the State.

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

Setup of Technical Environment at Police Headquarters:

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

Regression, Integration, System and Functional Testing:

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

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

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

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

Test Reports:

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

Test Data Preparation:

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

User Acceptance Testing (UAT):

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

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

4.3 Infrastructure at the district Training Center

The details of existing training infrastructure available in the state are given below, SI may use the existing training infrastructure for capacity building purpose and if required provide additional infrastructure based on the meeting project timelines and requirements of MP Police / MPCOPS:

Existing Training Infrastructure:

CCTNS Training Centers Detail									
S. N	Location name	Server	Desktop	Laser Printer	UPS 3kva	Computer Table	Computer Chair	Printer Table	Networking
1	Bhopal	1	10	1	1	11	11	1	11
2	Rajgarh	1	10	1	1	11	11	1	11
3	Vidisha	1	10	1	1	11	11	1	11
4	Sehore	1	10	1	1	11	11	1	11
5	Indore	1	10	1	1	11	11	1	11
6	Dhar	1	10	1	1	11	11	1	11
7	Jhabua	1	10	1	1	11	11	1	11
8	Alirajpur	1	10	1	1	11	11	1	11
9	Khargone	1	10	1	1	11	11	1	11
10	Khandwa	1	10	1	1	11	11	1	11
11	Burhanpur	1	10	1	1	11	11	1	11
12	Badwani	1	10	1	1	11	11	1	11
13	Gwalior	1	10	1	1	11	11	1	11
14	Shivpuri	1	10	1	1	11	11	1	11
15	Guna	1	10	1	1	11	11	1	11
16	Ashok Nagar	1	10	1	1	11	11	1	11
17	Jabalpur	1	10	1	1	11	11	1	11
18	Katni	1	10	1	1	11	11	1	11

CCTNS Training Centers Detail									
S. N	Location name	Server	Desktop	Laser Printer	UPS 3kva	Computer Table	Computer Chair	Printer Table	Networking
19	Chhindwara	1	10	1	1	11	11	1	11
20	Narsingpur	1	10	1	1	11	11	1	11
21	Sioni	1	10	1	1	11	11	1	11
22	Sagar	1	10	1	1	11	11	1	11
23	Damoh	1	10	1	1	11	11	1	11
24	Panna	1	10	1	1	11	11	1	11
25	Chhatarpur	1	10	1	1	11	11	1	11
26	Tikamgarh	1	10	1	1	11	11	1	11
27	Balaghat	1	10	1	1	11	11	1	11
28	Mandla	1	10	1	1	11	11	1	11
29	Dindori	1	10	1	1	11	11	1	11
30	Rewa	1	10	1	1	11	11	1	11
31	Satna	1	10	1	1	11	11	1	11
32	Sidhi	1	10	1	1	11	11	1	11
33	Singrauli	1	10	1	1	11	11	1	11
34	Shahdol	1	10	1	1	11	11	1	11
35	Anuppur	1	10	1	1	11	11	1	11
36	Umaria	1	10	1	1	11	11	1	11
37	Bhind	1	10	1	1	11	11	1	11
38	Morena	1	10	1	1	11	11	1	11
39	Datia	1	10	1	1	11	11	1	11
40	Sheopur	1	10	1	1	11	11	1	11
41	Ujjain	1	10	1	1	11	11	1	11
42	Dewas	1	10	1	1	11	11	1	11
43	Shajapur	1	10	1	1	11	11	1	11
44	Ratlam	1	10	1	1	11	11	1	11
45	Neemuch	1	10	1	1	11	11	1	11
46	Mandsaur	1	10	1	1	11	11	1	11
47	Hoshangabad	1	10	1	1	11	11	1	11
48	Raisen	1	10	1	1	11	11	1	11
49	Harda	1	10	1	1	11	11	1	11
50	Betul	1	10	1	1	11	11	1	11
51	SCRB,Bhopal	1	10	1	1	0	0	0	0
52	JNPA,Sagar	2	22	1	2	24	24	1	24
53	RAPTC,Indore	2	22	1	2	24	24	1	24
54	PTRI,Bhopal	2	22	1	2	24	24	1	24
55	6th Batalian, Jabalpur	2	22	1	2	24	24	1	24
56	PRTS,Indore	2	22	1	2	24	24	1	24

CCTNS Training Centers Detail									
S. N	Location name	Server	Desktop	Laser Printer	UPS 3kva	Computer Table	Computer Chair	Printer Table	Networking
57	PTS, Indore	2	22	1	2	24	24	1	24
58	PTS, Pachmari	2	22	1	2	24	24	1	24
59	PTS, Rewa	2	22	1	2	24	24	1	24
60	PTS, Tigra	2	22	1	2	24	24	1	24
61	PTS, Umaria	2	22	1	2	24	24	1	24
		71	**730**	**61**	**71**	**790**	**790**	**60**	**790**

4.4 Site Preparation at Police Stations and Higher Offices

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

I) Provision of Local area network (LAN cables, LAN ports,).

II) Ensure adequate power points in adequate numbers with proper electric-earthling.

III) Earthing and electric cabling as required at the site.

IV) 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.

4.5 Infrastructure at the Police Stations and Higher Offices

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

At each such location the following shall be carried out but not limited to:

I) Supply of the hardware, software, networking equipments, to the location as per the requirements.

II) Network Connectivity - Ensuring last mile connectivity Service Support and Testing.

III) Installation, Testing and Commissioning of UPS, DG-Set.

IV) Physical Installation of Desktops, Printer, Scanner, / MFD, Switch- Connecting peripherals, devices, Plugging in.

V) Operating System Installation and Configuration.

VI) Installation of Antivirus and other support software if any.

VII) Configuring the security at the desktops, switch, and broadband connection routers.

VIII) Network and browser Configuration.

IX) Test accessibility and functionality of CCTNS application from the desktops.

X) Ensuring all the systems required are supplied, installed, configured, tested and commissioned and declaring the site to be operational.

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

4.6 Network Connectivity for PS & Higher Offices

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

The Details on Network Connectivity is given in Annexure V.

4.7 IT Infrastructure at the data center and Disaster Recovery Center

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

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

SI shall ensure that support and maintenance, performance and up-time levels are compliant with SLAs. 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.

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

- The SI shall be responsible for the proposing of necessary hardware and determining the specifications of the same in order to meet the requirements of State.
- SI shall provide a Bill of Material that specifies all the hardware, software and any additional networking components of solution for the DC and DR, in detail so as to facilitate sizing of server room and DRC infrastructure such as Racks, Power and Cooling, Bandwidth among other components. The common DC and DR infrastructure shall be provided by State.
- SI shall ensure that effective Remote Management features exist in solution so that issues can be addressed by the SI in a timely and effective manner; and frequent visits to DC / DR can be avoided.
- After commissioning and testing of the entire system at DC / DR, the SI shall support the State in getting the system certified by a third party agency identified by State.
- State will provide the premises for Primary Data Centre (DC) and Disaster Recovery Centre (DRC) for hosting the solution. The solution shall be hosted in a collocation model in the Data Centers.

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

1) Power and Cooling
2) UPS, DG set power backup
3) Bandwidth and Connectivity
4) Fire prevention
5) Physical security surveillance
6) Network Operation Centre
7) Common Data Centre sub-systems facility Maintenance and Support

The SI is responsible for the below at the DC / DR:

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

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

4.8 Data Digitization & Data Migration

Data Migration:

Migration of 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 existing systems.

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

The Data migration strategy and methodology shall be prepared by SI and approved by MPCOPS. Though MPCOPS 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 MP Police / MPCOPS, during Data Quality Assessment and Review, in the data digitized/ migrated by SI, shall be addressed by SI at no additional cost to MPCOPS. So far as the legacy data is concerned, they are either available as structured data in the IT systems that are currently used by MP Police 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 MP Police / MPCOPS
2) Carry out the migration of legacy electronic data.
3) Carry out the migration of the data available in the existing registers, reports, case files etc.(Physical Copies)
4) Scan images and pictures within the case file in color and store them in the digital format.
5) Provide checklists from the migrated data to MP Police / MPCOPS for verification, including number of records, validations (where possible), other controls, / hash totals. Highlight errors, abnormalities, and deviations.
6) Incorporate corrections for the errors discovered during verification process, as proposed
7) Get final sign off from MPCOPS / Empowered Committee for migrated / digitized data.
8) At the end of migration, all the data for old cases and registers must be available in the new system.

Scope of Data Digitization / Migration

Estimated Digitization figure of IPC Crime:

S. No.	Head (Under IPC)	Number of Records
1.	Case File for Last nine Years	1762072
2.	Approximate Crime on 2010	Approx. 265000
3.	Assumed crime for first 6 months of 2011	Approx. 150678
Total Estimated Case Files		**Approx. 2177750**

Sources for data migration of data from legacy Application which is being used for registering crime is CIPA and Hardcopy registers involved in registering and crime and its proceedings

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

Recommended Methodology of Data Migration:

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

1) Analysis:

Analysis of the legacy data and its creation, conversion, migration and transfer to the proposed new database 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), and 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:

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

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

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

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

e) Migrate from staging servers to production servers.

f) 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 Madhya Pradesh Police.

2) SI shall formulate the “Data Migration Strategy document” which will also include internal quality assurance mechanism. This will be reviewed and signed–off by State prior to commencement of data migration.

3) SI shall incorporate all comments and suggestions of State in the Data Migration Strategy and process documents before obtaining sign–off from State.

4) SI shall perform mock data migration tests to validate the conversion programs.

5) SI shall ensure complete data cleaning and validation for all data migrated from the legacy systems to the new application.

6) SI shall validate the data before uploading the same to the production environment.

7) SI shall generate appropriate control reports before and after migration to ensue accuracy and completeness of the data.

8) SI shall convey to State in advance all the mandatory data fields required for functioning of the proposed solution and which are not available in the legacy systems and are required to be obtained by State.

9) In the event State is unable to obtain all the mandatory fields as conveyed by SI, SI shall suggest the most suitable workaround to State. SI shall document the suggested workaround and sign-off will be obtained from State for the suggested workaround.

10) SI shall develop data entry programs / applications that may be required for the purpose of data migration in order to capture data available with / obtained by State in non – electronic format.

11) SI shall conduct the acceptance testing and verify the completeness and accuracy of the data migrated from the legacy systems to the proposed solution.

12) State may, at its will, verify the test results provided by SI.

Data Digitization:

In addition to the data migration SI would also digitize the historical data (covering the last 10 years). The historical data to be digitized would include crime (case/incident) data, criminals' data, the data from the 7 IIF and relevant historical information parameters/data used to generate registers and reports. The unit of data digitization shall be one case file. Each case file shall consist of information pertaining to all 7 IIFs, information parameters relevant to generate specific registers from that case file and information parameters relevant to generate specific reports from that particular case file.

4.9 Migration of CIPA Police Stations to CAS (State) under CCTNS

The SI is also responsible for migrating the Police Stations currently operational on CIPA to CCTNS as part of the CCTNS implementation in the State. SI shall validate the data in the CIPA systems and migrate existing data available in CIPA to CAS (State).

Detailed list of Police Stations running CIPA along with the data to be migrated is enclosed as Annexure XII for the list of CIPA Police Stations

4.10 Capacity Building

Identification of Trainers (Internal):

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

Identification of Trainers (Police Training Institutes):

The MP Police / MPCOPS shall also identify the Trainers within each of the Police Training Institutes in the State who will be directly trained by the System Integrator. These trainers will be responsible for training on CCTNS within the training institutes, curriculum and impart the training on CCTNS to the new recruits and current personnel (refresher training).

Identification of Trainees:

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

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

- Refresher training, subsequent training to the remaining officers/constables in the Police Station and Higher Offices can be carried out by the internal trainers subsequent to the System Integrator trainings.

- **Group V:** Identify 2 constables for each Circle Office that can provide the basic computer operation support to the police stations within the Circle.

- Technical training will be carried out for the identified constables at District Training Centers in the respective Districts (if any) by the System Integrator

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

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

Develop Overall Training Plan:

SI shall be responsible for finalizing a detailed Training Plan for the program in consultation with MP Police / MPCOPS covering the training strategy, environment, training need analysis and role based training curriculum. SI shall own the overall Training plan working closely with the MP Police / MPCOPS Training team. SI shall coordinate overall training effort.

Develop District-Wise Training Schedule and Curriculum:

SI shall develop and manage the District-Wise training schedule in consultation with MP Police / MPCOPS, aligned with the overall implementation roadmap of the project and coordinate the same with all parties involved. Training schedule shall be developed by solution and shall be optimized to reduce business impact and effective utilization of Training infrastructure and capacities. The training curriculum for the CCTNS training program should be organized by modules and these should be used to develop the training materials. The training curriculum outlines the mode of delivery, module structure and outline, duration and target audience. These sessions should be conducted such that the users of the application/modules are trained by the time the application “goes-live” in the District with possibly no more than a week’s gap between completion of training and going live of modules. Continuous reporting (MIS) and assessment should be an integral function of training. SI shall also identify the languages to be used by the end-user for entering data and ensuring multi-language training to the end users as per requirement.

Develop Training Material:

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

1. **Basic IT skills** and use of computers to creating awareness about the benefits of ICT and basic computer skills.

2. **Role-based training on the CCTNS application** – Basic and Advanced. This training should be in a role based, benchmarked and standardized format, multi-lingual and lead to learning completion and assessment. It should also allow for self-learning and retraining. Training would include mechanism for demonstration using audio/video/simulated/demo practice exercises and evaluation of trainees.

3. **"Train the Trainer"** programs, where members of the police staff would be trained to enable them to conduct further training programs, thus helping build up scalability in the training program and also reducing the dependency on external vendors for training.

4. **System Administrator training**: a few members of the police staff with high aptitude would be trained to act as system administrators and troubleshooters for CCTNS.

5. Customization of the Training Manuals, User Manuals, Operational and Maintenance Manuals provided along with the CCTNS CAS Software.

6. Design and development of the Training Manuals, User Manuals, Operational, and Maintenance Manuals for the modules developed at the State level.

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

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

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

   Deliver Training to End Users:

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

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

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

An ILT course will have the following components:

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

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

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

Deliver Training to Trainers (Internal and Trainers from the Training Colleges) SI shall help MP Police / MPCOPS in assessing and selecting the internal trainers as well as the trainers at training colleges who can conduct the end user training subsequent to the training by the SI. SI shall coordinate the 'Train the Trainer' session for the identified trainers to ensure that they have the capability to deliver efficient training.

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

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

2. The second segment will be the formal CCTNS training which will consist of all modules of CCTNS relevant for their role.

3. The third segment will be a teach-back session where trained trainers will present course content and receive feedback regarding content, flow, and presentation techniques. This will also include a feedback session where trainers can provide feedback on the training materials, flow, comprehension level, and accuracy.

Training Effectiveness Evaluation:

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

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

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

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

Change management:

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

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

Communication and Awareness:

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

S NO.	Activities	Detail	Frequency
1	Develop detailed communication plan	• SI shall prepare a detailed communication plan for the program in line with the implementation timelines of each solution • SI shall ensure that all the impacted audience is covered in the communication plan and the most appropriate mode of communication is being used to deliver the messages to the target audience	Once
2	Develop Communication Content	• SI shall be responsible for developing the content for communication material in English & Hindi language. • SI shall ensure that the communication is simple, continuous and consistent.	Recurring Activity over the entire duration of the SI
3	Deliver Communication Events	• Prior to implementing the plan, the SI shall obtain the necessary sign-offs from State on the Communication Strategy & plan and make necessary changes as recommended by State. • SI shall determine who needs to approve communications prior to dissemination, who is responsible for distributing the message, and who is responsible for ensuring that those accountable for specific elements of the plan follow through on their responsibilities. • SI shall organize the communication events or interventions for the target audience. • SI shall ensure consistency between messages delivered via different interventions, since the engagement of a key individual stakeholder or stakeholder group is an integrated effort, aiming at the same objective.	Recurring Activity (once a month) over the entire duration of the SI

Change Management Workshops:

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

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

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

The Change management activity shall be monitored periodically by MPCOPS / SPMU. SI is responsible to design suitable monitoring and MIS mechanism for this purpose.

4.11 Handholding Support

The System Integrator will provide one qualified and trained person per police station for a period of six months to handhold the staff in the police station and ensure that the staffs in those police stations are able to use CCTNS on their own by the end of the handholding period. Apart from police stations additional support required to provide services during the project life cycle **i.e.** . SI must provide the project team as per details and eligibility qualifications given in this RFP.

Handholding and project support would be required only after the successful commissioning of Core Application (CAS) and the necessary infrastructure and completion of capacity building and change management initiatives in respective locations.

Information of all Police locations regarding engagement of handholding personnel has been provided in Geographical scope in this RFP.

Handholding staff for police stations will be required for 6 Months and Other Project Team is required for the entire project period including Operation & Maintenance phase.

Code of Conduct of Handholding personnel as Police Stations:

- The person to be engaged by SI for Handholding support should work as six days per week.
- Handholding personnel should give 100% availability on all working days.

Qualification Eligibility for Project Team:

Handholding staff for police station:

Handholding Staff	
Desired Qualification / Experience	• M.Sc. (IT/CS)/ PGDCA / BCA • Overall experience of 1-2 year of Application Software/LAN/WAN/PC troubleshooting, Data Entry on Computer Applications, Working proficiency on office suite. • Full computer literacy and excellent fluency in Hindi language
Location	Police Stations
Minimum manpower	996
Service Window	9 x 6

Other Project Team

1. **Project Manager:**

Project Manager	
Desired Qualification / Experience	• Post-Graduate Level of education in related fields of social sciences, environmental engineering, economics and/or planning (education and/or experience on sustainable development/ platform is an asset) • Minimum 5 years of proven professional experience as Project Manager/Project Leader in the management of state level government/ corporate projects in similar fields • Experience in project administration, coordinating, planning, execution, monitoring and reporting

	• Good understanding of Project Life Cycle & Management Full computer literacy and excellent fluency in English language
Location	HQ- Bhopal
Minimum manpower	1
Service Window	9 x 6

2. Helpdesk coordinator:

Help Desk Coordinator	
Desired Qualification / Experience	• BE (CS) / MCA / M.Sc. (IT/CS) • Overall experience of 2-3 year of Helpdesk Management • Full computer literacy and excellent fluency in English language
Location	HQ- Bhopal
Minimum manpower	2
Service Window	12 x 6

3. System and Network Administrator:

System and network administrator	
Desired Qualification / Experience	• B. Tech or BE (CS) / MCA / M.Sc. (IT/CS) • OEM Certified • Overall experience of 2-3 year of systems and network administration in large projects • Expert in Network Administration - LAN, MAN & WAN. • Full computer literacy and excellent fluency in Hindi & English language
Location	DC- Bhopal
Minimum manpower	3
Service Window	24 x 7

4. Security Specialist:

Security Specialist	
Desired Qualification / Experience	• B. Tech or BE (CS) / MCA / M.Sc. (IT/CS) and ISMS ISO 27001 or equivalent Certification • Overall experience of 2-3 year of implementing security policy, reviewing, auditing. • Expert in Network Administration - LAN, MAN & WAN / Firewall / VPN / IPS etc. • Must have successfully completed ISMS ISO 27001 training course. • Full computer literacy and excellent fluency in Hindi & English language
Location	DC- Bhopal
Minimum manpower	1
Service Window	9 x 6

5. Database Administrator:

Database Administrator (DBA)	
Desired Qualification / Experience	• Preferably a B.Tech/ BE/ MCA/ M.Sc. in the field of Computer Science/ Information Technology • Must be certified as an SQL Server 2005/08 / My SQL • Minimum 2-3 years of proven professional experience as DBA with any state level government/ corporate projects • Good understanding of Project Life Cycle & Management • Full computer literacy and excellent fluency in Hindi & English language
Location	DC- Bhopal
Minimum manpower	1
Service Window	9 x 6

6. **Technical field staff type – 1:**

Technical field staff type-1	
Desired Qualification / Experience	• BE (CS) / MCA / M.Sc. (IT/CS) • Overall experience of 2-3 year of LAN/ WAN/ Servers / Storage/ DC & DR Software / Hardware support • Full computer literacy and excellent fluency in Hindi & English language
Location	DC- Bhopal
Minimum manpower	3
Service Window	24 x 7

7. **Technical Field Staff type – 2:**

Technical field staff type – 2	
Desired Qualification / Experience	• BE (CS) / MCA / M.Sc. (IT/CS)/ PGDCA • Overall experience of 1-2 year of LAN / WAN/ PC / Hardware / Software Troubleshooting and support • Full computer literacy and excellent fluency in Hindi & English language
Location	For Other Offices
Minimum manpower	10
Service Window	12 x 7

4.12 Requirement of Adherence to Standard

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

Compliance with Industry Standards:

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

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

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

4.13 Support to acceptance testing, Audit and Certification

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

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

As part of Acceptance testing, audit and certification, performed through a third party agency, State shall review all aspects of project development and implementation covering software, hardware and networking including the processes relating to the design of solution architecture, design of systems and sub-systems, coding, testing, business process description, documentation, version control, change management, security, service oriented architecture, performance in relation to defined requirements, interoperability, scalability, availability and compliance with all the technical and functional requirements of the RFP and the agreement. Here it is important to mention that there may be two agencies selected by State, one for audit & certification of security and control aspect of the system and the other for audit & certification of overall application software.

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, workflow 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.

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.

Note: SI shall provide requisite support and coordinate with the MP Police / MPCOPS for Audit, User acceptance and Certification.

4.14 Scope of Services during Post-Implementation Phase

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

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

5. Implementation and Roll-Out Plan

Detailed Project Plan			
Phase	**Suggested Activities**	**Responsibilities**	**Time lines (month)**
Phase – I (T= Signing Date of Agreement)	**Setting up of Data Center**		
	Providing the Premises for Server Room & Disaster Recovery	MPCOPS	**T+1**
	Preparation of Bill of Quantity (Hardware, Software, Connectivity)	SI	
	Preparation of layout	SI	
	Sizing document for Common Server Room Infrastructure (Server Racks, Power arrangement, Cooling etc.)	SI	
	Approval from Respective authorities	SI, SPMU & MPCOPS	
	Preparation of Site	MPCOPS / SI	**T+3**
	Wiring (Electrical, WAN Connectivity etc.)	MPCOPS	
	Cooling Arrangements	MPCOPS	
	Procurement of Hardware, Software, Licenses	SI	
	24*7 Power backup Support Provision	MPCOPS	
	Installation and Testing of UPS, DG-Set	MPCOPS	**T+4**
	Supply of the Hardware, Software, License & Networking equipments	SI	
	Installation and Testing of Equipments	SI	
	Redundant Network Connectivity	SI / MPCOPS	
	24*7 Support system in case of break down	SI	
	Testing and Up-gradation	SI	**T+5**
	Inspection and Suggestions	SPMU / MPCOPS	
	Approval From Department	MPCOPS	**T+6**
	Operation Support	SI	
	Customization of CAS (State)		
	SRS preparation	SI	**T+1**
	Approval from SPMU & Department and Change Incorporation in case of suggestions	SI, SPMU & Department	**T+2**
	Customization, Configuration and Development of Application	SI	**T+4**
	User Acceptance Testing	SI	**T+5**
	Change Request	SI	
	Final Implementation at all Police Stations	SI	**T+6**
	CAS Integration with Identified applications		

	SRS preparation	SI	**T+2**
	Approval from SPMU & Department	SI, SPMU & MPCOPS	**T+3**
	Customization, Configuration and Integration	SI	**T+8**
	User Acceptance Testing	SI	**T+10**
	Change Request	SI	
	Roll out at all Police Stations	SI	
	CCTNS Site Preparation (Police Stations)		
	Site handover / Approval for CCTNS	MPCOPS	**T+1**
	Electrical & Local Area Networking Work	SI	**T+3**
	Procurement of Hardware, Software, Licenses	SI	
	Supply of the Furniture & Fixtures	SI	**T+4**
	Supply and Installation of Desktops/PCs, Printers, Scanners, UPS	SI	**T+5**
	WAN Testing and VPN configuration	SI	**T+5**
	Arrangements of Power Backup (DG Set/UPS)	SI	
	Testing of Connectivity with Data Center (WAN)	SI	
	Testing of CCTNS system at Police Station from User perspective	SI	
	Inspection and Suggestions	SPMU / MPCOPS	**T+6**
	CAS Operational at all Police Stations	SI	**T+6**
	Approval from Department	MPCOPS	
	Data Migration		
	Analysis of Data to be Migrated	SI	**T+3**
	Collection & Consolidation of Data	SI	
	Data Migration	SI	**T+6**
	Data Security	SI	
	Certification from Department about authenticity of Migrated data	SI	
	Data Digitization		
	Analysis of Data to be Digitized	SI	**T+3**
	Collection & Consolidation of Data	SI	**T+5**
	Data Digitization	SI	**T+15**
	Data Validation & Re entry	SI	**T+17**
	Certification from Department about authenticity of Digitized data	SI	**T+18**
	Capacity Building		
	Creating awareness and Sensitization (Through seminars, meetings, workshops)	SI / MPCOPS	**T+2**
	Training of Master Trainers for CCTNS	SI	**T+3**

	Application		
	Up-gradation & Revision of Basic Computer Training	SI	T+6
	Training of Core Application Software (CAS)	SI	
	System administration and Maintenance Training	SI	
	Handholding & Helpdesk Establishment		
	Starting of Handholding Support to PS for six months & Establishment of Helpdesk for PS & DC entire project period, Providing Technical Staff for DC	SI	T+6
Phase – II (D = T+6)	**CCTNS Site Preparation (PHQ, SSR, PCR, FBP, FSL, Zone, Range, Districts)**		
	Site Handover / Approval for CCTNS	MPCOPS	D+1
	Electrical & Local Area Networking Work	SI	D+3
	Procurement of Hardware, Software, Licenses	SI	
	Supply of the Furniture & Fixtures	SI	D+4
	Supply and Installation of Desktops/PCs, Printers, Scanners, UPS	SI	D+5
	WAN Testing and VPN configuration	SI	D+6
	Arrangements of Power Backup (DG Set/UPS)	SI	
	Connectivity with DC	SI	
	Testing of CCTNS system from User perspective	SI	
	Inspection and Suggestions	SPMU / MPCOPS	
	Approval from Department	MPCOPS	
	Capacity Building (Phase II)		
	Creating awareness and Sensitization (Through seminars, meetings, workshops)	SI / MPCOPS	D+2
	Training of Master Trainers for CCTNS Application	SI	D+6
	Up-gradation & Revision of Basic Computer Training	SI	
	Training of Core Application Software	SI	
	System administration and Maintenance Training	SI	
	Helpdesk & Technical Support		
	Starting Helpdesk and Technical Support for phase II locations for entire project period	SI	D+6
Phase – III (C = D+6)	**CCTNS Site Preparation (all other locations and DR site)**		
	Site Handover / Approval for CCTNS	MPCOPS	C+1
	Electrical & Local Area Networking Work	SI	C+3
	Procurement of Hardware, Software, Licenses	SI	

	Supply of the Furniture & Fixtures	SI	**C+4**
	Supply and Installation of Servers, Desktops/PCs, Printers, Scanners, UPS	SI	**C+5**
	WAN Testing and VPN configuration	SI	**C+6**
	Arrangements of Power Backup (DG Set/UPS)	SI	
	Connectivity with DC	SI	
	Testing of CCTNS system from User perspective	SI	
	Inspection and Suggestions	SPMU / MPCOPS	
	Approval from Department	MPCOPS	
	Capacity Building (Phase III)		
	Creating awareness and Sensitization (Through seminars, meetings, workshops)	SI / MPCOPS	**C+2**
	Training of Master Trainers for CCTNS Application	SI	**C+6**
	Up-gradation & Revision of Basic Computer Training	SI	
	Training of Core Application Software	SI	
	System administration and Maintenance Training	SI	
	Helpdesk & Technical Support		
	Starting Helpdesk and Technical Support for phase II locations for entire project period	SI	**C+6**
	Go-Live of CCTNS Project in entire State	SI	**C+6**
Operation and Maintenance Support	**Support after Implementation Phases after Go-Live**		
	Operations and Maintenance support	SI	**Go live + 36**
	Warranty and AMC services	SI	
	Continuations of Helpdesk for Providing Support to all Locations	SI	
	Regular supervision, monitoring and extending support to department for smooth functioning of project.	SI/SPMU	

Note: The Operation and Maintenance Support Period may be extended for further 12 or 24 Months.

It is suggested that the solution be piloted in a few police stations in one or two districts (if any) and the feedback incorporated before rolling out across the State. The rollout plan shall be defined date-wise, location-wise, module-wise, and training completion and change management completion wise. A detailed rollout checklist should be maintained for migrating application to production as well as for location readiness.

SI shall prepare a detailed roll-out plan for each of the location in Phase and get the same approved by the State. SI is also responsible for conducting workshops for the key officers (State

Mission Team, District Mission Team, and District Core Team) of the Districts / State for presenting the District-Wise roll-out plan and get the approval from the District Teams before getting the final approval of the MPCOPS / MP Police. The SI shall also provide the necessary assistance for the key officers (State Mission Team, District Mission Team, and District Core Team) of the Districts / State during the design and implementation of CCTNS in the State.

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

List of Indicative Deliverables:

1. Overall Project Plan.
2. CAS Configuration / Customization / Integration:
   a) Requirements Traceability Matrix
   b) Refined Functional Requirements Specification
   c) Systems Requirement Specification
   d) Design Document (High Level Design and Low Level Design)
   e) Test Plans
   f) CAS Configuration / Customization / Integration Document
   g) Change / Reference Document documenting changes to the base version of CAS (State)
3. Network Connectivity Testing:
   a) Network Architecture
   b) Network diagrams (LAN and WAN) for PS / HO to State DC / DRC
   c) Network diagrams for connectivity between State DC / DRC to NCRB DC / DRC
4. Data Migration Strategy and Methodology including Detailed Data Migration Plan:
5. Change Management and Capacity Building:
   a) Overall Change Management Plan
   b) Content for Change Management including Awareness and Communications Program
   c) Overall Capacity Building Plan and District-wise Training Schedule and Curriculum
   d) Training Material
6. District-wise Roll-out / Implementation Plans.

Service Levels:

This section describes the service levels to be established for the Services offered by the SI to State. The SI shall monitor and maintain the stated service levels to provide quality service to State. The Service levels are provided in "**Annexure-IX Service Levels**".

ANNEXURE I: Governance Structure (State Level)

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

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

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

State Apex Committee

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

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

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

Members	Composition Suggested
Member 1 (Chairperson)	Chief Secretary
Member 2 (Co-Chair)	Principal Home Secretary
Member 3	Secretary Finance
Member 4	IT Secretary
Member 5	Head of SCRB
Member 6	Representative of NIC
Member 7	Representative of GOI, MHA

Member 8 (Convener)	Nodal Officer (CCTNS Project)
Member 9	Any other member co-opted from the field of IT, Telecom, etc.

Frequency of Meeting: Once in a quarter

State Empowered Committee

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

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

The Composition of State Empowered Committee is as following:

Members	Composition Suggested
Member 1 (Chairperson)	**DGP**
Member 2 (Co-Chair)	**Head of SCRB**
Member 3	**Representative of NCRB**
Member 4	**Representative of Home Department at State level**
Member 5	**Representative of Finance at State level**
Member 6	**Director e-governance or representative of IT Department**
Member 7	**NIC representative at State Level**
Member 8 (Convener)	**Representative of State Implementation**

	agency
Member 9	**ADGP/IG level office as nominated by DGP**
The Committee may co-opt any other member whenever, felt necessary.	

Frequency of Meeting: Once a month

State Mission Team:

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

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

The composition of State Mission Team is as following:

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

Frequency of meeting: Once a month

District Mission Team

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

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

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

Members	Composition Suggested
Member 1 (Chairperson)	SSP/SP of the District
Member 2 (Co-Chair)	One officer of DCRB
Member 3	DIO of the NIC District Centre
Member 4	One officer from District Police having computer knowledge

Frequency of meeting: Once a month

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

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

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

CAS (State) Solution - Stack 1:

	Proposed Solution by Software Development Agency	Version and Year of Release	Original Supplier	Description (include major features/ services only)	Support Provided By
Web server	Sun Java System Web Server 7.0	7.0	SUN	HTTP Server	SUN
Application Server	Glassfish Application Server	3.0	SUN	J2EE Application Server	SUN
Database	MySQL	5.1	SUN	DB Store	SUN
Operating System	Solaris	10	SUN	Operating System	SUN
Others					
Reporting Engine	Jasper Reports	3.7	Jasper	Reporting Services	
Email/ Messaging	Q-Mail	1.4	Q mail Community	E-Mail Solution	
Search Engine	Search: Unstructured data: using open CMS search features Structured Data MySQL & Custom application interface	N/a	N/a	N/a	N/a
Portal Server	Glassfish Application Server	3.0	SUN	J2EE Application Server	SUN
Workflow Engine	jBPM	4.0	JBoss	Workflow engine	
Rules Engine	Custom Built	N/a	N/a	N/a	N/a
Directory Services	Sun Directory Services	7.0	SUN	LDAP	SUN
DMS/CMS	Open CMS	7.5.1	OpenCMS	Content Management System	
Security	Physical Security,	N/a	N/a	N/a	N/a

	Network Security, DB Encryption (MySQL), DB Access Controls, Role Based Access Control (Custom Developed), LDAP (Sun Directory Services),				
Identity Management	Open SSO	7.0	SUN	LDAP	SUN
Audit	log4j, Custom Built application audit	N/a	N/a	N/a	N/a
ETL	Custom Built	N/a	N/a	N/a N/a	N/a

CAS (State) Solution - Stack 2:

	Proposed Solution by Software Development Agency	Version and Year of Release	Original Supplier	Description (include major features/ services only)	Support Provided By
Web server	IIS	6	Microsoft	Web & App Server	Microsoft
Application Server	IIS	6	Microsoft	Web & App Server	Microsoft
Database	SQL Server 2008	2008	Microsoft	DB Store	Microsoft
Operating System	Windows Server 2008	2008	Microsoft	Operating System	Microsoft
Others					Microsoft
Reporting Engine	SQL Server Reporting Services	2008	Microsoft	Reporting Services	Microsoft
Email/Messaging	Q-Mail	1.4	Q mail Community	E-Mail Solution	
Search Engine	Search: Unstructured data: using open CMS search features	N/a	N/a	N/a	N/a

	Structured Data: SQL DB Search Engine & Custom application interface				
Portal Server	IIS	6	Microsoft	Web & App Server	Micro soft
Workflow Engine	Windows Workflow Foundation	N/a	N/a	N/a	N/a
Rules Engine	Custom Built	N/a	N/a	N/a	N/a
Directory Services	Microsoft Active Directory	2008	Microsoft	LDAP	Micro soft
DMS/CMS	Windows SharePoint Services	n/a	n/a	n/a	n/a
Security	Physical Security, Network Security, DB Encryption (MSSQL), DB Access Controls, Role Based Access Control (Custom Developed), Active Directory	N/a	N/a	N/a	N/a
Identity Management	Microsoft Active Directory	2008	Microsoft	LDAP	Micro soft
Audit	IIS Log, Custom Built	N/a	N/a	N/a	N/a
ETL	SQL Server ETL	2008	Microsoft	ETL	Micro soft

CAS (State) Offline Solution:

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

CAS (Center) Solution:

The below list is indicative only	Proposed Solution by Software Development Agency	Version and Year of Release	Original Supplier	Description (include major features/ services only)	Support Provided By
Web server	Sun Java System Web Server 7.0	7.0	SUN	HTTP Server	SUN
Application Server	Glassfish Application Server	3.0	SUN	J2EE Application Server	SUN
Database	Sybase IQ Enterprise	15.1	Sybase	ETL	Sybase
Operating System	Solaris				
Others					
Reporting Engine	Jasper Reports	3.7	Jasper	Reporting Services	
Search Engine	Search: Unstructured data: using Alfresco search features Structured Data: Sybase DB Search Engine &	N/a	N/a	N/a	N/a

	Custom application interface				
Portal Server	Glassfish Application Server	Glassfish Application Server	SUN	HTTP Server	SUN
Workflow Engine	jBPM	4.0	JBoss	Workflow engine	
Rules Engine	Custom Built	N/a	N/a	N/a	N/a
Directory Services	Sun Directory Services	7.0	SUN	LDAP	SUN
DMS/CMS	Alfresco				
Email/ Messaging	N/A				
Security	Physical Security, Network Security, DB Encryption (MySQL), DB Access Controls, Role Based Access Control (Custom Developed), LDAP (Sun Directory Services),	N/a	N/a	N/a	N/a
Identity Management	Open SSO	7.0	SUN	LDAP	SUN
Audit	log4j, Custom Built	N/a	N/a	N/a	N/a
ETL + Data Quality	Sybase ETL	15.1	Sybase	ETL	Sybase

ANNEXURE III: Bill of Quantity

Scope of Hardware SITC

System integrator is responsible for supply, install, commission, testing and maintenance of Hardware and other peripheral to all police stations and higher offices. This includes Non-CIPA police stations-575, CIPA Police Stations- 373, Traffic police stations – 48, Sub-Divisional Police Offices/ DSP/ Addl. SP-288, District Police Control Room (PCR)-50, SP/SRP offices -53, Ranges-12, Zones-16, SCRB-1, State Police Control Room (SSR)-1, State Finger Print Bureau-1, State Forensic Science Lab-1, PHQ-1 locations. Location wise distribution of hardware and peripherals is given below:

Police Station Hardware Distribution (Non-CIPA – 623 Locations):

SI has to supply, install, commission, testing of below hardware and peripherals at each location:

Police Station Hardware and Site Preparation (Each PS)			
Item Description	**Qty.**	**Make**	**Model**
Desktop System	4		
HDD 160 GB	1		
Duplex Laser Printer (Network)	1		
Multi-Function Laser (Print/ Scan/ Copy)	1		
UPS for 120 min backup (2 KVA)	1		
Generator Set (2 KVA)	1		
Network Switch 16 Ports 10/100 Layer 2 Managed	1		
Finger Print reader	1		
Digital Camera	1		
Electronic Pen	1		
Site Preparation:-			
Adequate Furniture	1		
Electrical Cabling	1		
Earthing & Earth Pit	1		
Wall Mountable Network Rack - 9 U	1		
Patch Panel 12 Ports CAT 6	1		
Information Outlet CAT 6	6		
Cat 6 Cable with Cabling (In Meters)	120		
Patch Cords 1 Mtr. CAT 6	6		
Patch Cords 2 Mtr. CAT 6 **Operational Expenses Each PS (In Years)**	6 3		
Software:-			
MS Windows-7 Professional	4		
MS Office 2010 Std. Indic	1		
Client Antivirus (3 Years)	4		
Application Patch Management & Asset Management Software (EMS CAL)	4		

CIPA Police Stations (Phase I - 93 Locations):

CIPA has been commissioned in three phases at State to 373 police stations. Under phase-I of 93 police stations have been covered. Hardware provided to these 93 police stations are completed their life span and needs to be replaced. System Integrator is responsible for supply, install, testing, commissioning and maintenance of hardware in these 93 locations.

This is responsibility of System Integrator; to collect and redistribute the hardware distributed under this phase of CIPA as directed by MPCOPS.

Details are given below for hardware and peripherals at each location:

Hardware and Site Preparation Gap for Police Stations Covered Under CIPA (Phase-I)			
Item Description	**Qty.**	**Make**	**Model**
Desktop System	4		
HDD 160 GB	1		
Duplex Laser Printer (Network)	1		
Multi-Function Laser (Print/ Scan/ Copy)	1		
UPS for 120 min backup (2 KVA)	1		
Generator Set (2 KVA)	1		
Network Switch 16 Ports 10/100 Layer 2 Managed	1		
Finger Print reader	1		
Digital Camera	1		
Electronic Pen	1		
Site Preparation:-			
Wall Mountable Network Rack - 9 U	1		
Patch Panel 12 Ports CAT 6	1		
Patch Cords 1 Mtr. CAT 6	6		
Operational Expenses Each PS (In Years)	3		
Software:-			
MS Windows-7 Professional	4		
MS Office 2010 Std. Indic	1		
Client Antivirus (3 Years)	4		
Application Patch Management & Asset Management Software (EMS CAL)	4		

CIPA Police Stations (Phase II - 108 & Phase III - 172 Locations, Total 280 Locations):

Under CIPA phase-II of 108 police stations has been covered. Warranty period of hardware distributed under this phase has been expired. System Integrator has to provide warranty for 3 years to the distributed hardware and peripherals of these locations. For details of these locations **please refer Annexure- XIV CIPA Police Stations**

System Integrator is responsible for supply, install, testing, commissioning, and maintenance of GAP hardware and peripherals to each location. Details are given below:

Hardware and Site Preparation Gap for Police Stations Covered Under CIPA (Phase-II & III)			
Item Description	**Qty.**	**Make**	**Model**
Generator Set (2 KVA)	1		
Finger Print reader	1		
Digital Camera	1		
Electronic Pen	1		
Additional HDD 160 GB	1		
Network Switch 16 Ports 10/100 Layer 2 Managed	1		
Site Preparation:-			
Wall Mountable Network Rack - 9 U	1		
Patch Panel 12 Ports CAT 6	1		
Patch Cords 1 Mtr. CAT 6	6		
Operational Expenses Each CIPA PS (In Years)	3		
Software			
MS Windows-7 Professional	4		
MS Office 2010 Std. Indic	1		
Client Antivirus (3 Years)	4		
Application Patch Management & Asset Management Software (EMS CAL)	4		
1 Year AMC of Hardware for each police station (CIPA - Phase II only)	1		

State Finger Print Bureau and State Forensic Science Lab:

Madhya Pradesh Police has one-one State Finger Print Bureau/ Forensic Science Lab office. System Integrator is responsible for supply, install, testing, commissioning and maintenance of below hardware and peripherals at each location:

Hardware and Software – Forensic Science Lab & Finger Print Bureau (Each Location)			
Item Description	**Qty.**	**Make**	**Model**
Desktop System	2		
Multi-Function Laser (Print/ Scan/ Copy)	1		
Network Switch 16 Ports 10/100 Layer 2 Managed	1		
Site Preparation:-			
Adequate Furniture	1		
Patch Cords 2 Mtr. CAT 6	3		
Operational Expenses Each Office (In Years)	3		
Software:-			
MS Windows-7 Professional	2		
MS Office 2010 Std. Indic	2		
Client Antivirus (3 Years)	2		
Application Patch Management & Asset Management Software (EMS CAL)	2		

District Police Control Room:

District Police Control Rooms are 50 in numbers. System Integrator is responsible for supply, install, testing, commissioning and maintenance of below hardware and peripherals at each location:

Hardware, Software & Site Preparation at Police Control Rooms (50 Locations)			
Item Description	**Qty.**	**Make**	**Model**
Desktop System	3		
Multi-Function Laser (Print/ Scan/ Copy)	1		
Network Switch 16 Ports 10/100 Layer 2 Managed	1		
Site Preparation:-			
Adequate Furniture	1		
Patch Cords 2 Mtr. CAT 6	4		
Operational Expenses Each Location (In Years)	3		
Software:-			
MS Windows-7 Professional	3		
MS Office 2010 Std. Indic	3		
Client Antivirus (3 Years)	3		
Application Patch Management & Asset Management Software (EMS CAL)	3		

State Police Control Room (SSR):

Madhya Pradesh Police has one State Police Control Room office. System Integrator is responsible for supply, install, testing, commissioning and maintenance of below hardware and peripherals at each location:

Hardware, Software & Site Preparation at State Control Rooms (SSR-1)			
Item Description	**Qty.**	**Make**	**Model**
Desktop System	5		
Multi Function Laser (Print/ Scan/ Copy)	1		
Network Switch 16 Ports 10/100 Layer 2 Managed	1		
Site Preparation:-			
Adequate Furniture	1		
Patch Cords 2 Mtr. CAT 6	6		
Operational Expenses Each Location (In Years)	3		
Software:-			
MS Windows-7 Professional	5		
MS Office 2010 Std. Indic	5		
Client Antivirus (3 Years)	5		
Application Patch Management & Asset Management Software (EMS CAL)	5		

Sub-Divisional Police Offices/ DSP/ Addl. SP:

Sub-Divisional police offices/ DSP/ Addl. SP are 288 in numbers. System Integrator is responsible for supply, install, testing, commissioning and maintenance of below hardware and peripherals at each location:

Hardware and Site Preparation - Sub Division (Addl. SP / DSP / SDOP / CSP) Total - 288 Locations			
Item Description	**Qty.**	**Make**	**Model**
Desktop System	3		
Multi Function Laser (Print/ Scan/ Copy)	1		
UPS for 120 min backup (2 KVA)	1		
Network Switch 16 Ports 10/100 Layer 2 Managed	1		
Site Preparation:-			
Adequate Furniture	1		
Electrical Cabling	1		
Earthing & Earth Pit	1		
Wall Mountable Network Rack - 9 U	1		
Patch Panel 12 Ports CAT 6	1		
Information Outlet CAT 6	6		
Cat 6 Cable with Cabling (In Meters)	120		
Patch Cords 1 Mtr. CAT 6	6		
Patch Cords 2 Mtr. CAT 6	6		
Operational Expenses Each Location (In Years)	3		
Software:-			
MS Windows-7 Professional	3		
MS Office 2010 Std. Indic	3		
Client Antivirus (3 Years)	3		
Application Patch Management & Asset Management Software (EMS CAL)	3		

SP/SRP offices:

District offices are 53 in numbers. System Integrator is responsible for supply, install, testing, commissioning and maintenance of below hardware and peripherals at each location:

Hardware and Site Preparation - Districts (SP Offices / SRP) Total - 53 Locations			
Item Description	**Qty.**	**Make**	**Model**
Desktop System	10		
Multi Function Laser (Print/ Scan/ Copy)	10		
UPS for 120 min backup (1 KVA)	10		
Network Switch 16 Ports 10/100 Layer 2 Managed	1		
Site Preparation:-			
Adequate Furniture	1		
Electrical Cabling	1		
Earthing & Earth Pit	1		
Wall Mountable Network Rack - 9 U	1		
Patch Panel 12 Ports CAT 6	1		
Information Outlet CAT 6	11		
Cat 6 Cable with Cabling (In Meters)	220		
Patch Cords 1 Mtr. CAT 6	11		
Patch Cords 2 Mtr. CAT 6	11		
Operational Expenses Each Location (In Years)	3		
Software:-			
MS Windows-7 Professional	10		
MS Office 2010 Std. Indic	10		
Client Antivirus (3 Years)	10		
Application Patch Management & Asset Management Software (EMS CAL)	10		

Range/ Zones/ SCRB:

Range/ Zones/ SCRB offices are 29 in numbers. System Integrator is responsible for supply, install, testing, commissioning and maintenance of below hardware and peripherals at each location:

Hardware and Site Preparation - Range / Zone / SCRB Total - 29 Locations			
Item Description	**Qty.**	**Make**	**Model**
Desktop System	4		
Multi Function Laser (Print/ Scan/ Copy)	1		
UPS for 120 min backup (2 KVA)	1		
Network Switch 16 Ports 10/100 Layer 2 Managed	1		
Site Preparation:-			
Adequate Furniture	1		
Electrical Cabling	1		
Earthing & Earth Pit	1		
Wall Mountable Network Rack - 9 U	1		
Patch Panel 12 Ports CAT 6	1		
Information Outlet CAT 6	6		
Cat 6 Cable with Cabling (In Meters)	120		
Patch Cords 1 Mtr. CAT 6	6		
Patch Cords 2 Mtr. CAT 6	6		
Operational Expenses Each Location (In Years)	3		
Software:-			
MS Windows-7 Professional	4		
MS Office 2010 Std. Indic	4		
Client Antivirus (3 Years)	4		
Application Patch Management & Asset Management Software (EMS CAL)	4		

Police Head Quarter (PHQ):

System Integrator is responsible for supply, install, testing, commissioning and maintenance of below hardware and peripherals to Police Head Quarter:

Hardware and Site Preparation - Police Head Quarter (Large)			
Item Description	**Qty.**	**Make**	**Model**
Desktop System	50		
Multi Function Laser (Print/ Scan/ Copy)	50		
UPS for 120 min backup (1 KVA)	50		
16 Port Network Switch Layer 2 Managed	4		
Site Preparation:-			
Adequate Furniture	1		
Wall Mountable Network Rack - 9 U	4		
Patch Panel 18 Ports CAT 6	4		
Information Outlet CAT 6	50		
Cat 6 Cable with Cabling (In Meters)	1150		
Patch Cords 1 Mtr. CAT 6	50		
Patch Cords 2 Mtr. CAT 6	50		
Operational Expenses Each Location (In Years)	3		
Software:-			
MS Windows-7 Professional	50		
MS Office 2010 Std. Indic	50		
Client Antivirus (3 Years)	50		
Application Patch Management & Asset Management Software (EMS CAL)	50		

Note:

Desktops: One number of Intel i5 / AMD Phenom 555 and three numbers of Intel Core 2 Duo / AMD Phenom 550 Processor based desktop computers are to be supplied at all the Police Stations where new desktops are provisioned under this project. At all the other locations only Intel Core 2 Duo / AMD Phenom 550 processor based desktop computers are to be supplied.

Adequate Furniture: 4 Computer table, 4 Chairs and 1 Printer table to supplied at each Police Station, where Furniture is provisioned under this project. At all other locations one computer table and one chair to be supplied against each Desktop computer provisioned.

Operation expense: This includes free of cost replacement of toner cartridge for Laser and Multi-function printer. The frequency of cartridge replacement shall be quarterly, i.e. every 3 months one cartridge to be replaced in each printer. Free of cost replacement of Teflon paper of each laser & multifunction printer on yearly basis is also a part of Operational expense. However cost of stationery item is not included in this head. Consumption of cartridges may vary based on usage of individual police locations, although SI shall strictly supply total number of cartridges as per quantity mentioned above. Spare cartridges of any location may be used at other location on need basis. All

the supplied cartridges must be of the same original printer manufactures only and must follow standards of printer manufacturer. Refilling of cartridges is not permitted.

Data Center and DR Site Hardware & Software:

System Integrator is responsible for supply, install, testing, commissioning and maintenance of below hardware and software at Data Center and DR Site:

Data Center & Disaster Site Hardware & Software			
Item Description	**Qty.**	**Make**	**Model**
Data Center Storage with SAN Switch	1		
Disaster Recovery Storage with SAN Switch	1		
Data Center Server Cost			
Database & Reporting Server (Rack)	2		
Application Server	2		
Intranet Web Server	2		
Internet Web Server	2		
Directory & Access Server	2		
Communication & Mail Server	2		
DR Center Server Cost			
Database & Reporting Server	1		
Application Server	1		
Intranet Web Server	1		
Internet Web Server	1		
Directory & Access Server	1		
Communication & Mail Server	1		
Automated Tape Library (ATL) for Data Center with Backup Software	1		
Fiber Cabling and Network Items for Data Center and DR Center			
WAN / Core Router	2		
Internet Router	2		
Core Switch L3 Gigabit 48 Port	2		
Network Racks 42 U	2		
Patch Panel 24 Ports CAT 6	2		
Information Outlet CAT 6	36		
CAT 6 Cable (305 Mtr. Box)	3		

Data Center & Disaster Site Hardware & Software			
Item Description	**Qty.**	**Make**	**Model**
Patch Cord 1 Mtr CAT 6	36		
Patch Cord 2 Mtr CAT 6	36		
UTM Firewall with VPN and IPS	2		
Software for Data Center and DR Center			
Data Center Software (Server OS with CAL, Server Management, Intranet Portal, MIS & Reporting Dashboard etc.)	18		
Database Software (Processor Based for unlimited users)	8		
Antivirus Software for Servers	18		
Email Security Software	2		
Enterprise Management System (EMS) (EMS for managing & monitoring all the devices of DC and DR including all Servers for the entire project period)	2		
Outsourced manpower for datacenters 2 nos. × 3 shifts for 6 Years, (432 Man Months)	432		

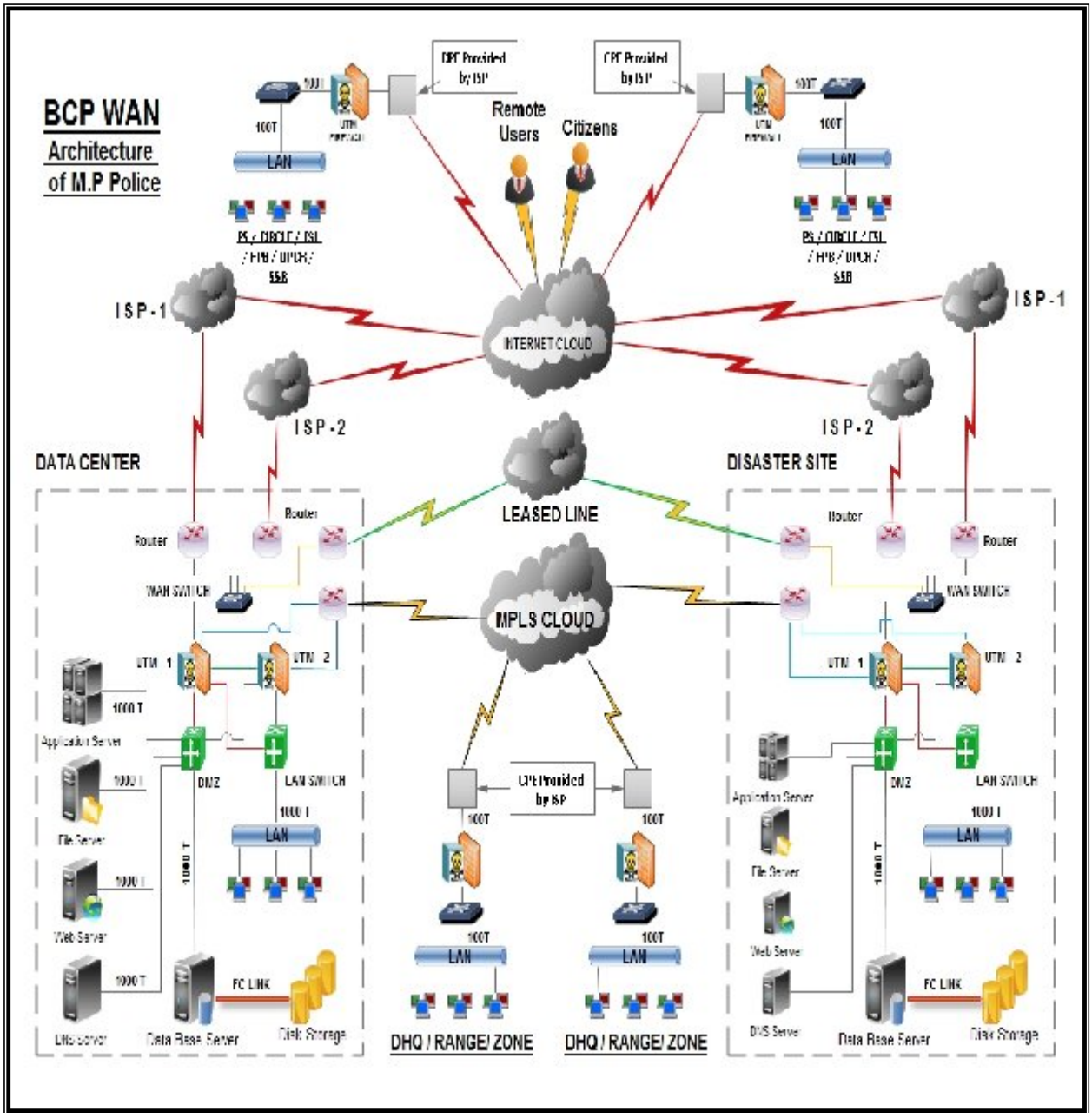
The breakup of outsourced manpower for data center is given below:

Technical Support and Other Project Team	
Items	**Minimum Manpower**
System & Network Administrator at DC	3
Technical Support Staff at DC	3

Note:

- The cost of outsourced manpower is required for the entire project period after readiness of Data Center i.e. for the period of approximately six (6) years (One year implementation phase and five years of O&M phase).
- "Application Patch Management & Asset Management Software" should be from same EMS vendor to provide tight integration between EMS & Asset Management Software.
- The Servers, Storage and Tape Library must be supplied at DC and DR along with the required Racks and associated accessories as per industry standard.
- **The bidders must submit bill of quantity in the above prescribes format along with the technical bid clearly specifying the Make and Model of the proposed hardware and software.**

ANNEXURE IV: Indicative Network Connectivity Solution



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

The SI shall provide the service and support for testing & running of last mile connectivity to the Police Stations / Higher Offices wherever required. SI shall support for procurement of he connectivity from a service provider and the SI is expected to provide service support during setup the last mile connectivity to the client site. SI shall use SWAN for the connectivity redundancy where feasible. SI shall prepare comprehensive network architecture for connecting all the Police Stations / Higher Offices to the Police Head Quarters Server room and DRC and also the connectivity from the Police Head Quarters Server room / DRC to the DC / DRC at the Center hosting the CAS (Center).

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

Scope of Network Connectivity:

Madhya Pradesh Police has 1420 locations across the state and under CCTNS project all the police locations must have network connectivity to use CAS application for tracking crime and criminal. By considering this guideline; it is proposed to setup multi-level network schemes for connectivity. For 996 police stations; it is proposed to setup VPN over broadband and for rest of the higher locations i.e. 371 would be connected through MPLS, Remote Locations (Police Stations) must be connected via VSAT/Wireless mode if there are unable to get in line connectivity, apart from these Location like State FSL, State FPB, State Police Control Room and District Police Control Room and other offices would be connected through Broadband Connectivity. At DC & DR Site MPLS Link as well as Internet Link is proposed with adequate capacity and redundancy.

As Per the Directives obtains from MHA/ NCRB; Broadband connectivity can be taken from BSNL and / or SWAN only.

The Networking solution of CCTNS project shall be based on a Hybrid Model which will consist of State Wide Area Network (SWAN) operated by State under SWAN scheme and Data network operated by Bharat Sanchar Nigam Limited (BSNL) which consists of Point to point leased lines, VPNoBB, WiMax, VSAT and MPLS technologies. BSNL shall be providing the Networking & Connectivity services along with Operations & Maintenance for all the locations implemented by BSNL in the Madhya Pradesh. BSNL shall also provide connectivity on MPLS VPN network for aggregated bandwidth at Madhya Pradesh SDC (State Data Center) for the locations connected on VPNoBB, WiMax and VSAT network and also provide connectivity for SDCs (State Data Centre) at State Headquarters (SHQs) to the National Data Centre (NDC) of NCRB. Further BSNL shall provide MPLS VPN network for connecting SDC and Disaster Recovery Centre (DRC) of the MPCOPS/ MP Police. The DRC location will be finalized by the MPCOPS/MP Police at the time of execution of project or Other State's Data Center (SDC) may be mutually considered as DRC.

System Integrator shall provide necessary service support and assistance to MP Police / MPCOPS for taking the bandwidth for WAN connectivity from BSNL and / or SWAN and also provide and subsequent, required, and related maintenance / support services.

Note: Provisions of WAN connectivity is subject to the approval of MHA/ NCRB.

Scope of work for BSNL:

The details of scope of work of BSNL are as under:

a) Provisioning of 2Mbps Point to Point Lease Line (P2PLL) for locations to be connected with the nearest SWAN POP.
b) Provisioning of WAN connectivity on VPNoBB/ WiMax/ VSAT for locations which are not feasible to be connected directly with the SWAN on P2PLL.
c) Provisioning of the Routers (at CCTNS site) and Modems for locations to be connected directly with SWAN and all other hardware and network infrastructure provided for VPNoBB/ WiMax/ VSAT connectivity.
d) Provisioning of Aggregated bandwidth on MPLS network at State SDC for the locations connected on VPNoBB, WiMax and VSAT network.
e) Provisioning of MPLS connectivity between State SDCs and DRC.
f) Provisioning of MPLS connectivity between NDC and State SDC.
g) Maintaining the network including hardware supplied for minimum period of 5 years.

Role of System Integrator:

The SI shall coordinate with all stack holder of the project viz. BSNL and the MPCOPS / MP Police Department etc. for implementation of the Network and Connectivity solution of CCTNS project. The following are the key responsibilities of the SI with respect to Networking and Connectivity.

a) Site preparation at all locations for establishment and installation of networking and connectivity solution.
b) Coordination with the State Police Department and nominated officials of BSNL for Installation, Configuration, Testing, and Commissioning of BSNL's 2Mbps Point to Point Leased Lines for connecting with SWAN, VPNoBB, WiMax, VSAT, and MPLS links.

c) Coordination with BSNL for ensuring Operations and Maintenance of networking hardware to ensure compliance to the SLAs as offered by BSNL.

d) The SI will also be coordinating with BSNL and State Police Department for SLA Monitoring, Fault Reporting & Troubleshooting of the links for meeting the Service levels and Service Agreement.

e) The Police Stations and Higher Offices which are within the proximity of SWAN PoP (Point of Presence) will be connecting on LAN directly from SWAN PoP. The SI shall also coordinate with SWAN operator (Appointed under SWAN project) for Installation, Configuration, Testing and Commissioning of LAN connectivity for sites co-located within the SWAN PoP and LAN connectivity from SWAN NOC (Network Operation Centre) to the SDC. The SI shall be coordinating with SWAN operator for SLA Monitoring, Fault Reporting & Troubleshooting of the LAN links as per SWAN SLA.

f) SI shall also coordinate with State CCTNS Nodal Officer (State Police Department) for finalizing Police stations lists for the connectivity options, issuing commissioning report for demand note/payment clearance, reporting SLA and providing for link status updates.

Note: The process of finalization for signing of contract with BSNL as Service provider for CCTNS project is in progress and detailed guidelines on implementation of Networking and Connectivity will be sent to MP Police/MPCOPS by NCRB/MHA.

Annexure V: Technical Specifications

Note: The bidders must submit technical compliance statement in the prescribed formats given below and product datasheet, along with the technical bid for all the proposed hardware and software.

1) Desktop System:

Scope:

MP Police needs desktop computers for implementing Mission Mode Project –CCTNS. Information technology based project includes complete IT tools to make Police personnel quipped for improving their day to day working and G2G & G2C service n service levels. Due to complete dependability of this project on IT, high end desktop systems are required to smoothly run CAS application and support to several queries. System Integrator is responsible for supply, install, testing, commissioning, and maintenance of desktop computers as per below specification:

Specification of Desktop:

Type	Details	Compliance (Y/N)
1. With Core 2 Duo		
CPU	Intel Core 2 Duo, 2.93 GHz or higher, 3 MB L2 Cache and 1066 MHz FSB / AMD Phenom II X2 550, 2.93 GHz, 6 MB L3 Cache, 4000 MHz HT or higher.	
Chipset	Intel 4 Series / AMD or better	
Graphics	Integrated Intel / AMD Graphics Media Accelerator	
Bus Architecture	Two PCI, One PCI Express x1 and One PCI Express x16	
Memory	2 GB 1066 MHz or higher DDR2 RAM with 4 GB Expandability	
Hard Disk Drive	320 GB 7200 rpm Serial ATA HDD.	
Monitor	47 cm (18.5 inch) TFT Digital Color Monitor TCO-05 certified	
Keyboard	**Bilingual (Hindi & English)** USB Keyboard with 104 or higher keys	
Mouse	USB Optical Mouse, Two button Scroll	

Bays	4 Nos. (2 Nos. 5.25 inches for Optical Media Drives and 2 Nos. 3.5 inches for Hard Disk Drives).	
Ports	6 USB Ports (with at least 2 in front), 1 Serial, Audio ports for microphone and headphone in front.	
Cabinet	Mini Tower	
DVD ROM Drive	8X or better DVD ROM Drive.	
Networking facility	10/100/1000 on board integrated Network Port with remote booting facility remote system installation, remote wake up.	
Product Certifications	Windows 7 & Linux Certification. However UL and FCC Certification is preferable	
OEM Certifications	ISO 9001-14001, ISO 9001-2008, Should be in the list of Top 5 Desktop brands as per IDC report published for India during year 2010. However Greenpeace international certification is preferable	
Power Management	Screen Blanking, Hard Disk and System Idle Mode in Power On, Set up Password, Power supply SMPS Surge protected.	

Type	**Details**	**Compliance (Y/N)**
2. With Intel Core i5 Processor		
CPU	Intel Core i5-650, 2.93 GHz, 4 MB L3 Cache and 1066 MHz FSB / AMD Phenom II X2 555, 6 MB L3 Cache, 4000 MHz HT or higher	
Chipset	Intel 5 series / AMD or better	
Bus Architecture	Two PCI, One PCI Express x1 and One PCI Express x16	
Memory	2 GB 1066 MHz or higher DDR2 RAM with 4 GB Expandability	
Hard Disk Drive	320 GB 7200 rpm Serial ATA HDD.	
Monitor	47 cm (18.5 inch) TFT Digital Color Monitor TCO-05 certified	
Keyboard	Bilingual (Hindi & English) Keyboard with 104 or higher keys	

Mouse	USB Optical Mouse, Two button Scroll	
Bays	4 Nos. (2 Nos. 5.25 inches for Optical Media Drives and 2 Nos. 3.5 inches for Hard Disk Drives).	
Ports	6 USB Ports (with at least 2 in front), 1 Serial, Audio ports for microphone and headphone in front.	
Cabinet	Mini Tower	
DVD ROM Drive	8X or better DVD Writer	
Networking facility	10/100/1000 on board integrated Network Port with remote booting facility remote system installation, remote wake up.	
Product Certifications	Windows 7 & Linux Certification. However UL and FCC Certification is preferable	
OEM Certifications	ISO 9001-14001, ISO 9001-2008, Should be in the list of Top 5 Desktop brands as per IDC report published for India during year 2010. However Greenpeace international certification is preferable	
Power Management	Screen Blanking, Hard Disk and System Idle Mode in Power On, Set up Password, Power supply SMPS Surge protected.	

Software for Desktops:

System Integrator is responsible for supply, install, testing, commissioning and maintenance of software in desktops as per details and quantities specified in **Annexure-III Bill of Quantity**.

All the licenses should be in the name of DGP, MP Police, Bhopal.

All System software licenses shall be genuine, perpetual, full use and should provide patches, bug fixes, security patches, and updates directly from the respective developer / manufacturer for the contract period.

The software product used should have well defined product roadmap by the respective developer / manufacturer.

The proposed system software must provide indemnification and indemnification must cover patent claims, copy right claims, legal fees and damages claim. System integrator or respective developer / manufacturer must protect the department from all such legal cost that may arise out of any claim by a third party alleging intellectual property infringement i.e. related to the software.

Bidder shall provide a comprehensive warranty that covers all components after the issuance of the final acceptance test of department. The warranty should cover all materials, licenses, services and support for both hardware and software. Bidder shall administer warranties with serial number of

equipment during warranty period. Upon final acceptance of the MP Police / MPCOPS any developer / manufacturer warranties will be transferred to the MP Police / MPCOPS at no additional charge. All warranty documentation (whether expired or not) will be delivered to MP Police / MPCOPS at the issuance of final acceptance certificate.

2) HDD 160 GB:

Scope:

System Integrator is responsible for supply, install, testing, commissioning and maintenance of addition hard disk drive in one of the desktop computer to be supplied at police station level as per direction of MPCOPS.

Specification:

Type	Details	Compliance (Y/ N)
Type	Internal – Serial ATA	
Speed	5400 RPM or higher	
Hard Disk Size	160 GB	

3) Duplex Laser Printer (Network):

Scope:

As CCTNS would bring automated way of crime registration and proceedings; this leads to dependability over computers for fast working. Swift hardcopy retrieval would be the key requirement after implementing CCTNS project. By focusing this point; each police station needs a duplex laser printer that helps them for fast retrieval of Hard copy document as well as printer must furnish multi user accessibility (Networking Mode) so that everyone can access printer and get the desired document.

System Integrator is responsible for supply, install, testing, commissioning and maintenance of laser printer at every police station as per below specifications:

Specification:

Type	Details	Compliance (Y/N)
Speed	28 PPM (A4) or higher	

Processor	400 MHz or higher	
Resolution	Min. 1200 x 1200 dpi	
Duty Cycle	Min. 50,000 page / month	
Memory	64 MB or higher	
Interface	USB 2.0 (High Speed) with USB Cable	
Network	Yes (10/100Mbps)	
Duplex	Yes	
Paper support	A4	
Compatibility	Windows XP/ Windows Vista/ Windows 7 / Linux	

4) Multi-Function Laser (Print, Scan, Copy):

Scope:

To get Fast hard copy document from system is a vital need of every police locations; along with this police stations need a tool that help them to get photo copy/scanned copy of any authentic hard copy document. To achieve this, it is proposed to get a multi-function (Scan/Copy/ Print) printer for police locations so that they can get all the facility from a single point as well as this will help police staff to get print out when another printer is occupied on printing work this will lead to fast working of police.

System Integrator is responsible for supply, install, testing, commissioning, and maintenance of Multi-function laser printer to all police locations and must make sure that it would run without any interruption.

Specification:

Type	**Details**	**Compliance (Y/N)**
Functions		
All-in-one functions	Print, Copy, Scan	
Multitasking capability	Yes	
Printing specifications		

Print speed, black (normal quality mode)	18 PPM or higher	
First page out (black)	As fast as 8 to 9 second	
Monthly duty cycle	Up to 8000 pages	
Print technology	Laser	
Print resolution, black	Minimum **600 x 600 x 2 dpi** preferable Up to 1200 x 1200 dpi	
Scanner specifications		
Scanner type	Flatbed, ADF	
Scan resolution, optical	Up to 1200 dpi	
Bit depth	24-bit OR 64 bit	
Scan size, maximum (flatbed)	A4	
Scan size, maximum (ADF)	A4	
Scan speed (default)	15 ppm or higher	
Copier specifications		
Copy resolution, black	Up to 600 x 600 dpi	
Copy resolution, color	Up to 1200 x 1200 dpi	
Copy reduce/enlarge settings	25 to 400%	
Maximum number of copies	Up to 99 copies	
Compatibility	Windows XP/ Windows Vista/ Windows 7 / Linux	

5) Offline UPS SYSTEM (1 KVA)

Scope

1 KVA UPS is required for back-up purpose to feed power to the desktops and network devices in odd time when electricity would not be available. UPS is required to get uninterrupted working from police.

System Integrator is responsible for supply, install, testing, commissioning and maintenance of line interactive (Offline) UPS at SP/SRP /PHQ offices and must ensure that it will work without any interruption.

Specification:

Type	Description	Compliance (Y/ N)
Capacity	1 KVA	
Technology	PWM using MOSFET / IGBT (Indicate the make, capacity and other technical details of the MOSFET/IGBT)	
A. MAINS MODE		
1. AC INPUT		
1. Voltage	160 to 270Volts	
2. Frequency	50 Hz + 3 Hz	
2. AC OUTPUT		
1. Voltage Window	200V to 245V (with AVR). The output voltage should be within 200V to 245V range at any point of time during input window of 160V to 270V. Please mention type of AVR.	
2. Frequency	Sync to Mains	
B. INVERTER MODE (Output)		
1. Voltage	230 volts + 5% during all condition in inverter mode like Full load to no load, backup period etc.	
2. Frequency	50 Hz + 0.5 Hz	

3. Load Power Factor	0.6 (Lag)	
4. Output Load	600W for 1 KVA	
5. Wave Form	Quasi Sine wave	
6. Inverter Efficiency	≥ 65 % (on full rated capacity of UPS at 0.6 load PF)	
7. Total Harmonic Distortion	**≤ 22%**	
Battery Bank		
1. BATTERY	VRLA (Sealed Maintenance Free)	
2. Minimum Battery Backup	120 minutes on full load	
3. Battery End Cell Voltage	> 10.5V (None of the Battery should be discharge below 10.5V)	
4. Battery Cabinet	Inbuilt / separate cabinet matching to the UPS cabinet. In case of separate battery cabinet, the cabinet should be free from sharp edges, scratches, nicks & burs etc.	
5. UPS Cabinet	UPS cabinet should of minimum 1mm thick material and should be free from sharp edge, scratches, nicks, & burs etc.	
PROTECTIONS		
1. Short Circuit	Electronic current limit in inverter mode & Fuse/MCB in mains mode.	
2. Surge/Spikes	Through Line Filters	
3. DC under Voltage	Yes	
4. Overload	Yes	
DISPLAY	1. UPS Status, 2. Load Status, 3. Battery Status / Low Battery	
ALARMS	For any Fault Condition and Low Battery	
OTHER FEATURE	Cold Start, Night Guard, No load shutdown, & Generator Compatibility should be provided.	
AC Output SOCKETS	Minimum 3 Nos. (230V/5A ISI mark) sockets / IEC socket with cable and additional output terminal for 700VA and above capacity.	

6) ONLINE UPS SYSTEM (2 KVA)

Scope:

2 KVA UPS is required for back-up purpose to feed power to the desktops and network devices in odd time when electricity would not be available. UPS is required to get uninterrupted working from police.

System Integrator is responsible for supply, install, testing, commissioning and maintenance of Online UPS at all police stations (including CIPA PS) / Sub Division/ Ranges/ Zones/ SCRB offices and must ensure that it will work without any interruption.

Specification:

Type	Details	Compliance (Y/N)
Type	True Online, Double Conversion	
Capacity	2 KVA	
Technology	PWM Technique using IGBT with internal / external Isolation transformer or Transient Voltage Surge Suppressor	
Input Volt	120-270 Volt (on full load)	
Input Power factor	> 0.95	
Output volt	230 V ± 1%	
Output Frequency	50Hz ± 0.1%	
Wave form	Sine Wave	
Distortion	THD < 3%	
Battery backup time on full rated load (SMF batteries)	2 Hours (Min 5000 VAH)	
LED or LCD	Display should be as per industry standard that Allows users to monitor same as its place of installation.	
Make of SMF batteries	Panasonic/ Exide/ Amar raja/ Luminous SMF(VRLA) or equivalent	
Rack	Suitable metallic rack for housing of SMF batteries	
SNMP Support	Yes	

7) Portable Generator Set:

Scope:

DG set would have great importance to keep the system running in the absence of Electricity. Success of CCTNS project depends upon uninterrupted power supply that can only be achieved with standard portable DG sets, so that in absence of power it would provide backup to the systems.

System Integrator is responsible for supply, install, testing, commissioning and maintenance of Portable Generators at all police stations (including CIPA PS) / Sub Division/ Ranges/ Zones/ SCRB offices and must ensure that it will work without any interruption.

Specification:

Type	Details	Compliance (Y/N)
Rated Power	2 KVA	
Rated Current	AC 3.0 A/ AC 7.1A	
Ignition system	Transistor Controlled Ignition (TCI)	
Fuel Tank Capacity(Diesel run)	2.7 L or higher	
Fuel Tank Capacity(petrol starting)	0.25 L	
Continuous running hours	6 Hours	
Frequency (Hz)	50 Hz	
Rated Output (VA)	350 VA	
Maximum Output (VA)	450 VA	
Silent type	Yes	

8) Layer 2 Managed Network Switch 16 Ports 10/100 MBPS

Scope:

Network switch is required to connect computers in one LAN. System Integrator is responsible for supply, install, testing, commissioning and maintenance of Network Switches to provide data connectivity to all desktop computers.

Specification:

Type	Details	Compliance (Y/N)
Standards	IEEE 802.3 Ethernet, IEEE 802.3u Fast Ethernet, IEEE 802.3x Flow Control, Compatible with all major network software.	
Network Interface	RJ 45 UTP - 10/100BaseT	
Switching Method	Store – and – forward	
Switch Fabric	4.8 Gbps	
MAC Address Table	4000 Entries or higher, however 8000 entries are preferable	
Filtering/ Forwarding/Learning Rates	Full line rate/full wire speed	
Physical Specifications	Metal Housing Side Air Vents with proper Air-Cooling Design	
LEDs	100Mbps – one per port 10Mbps – one per port Power Link/Act (activity)	
Power Requirements	Universal AC input: 100 to 240 VAC, 50 to 60 Hz, Internal Universal Power Supply	

9) Finger Print Reader:

Scope:

System Integrator is responsible for supply, install, testing, commissioning and maintenance of finger print reader to all police stations and must make sure that it will work uninterrupted.

Specification:

Type	Details	Compliance (Y/N)
Sensor Type	Optoelectronic	
Prism Architecture	Dual Prism	
Size of window	Minimum – 45mm x 45mm Preferable upto – 45mm x 48mm	
Glass thickness	25mm	
Resolution	500 PPI or higher	
Image grey scale	256 level Dynamic	
Scanning time	0.01Sec.	
Distortion rate	0.1%	
Computer interface	USB2.0 , USB Powered	
Operating temperature	0 – 55 Degree C	
Environmental humidity	Up to 90%	
Optical /Film Coating	Hygroscopic	
Operating system Support	Window XP / Vista / 7 / Linux	
Complaint	P.I.V.	

10) Digital Camera:

Scope:

To capture crime scene and criminal's snap, Police personnel needs a handy digital camera that makes them equipped for investigation process.

System Integrator is responsible for supply, install, testing and maintenance of digital camera to every police station and must ensure that it will work properly.

Specification:

Type	Details	Compliance (Y/N)
Pixels (Min.)	12 megapixels or higher	
LCD Monitor		
Type	TFT	
Display Size	2.7 inches or higher	
Recording Format	JPEG	
Zoom	4X or higher	
ISO Sensitivity Setting	Auto / 80 / 100 / 200 / 400 / 800 / 1600 / High	
Recording Media	SD memory card, SDHC memory card, SDXC memory card, Multimedia Card	
Optical Zoom During Movie Recording	Yes	
Auto Focus Range	Approx: (W)=3 cm to infinity, (T)= 80 cm to infinity	
Self Timer	Yes	
Shooting Modes	Auto, Portrait, Landscape, Night Snapshot, Indoor, Face self-timer, Low Light, Beach, Foliage, Snow, Fireworks, Long Shutter, Movie & Documents. Underwater support is preferable	

White Balance	Auto / Daylight / Cloudy / Fluorescent / Incandescent / Flash	
Flash Function	Auto/ Red Eye Reduction/Off/Face detection/noise reduction	
USB Connectivity	Yes (Hi- Speed)	
Battery Backup	120 Min	
Operating system Support	Window XP / Vista / 7 / Linux	

11) Electronic Pen:

Scope:

System Integrator is responsible for supply, install, testing, commissioning and maintenance of Electronic pen at each police stations and must make sure that it will work properly and uninterrupted.

Specification:

Item	Details
Data communication	USB 1.1 standard (also supports USB 2.G standard), Bluetooth 1.2 standard
Built-in battery	Rechargeable battery
Continuous writing time	2 hours or longer Standby time:1 hours (min.) without a cap
Charging time	Approx. 2 hours (from 0 to100% charge)
Charging method	Dox cradle or USB adapter
Operating system Support	Window XP/ Vista/ 7/ Linux

12) Furniture:

Scope:

System Integrator is responsible for supply, install, testing, commissioning and maintenance of computer furniture to all the police stations (excluding CIPA Police Stations)/ higher offices (Sub Division, Range/ Zone /SCRB, SP/SRP, PHQ) and must ensure the quality of delivered furniture as per details given below.

Specification:

Type	Details	Compliance (Y/N)
Computer Table **Size: L 910 x W 610 x H 728 mm**	Top: Size 910 x 610 mm made of 18 mm thick pre laminated medium density fiber (MDF) board ISI Marked (IS: 14587-1998). The top shall be firmly screwed on 25x25x1 mm square tube frame as shown in figure.	
	Upper side of laminated board shall be in natural teak shade while the bottom side shall be white/cream shade.	
	Sliding key Board tray: A Sliding key Board tray shall be made of 18mm pre laminated medium density fiber board of size 725x450 mm. The gap between top and tray shall be 100mm.	
	Key board tray shall slide smoothly on sliding channel duly powder coated having nylon roller arrangement.	
	The storage shelve for CVT : A storage shelve made of 18 mm particle board shall be provided along with the length of the table at bottom about 100 mm above from the ground level. Shelves shall be screwed on frame work of 25x25x1 mm square tube. The shelve shall be covered from back side with 18mm pre laminated medium density fiber board as shown in drawing.	
	Steel Structure: The rigid steel structure shall consist of two nos. rectangular base tubes of size 50x25x1.25 mm about 520 mm length placed along the width on vertical tubes of size 25x25x1 mm shall be welded for fixing up of side panels. A supporting frame of 25x25x1	

Type	Details	Compliance (Y/N)
	mm square tube shall be welded on the top of the tubes for the side panels as shown for supporting the top of the table.	
	The base tube shall be provided with adjustable shoes 2 nos. on each side.	
	Painting: Complete frame of tubes shall be powder coated.	
Printer Table **Size: L 610 x W 610 x H 660 mm**	Printer table shall be as per figure/ drawing.	
	Shelves : 3 no. made of 18mm thick pre laminated Medium Density Fiber Board(MDF) ISI marked (IS 14587 – 1998)	
	Top shelve size 610x610 mm for placing printing unit.	
	Middle Shelve size 460x330 mm for placing feet on stationary.	
	Bottom shelve size 460x380 mm for collecting print out.	
	The top faces of the shelve shall be natural teak wood shade.	
	The bottom faces shall be in plain white/cream shades.	
	Structure: The structure shall be made from square and rectangular steel tubes duly welded finished and powder coated.	
	Vertical tubes shall be welded in two rectangular bottom tubes 50x25x1.25 mm as shown in drawing.	
	The horizontal tube 25x25x1 mm thick 330 m	

Type	Details	Compliance (Y/N)
	long shall be welded over vertical tubes 25 mm off the center width /depth wise.	
	Panels made of 18 mm pre laminated particle board shall be screwed rigidly between vertical tubes on both sides.	
	Two nos. bottom support tubes 50x25x1.25mm thick shall also be provided with two nos. of adjustment shoes.	
	A rectangular slot of size 455x25 mm shall be provided on top shelve along with length for feeding stationary as shown in figure. A slot shall be covered with PVC insertion for safely of paper.	
	The ends of bottom and top shall be plugged with PVC/ plastic caps.	
	Painting: Complete steel structure shall be pretreated and powder coated with minimum thickness of 60 microns coating.	
Computer Chair with Handle	Seat size shall be 430x430 mm on 10 mm. thick molded comm. ply with 60 mm thick 40 density molded PU foam	
	Back rest size shall be 400x300 mm on 10 mm thick molded comm. ply with 40 mm thick 32 density molded PU foam covered with tapestry.	
	The height of back rest shall be 900x500 mm for top and bottom edges respectively. The black rest shall be provided with lifting arrangement on flat iron & helical spring.	
	Two nos. suitable PU handles shall be proved.	
	The base stand should be made up of 5 prongs duly pressed welded together centrally with a	

Type	Details	Compliance (Y/N)
	pedestal bush with good quality twin wheel castors. The stand and other metal parts excluding central spindle shall be powder coated. Complete steel structure shall be pretreated and powder coated with minimum thickness of 60 microns coating.	
	A central spindle of 25mm dia rod without threads shall be provided with revolving arrangements. The adjustable height of chair shall be from 530 to 570 mm.	
	A good quality tapestry cloth shall be provided on seat & back in attractive color/ shade.	

13) Electric Cabling:

Scope:

Scope of Electrical cabling, is to provide power supply for devices installed. System Integrator is responsible for supply, install, testing, commissioning and maintenance of electrical cabling for supplying power to run installed devices at police locations.

Specification:

1. Total 5 Electrical Points Including 3 Switches & 3 Sockets in Each Point, (2 No. 5-Amps and 1 No. 15 Amps.) - Point wiring using ISI approved PVC Conduit / Casing Capping, 1.1 KV grade 2.5 square meter FRLS Cu flexible wire including supply of wire, switch, socket and GI Box. Including all necessary hardware & accessories complete, material and labor as per requirement of the MP Police. For point wiring having Average Point length is12 to 18 Meters.

2. UPS & Generator Set Cabling: Electrical Cabling for Network Rack, Four Computer Points, separate cabling for Two Printers from main input and Generator set to UPS Including change-over, MCB and all other accessories as per requirement.

14) Earthing and Earth Pit:

Adequate earthing through underground earth pit should be prepared that prevent causes generated from improper power supply. Separate Copper Plate Earthing (With Plate Size 300X300X3 MM), The Earth resistance should not exceed 2.5 Ohms, and Ground to earth Voltage should not be more than 3 volts.

15) Wall Mounted Network Rack- 9U

Scope:

Wall mounted rack is required for structured cabling. Wall mounted rack should be supplied as per below specifications and follows industry standards.

System Integrator has to supply, install and commission wall mounted network rack (9U) and make sure its quality with all its prerequisites accessories.

Specification:

Details	Compliance (Y/N)
19" Wall mount, 9 U height	
Minimum Powder quoted steel Body with front door of glass.	
Completely covered & have security locks.	
Proper ventilated with One Fan, One Cable Manager, Power Distribution Unit of 6 No. (5 and 5 Amp) Sockets with surge protection, Mounting Accessories,	
Fitted with Copper Strip for earthing the equipments	

16) Cat- 6 Patch Panel

Scope:

Scope of Patch panel is to get structured cabling as per industry standards and distribution of data Bandwidth. System Integrator must ensure that patch panel is properly mounted in racks with necessary impacting of data cables.

Specification:

Type	Details	Compliance (Yes/No)
Type	24 or 12 port patch panel as per requirement, Unshielded Twisted Pair, Category 6, ANSI/TIA/EIA 568-B.2.1	
Category	Category 6	

Circuit Identification Scheme	Port Labeling for port identification on each of 24-ports	
Port Identification	Labels on each of 24/48-ports (to be included in supply)	
Height	1 U (1.75 inches)	
Modular Jack	750 mating cycles	

17) Information Outlet Cat 6(Single Port wall mounted)

Scope:

Scope of IO cat 6 is to get better connectivity to computers and maximum utilization of bandwidth as per industry standards.

System Integrator has to install and commission information outlet (cat 6) to provide network connectivity to the systems / Devices. System Integrator must make sure its quality and proper functioning.

Specification:

Type	Details	Compliance (Yes/No)
Type	1-port, Shuttered, White, with surface box for surface mount applications, Category 6,TIA/EIA 568-b Category	
Material	ABS/Polycarbonate	
No. of ports	One	
Protection	Shutters	
Identification	To be supplied with label for port identification	

18) Cat - 6 Cable with cable lying in PVC conduit

Scope:

The cabling material shall be supplied, laid tested and commissioned in accordance with specifications and site requirements.

System Integrator must make sure that all the cabling shall run through PVC conduit / Casing Capping of suitable size of ISI standard. Separate PVC conduits or Casing Capping shall be used for electrical and data cabling.

Laying of Cables- SI must make sure that Cables shall be laid by skilled and experienced workmen using adequate equipments to minimize stretching of the cable.

All terminations should be carried out according to the manufacturer's instructions and guidelines and standards of generic cabling systems. When terminating outlets, care must be taken to avoid damaging the copper cores when stripping back the outer sheathing.

Testing and Documentation: SI must make sure that Testing of each node should be done as per manufacturer standards and the final report should be submitted.

UTP COMPONENTS: SI must make sure that the system should Meet or exceed TIA/EIA 568 B-2 specifications of Category-6 as a system. All performance parameters -Attenuation, Pair -to-Pair and power sum NEXT, Pair And Power sum ELFEXT, Return Loss and Delay skew should be tested for 100m Channel as well as 90m permanent Link. It should be a single OEM solution and should ensure optimum system performance. There should not be any Impedance mismatch problems among components of the cabling system. The complete system should be tested up to 600 MHz for all the test parameters to ensure the end-to-end system performance.

Specification:

Type	Details	Compliance (Yes/No)
Type	Unshielded Twisted Pair, Category 6, ANSI/TIA/EIA 568-B.2.1	
Conductors	24 AWG solid bare copper	
Insulation	Polyethylene/Polyolefin	
Jacket	Flame Retardant PVC	
Approvals	UL Listed	
	ETL verified to ANSI/TIA/EIA 568-B.2.1 Cat 6	
Operating temperature	-20 Deg. C up to +60 Deg. C	
Frequency tested up to	600 MHz	
Delay Skew	25ns-45ns / 100m MAX.	
Impedance	100 Ohms + / - 6 ohms	

19) Cat-6 Patch Cord (1-Meter)

Scope:

Scope of 1 meter Patch cord is to get connectivity between patch panels to switch. System Integrator has to provide proper connectivity via Cat-6 Patch Cord (1 Meter) and must make sure it will be proper dressed in rack and function properly.

Specification:

Type	Details	Compliance (Yes/No)
Length	3 Feet	
Conductor	24 AWG 7 / 32, stranded copper	
Cable Type	UTP CAT 6 ANSI/TIA/EIA 568-B.2.1	
Plug Protection	Matching colored boot to maintain bend radius	
Warranty	20-year component warranty	
Category	Category 6	
Terminals	Phosphor Bronze with gold plating	
Jacket	PVC	
Insulation	Flame Retardant	

20) Cat - 6 Patch Cord (3 Meters Length)

Scope:

Scope of 2 meter Patch cord is to get connectivity between IO to desktop/Printers. System Integrator has to provide proper connectivity via Cat-6 Patch Cord (3 Meter) and must make sure it will function without any interruption.

Specification:

Type	Details	Compliance (Yes/No)
Length	7 Feet	
Conductor	24 AWG 7 / 32, stranded copper	
Cable Type	UTP CAT 6 ANSI/TIA/EIA 568-B.2.1	

Plug Protection	Matching colored boot to maintain bend radius	
Warranty	20-year component warranty	
Category	Category 6	
Terminals	Phosphor Bronze with gold plating	
Jacket	PVC	
Insulation	Flame Retardant	

Annexure VI: Technical Specification: Data Center

1) Blade Chassis Specification:

Item	Description of Requirement	Compliance (Y/ N)
Base Chassis	Single blade chassis should accommodate at least 16 hot pluggable blades or more. Should support two and Two and four processor based blade server of latest generation	
	Same chassis should support Intel, AMD and RISC / EPIC processor based Blade Servers for future applications	
	Minimum 2 external USB connections functionality,	
	Height of chassis should be 10 U or Less Rack-mountable	
	Single console for all blades in the enclosure or KVM Module with built in KVM switch or Virtual KVM feature over IP.	
	Should support Hot Pluggable & Redundant chassis Management Modules	
	Dual network connectivity for each blade server for redundancy should be provided. Backplane should be completely passive device. If it is active, dual backplane should be provided for redundancy	
	DVD ROM can be internal or external, which can be shared by all the blades allowing remote installation of S/W and OS	
Interconnect support	Should support simultaneous housing of Ethernet, FC, SAS, iSCSI, IB interconnect fabrics, offering Hot Pluggable & Redundancy as a feature. Enclosure Should have minimum 8 Interconnect Bays.	
Blade Server Ethernet Interconnect	The chassis should have 2 Nos. of 10 Gb redundant network switches with 16 Nos. of 10 Gb Downlinks ports and at least 4 x 1 Gigabit and 4 x 10 GB uplink ports per switch for connecting to the data center switch.	
Blade Server FC Interconnect	The enclosure should support 24 ports redundant fiber channel SAN switch with at least 8 Gbps auto negotiating FC uplink and 8 Gbps auto negotiating downlink to all server bays and 8 Gbps Fiber Channel for connectivity to the external Fiber channel Switch and ultimately to the Storage Device.	

Item	Description of Requirement	Compliance (Y/ N)
Power Supply	Hot Swap redundant power supplies to be provided, Power supplies should have N+N. All Power Supplies modules should be populated in the chassis	
Cooling	Each blade enclosure should have a fully populated cooling subsystem consisting of hot pluggable fans / blowers enabled with technologies for improved power consumption and acoustic	
OS Environment	Support heterogeneous environment: AMD, Xeon and RISC/EPIC CPU blades must be in same chassis with scope to run Win2003/2008 Server, Red Hat Linux / 64 Bit UNIX, Suse Linux / 64 Bit UNIX / Solaris x86	
Management	Systems Management and deployment tools to aid in Blade Server configuration and OS deployment, It should provide Secure Sockets Layer (SSL) 128 bit encryption and Secure Shell (SSH) Version 2 and support VPN for secure access over internet. Ability to measure power historically for servers or group of servers for optimum power usage. Blade enclosure should have provision to connect to display console /central console for local management like trouble shooting, configuration, system status / health display. Dedicated management network port should have separate path for management.	
Deployment & Remote Management	Complete Hardware based Remote Administration from a standard web-browser with Event logging, detailed server status, Logs, Alert Forwarding, virtual control, remote graphical console, Remote Power Control / Shutdown, Virtual Media for Remote boot and configuration, Virtual Text and Graphical Control. The blade system should have the capability of managing all the blades in the same enclosure simultaneously.	

2) Blade Server Specification (Web, Application, Directory, Communication, EMS & Backup):

Item	Feature Requirements	Compliance
Form Factor	Blade	
Processor	Two Nos. Intel Xeon Quad Core 5640, 2.66 GHz or higher with 12MB L2 cache or higher, 5.86 GT/s or higher with QPI technology	
Chipset	OEM or Intel Chipset	
Memory	Minimum Memory: 32 GB DDR3 RAM	
	Maximum Memory Support: Scalable up to 192 GB per blade, however scalability upto 384 GB is preferable. Memory should support advanced memory protection features like multi-bit error correction and memory mirroring for higher reliability,	
HBA	The Blade should have dual port 8 Gbps Fiber Channel HBA.	
Ethernet Controller	2 x 10 G multifunction network ports with support for FC/iSCSI, FCoE protocols 1 Additional NIC for remote management	
Internal Storage	2 x 146GB 15K RPM HDD or more hot swappable system disk with mirroring using integrated RAID 0,1 on internal disks. It should be possible to hot swap the drives without shutting down the server.	
Ports	1 USB 2.0	
Expansion Slot	Minimum 2 nos. PCI-e based x8 Slots	
Display	VGA / Graphics Port / Controller	
OS Environment	Should support heterogeneous OS environment to run Windows 2008 Server (32 & 64 Bit), Red Hat Linux / Suse Linux / 64 Bit UNIX / Solaris x86	
Industry Standard	The server must be compliant with following international standards: PCIE 2.0 Compliant, WOL Support, Microsoft® Logo certifications, USB 2.0 Support, however ACPI 2.0. Compliant / Energy certification from any international certifying authority is preferable	
Products Certifications	Windows and Linux Certification, UL, FCC. Should be in the in the list of top 5 server brands as per IDC report published for India during year 2010.	
OEM Certifications	ISO 9001-14001, ISO 9001-2008, However Greenpeace international certification is preferable	

3) Server Specifications (Database Server):

Item	Feature Requirements	Compliance
Form Factor	4 U - Rack Mount	
Processor	Intel Xeon 6 Core 2.66GHz / 18MB L3 Cache / 5.86 GT/s with QPI technology or higher	
	Shipped with Four Nos. of Processor	
Memory	Supplied with 64 GB, Scalable up to 1 TB ECC DDR3 1333MHz	
Storage	3 Nos. of 300 GB, 2.5" 10K RPM or higher, 6Gbps SAS HDD	
Disk bays	Minimum 8 hot-swap SAS HDD	
Maximum Storage	8.0 TB through hot swap SATA / SAS HDD (Internal/External)	
Network Interface:	2 ports Gigabit Ethernet, 2 optional ports for Gigabit Ethernet	
Ports :	Rear: Two USB ports (Ver 2.0); Two RJ-45 Ethernet; keyboard and mouse; Front: Two USB (Ver 2.0)	
Graphics Controller:	Integrated Graphic Controller with external VGA port and minimum 16MB Video RAM and 1280x1024 resolution	
Power Supply:	Redundant Power supply (Hot Plug)	
HBA Card	Fiber Card for SAN: 8Gb FC Dual Port HBA Card	
RAID	SAS RAID Controller supporting RAID - 0, 1 & 5 with minimum 512MB cache for RAID operations	
Systems Management	Management feature to identify failed components even when server is switched off , Should be able to manage systems through a web-browser, Virtual media features for optional remote presence enablement, predictive failure analysis, diagnostic LEDs, light path diagnostics panel, Automatic Server Recovery, Integrated systems management process to provide system and environmental monitoring, event recording, alert capability etc.	
Industry Standard	The server must be compliant with following international standards: PCIE 2.0 Compliant, WOL Support, Microsoft® Logo certifications, USB 2.0 Support, however ACPI 2.0. Compliant / Energy certification from any international certifying authority is preferable	
Operating systems support	Microsoft Windows Server 2008 R2, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESX and ESXi 4.0, Sun Solaris for X86	
Product Certifications :	Windows and Linux Certification, UL, FCC, Should be in the in the list of top 5 server brands as per IDC report published for India during year 2010.	
OEM Certifications	ISO 9001-14001, ISO 9001-2008, However Greenpeace international certification is preferable	

4) Storage & Backup Solution

SAN Switch:

Feature Requirements	Compliance
Minimum 16 Active ports (each with minimum port speed 4 GB) within same switch upgradeable to 40 Ports or higher – Minimum 2 number of SAN switch to be provided	
All cable of length of 10 meter each and accessories for connecting Servers /Devices to SAN	
Should have capability of ISL trunking of minimum 8 ports	
Should support multiple OS	
Non-disruptive subsystem maintenance	
Should have Hot plug Fans and Hot plug power supplies switching and service modules.	
Should have web based management software for administration and configuration	
Non-disruptive microcode / firmware upgrades and hot code activation	
Switch shall support in built diagnostics, power on self-test, command level diagnostics, online and offline diagnostics.	
Should support hardware ACL based Port security, Port Zoning and LUN Zoning Should support Secure Shell (SSH) encryption to provide additional security for Telnet sessions to the switch	
Should support multilevel security on console access prevent unauthorized users from altering the switch configuration	
Should support Fiber Channel trace route and Fiber Channel Ping for ease of troubleshooting and fault isolation	
Should support the following diagnostics: ▪ Online Diagnostics ▪ Internal Loopbacks ▪ FC Debug ▪ Syslog ▪ Online system health ▪ Power on self-test (POST) diagnostics	
Should support Applications for device management and full fabric management. The management software shall be able to perform following: ▪ Fabric View ▪ Summary View ▪ Physical View ▪ Discovery and Topology Mapping ▪ Network Diagnostics ▪ Monitoring and Alerts	

Storage Area Network:

Feature Requirements	Compliance
SAN controller: Dual Active Controller	
Cache: 8 GB Total Mirrored Cache for Disk IO Operations scalable to min 16 GB	
Host interface: 4 host ports per controller, Fiber Channel (FC), 4Gbps per port	
Drive interface: 4 drive ports per controller—Fiber Channel (FC) Switched or FC Arbitrated Loop(FC-AL) standard per controller, 4 Gbps per port	
RAID levels Supported: 0, 1, 5 / 6	
Fans and power supplies: Dual redundant, hot-swappable	
SAN support: Box should be compatible of SAN environment	
The storage array shall be configured with at least 8 GB cache scalable to min 16 GB mirrored across two storage controllers for disk I/O operations	
Storage subsystem shall support 146GB/300GB/ 400GB/600GB or higher with 10K RPM or higher Fiber channel/SAS drives & 750GB/1TB or higher FATA/SATA or equivalent drives in the same device array	
Presently, the storage sub system shall be configured with 400/600 GB or Higher Performance drives on Fiber channel/SAS and 750 GB/1TB or higher on FATA/SATA or equivalent for archiving purpose	
The storage system must provide upgrade path to larger or future array controller and software technology while maintaining the existing investment	
The storage array proposed should have an upgrade path from the earlier generation product to the current generation product	
All the necessary software to configure and manage the storage space, RAID configuration, logical drives allocation, virtualization, snapshots (including snap clones and snap mirrors) for entire capacity etc	
Redundant power supplies, batteries and cooling fans and data path and storage	

controller	
Load balancing must be controlled by system management software tools	
The multi-path software should not only support the supplied storage and operating systems but should also support heterogeneous storage and operating systems from different OEMs	
The storage array must have complete cache protection mechanism either by de-staging data or providing complete cache data protection with battery backup for up to 72 hours or more	
The storage system should be supplied with minimum 30TB usable space and should be scalable up to 80TB usable space. The Storage should have at least 2 ports of 4 Gbps Frontend ports and 2 no's of back end ports of 4Gbps"The storage array must have the capability to do array based remote replication using FCIP or IP technology	
The storage array should support block level Synchronous and Asynchronous replication across storage arrays of the same family however heterogeneous support is preferable.	
The storage array should support Operating System Platforms & Clustering including: Windows Server 2003 (Enterprise Edition), Sun Solaris, HP-UX, IBM-AIX, Linux / Solaris for x86	
Storage should support non-disruptive online firmware upgrade for both Controllers and disk drives	
The storage array should support hardware based data replication at the Block level across all models of the offered family	
The storage should provide automatic rerouting of I/O traffic from the host in case of primary path failure	
Should provision for LUN masking, fiber zoning and SAN security	
Should support storage virtualization, i.e. Easy logical drive expansion	
Should support hot-swappable physical drive raid array expansion with the addition of extra hard disks	
Should be able to support clustered and individual servers at the same time	
Should be able to take "snapshots" of the stored data to another logical drive on a different Disk/RAID Group for backup purposes	

Should be configured with "snapshots and clone"	
SI should also offer storage performance monitoring and management software	
The SI must provide the functionality of proactive monitoring of Disk drive and Storage system for all possible hard or soft disk failure	

5) Tape Library:

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

Backup Software:

Feature Requirements	Compliance
The proposed Backup Solution should be available on various OS platforms such as Windows and UNIX platforms and be capable of supporting SAN based backup / restore from various platforms including UNIX, Linux, and Windows etc.	
Centralized, web-based administration with a single view of all back up servers within the enterprise. Single console must be able to manage de-duplicated and traditional backups	
The proposed backup solution should allow creating tape clone facility after the backup process	

The proposed Backup Solution has in-built frequency and calendar based scheduling system	
The proposed backup Solution supports the capability to write multiple data streams to a single tape device or multiple tape devices in parallel from multiple clients to leverage the throughput of the Drives using Multiplexing technology	
The proposed backup solution support de-multiplexing of data cartridge to another set of cartridge for selective set of data for faster restores operation to client/servers	
The proposed backup solution should be capable of taking back up of SAN environment as well as LAN based backup	
The proposed backup solution shall be offered with appropriate License for SAN based backup and LAN based backup for at least 50 servers, which supports Windows/Linux/Unix OS as per requirements.	
The proposed solution also supports advanced Disk staging	
The proposed Backup Solution has in-built media management and supports cross platform Device & Media sharing in SAN environment. It provides a centralized scratched pool thus ensuring backups never fail for media	
Backup Software is able to rebuild the Backup Database/Catalog from tapes in the event of catalog loss/corruption	
The proposed Backup Software should offer online backup for the Operating Systems offered in the solution stack	
The proposed Backup Solution has online backup solution for different type of Databases such as Oracle, MS SQL, and Sybase / DB2 etc. on various OS	
The Proposed backup solution shall provide granularity of single file restore	
The Proposed backup solution shall be designed in such a fashion so that every client / server in a SAN can share the robotic tape library	
Backup Solution shall be able to copy data across firewall	
The backup software must also be capable of reorganizing the data onto tapes within the library by migrating data from one set of tapes into another, so that the space available is utilized to the maximum. The software must be capable of setting this utilization threshold for tapes	
The backup software should be able to support versioning and should be applicable to individual backed up object's	
Should have the ability to retroactively update changes to data management policies that will then be applied to the data that is already being backed up or archived	
All software licenses should be in the name of MP Police and should be a perpetual license, i.e. the software license should not expire after the contract period. The software Licenses should be comprehensive and no further licenses should be required for DC/DR operations. The software installed should necessarily be the latest version at the time of actual implementation.	

6) Multilayered Core Layer 3 Switches:

Feature Requirements	Compliance
General Features	
Standard 19" Rack mountable switch	
Redundant Power Supply (RPS)	
Switching Capacity – 160 Gbps or above	
DRAM Minimum 256 MB, Flash Minimum – 64 MB	
Forwarding Rate – 100 Mpps or higher	
LAN Ports - 48 x 10/100/1000BaseTports	
Combo Ports - 2 or higher SFP and additional 4 x 10G ports (or more)	
Console Port	
Stackability	
Virtual Stacking should Support Single IP Management(SIM) up to 16 or higher devices	
Physical stacking should support stacking 9 or above units per stack which provide bidirectional redundant stacking topology with 40 G (full duplex) or above Bandwidth	
Allows trunking or mirroring to span multiple units of the stack	
L2 Features	
12K or above MAC Address Table and support 256 static MAC, however 16K MAC address table preferable	
IGMP snooping v1,v2,v3	
802.1D STP, 802.1w RSTP and 802.1s MSTP	
Per device and Per port BPDU filtering	
Loopback Detection (LBD)	
Port Mirroring - Supports One-to-one, Many-to-one and flow based mirroring	
Link Aggregation (802.3ad) with 26 groups or higher per device, max Eight Gigabit or Two 10G ports per group	

GVRP and STP or equivalent for L2 Protocol Tunneling	
VLAN	
802.1Q Tagged VLAN	
4K static and 255 dynamic VLAN groups	
Double VLAN (Q in Q)	
MAC-based VLAN with 1000 or higher entries	
L3 Features	
VRRP or equivalent	
IPv6	
ARP Proxy, Gratuitous ARP	
L3 Routing	
Support Static Route, RIP v1/V2, OSPF v3 and all IPv6 Protocols	
IPv4/IPv6 Routing Table Size - 12K	
Policy Based Route - Based on ACL	
L3 Multicasting	
IGMP v1/v2/v3, DVMRP v3 / PIM DM and PIM SM or equivalent / better	
QoS (Quality of Service)	
802.1p Class of Service (CoS)	
Number of Queues – 8	
Queue handling mode - Strict and Weighted Round Robin(WRR)	
CoS based on - Switch port, VLAN ID, 802.1p priority queues, MAC address, IP address, DSCP, Protocol type, TCP/UDP port number, IPv6 Traffic Class, IPv6 Flow Label, User-defined Packet Content	
Port and Flow based bandwidth control (Ingress/Egress, minimum granularity 64Kbps)	
ACL(Access Control List)	
ACL based on - 802.1p priority, VLAN ID, MAC address, Ether type, IP address, DSCP, Protocol type, TCP/UDP port number, IPv6 Traffic Class, IPv6 flow label, User defined packet content	

CPU interface filtering or equivalent	
Time-Based ACL	
Security	
SSH, SSL	
Should support Port Security feature	
Broadcast/Multicast/Unicast Storm Control - Allow specifying the threshold in terms of packet/s for per port	
Traffic Segmentation	
Safeguard Engine or equivalent / better	
IP-MAC-Port Binding and DHCP snooping to dynamically collect IP-Mac-Port info	
AAA	
802.1X - Port-based and MAC-based Access Control	
Microsoft NAP function via 802.1X guest VLAN	
Guest VLAN with 802.1X authentication method	
RADIUS and TACACS+ Authentication for Management Access	
Database failover-When RADIUS server fails, switch to local database for authentication	
Management	
Web-based GUI, Command Line Interface	
Telnet Server, TFTP Client	
SNMP v1/v2c/v3	
RMON v1 / v2 /equivalent	
sFlow	
RSPAN	
DHCP Server, DHCP relay - Support DHCP relay option 82	
CPU Monitoring - Allow monitoring the utilization of CPU via Web/ CLI/ SNMP	
802.3ah	

Cable Diagnostic	
Physical & Environment	
AC input - 100-240 VAC, 50/60Hz, Internal universal power supply	
Emission (EMI) and Safety Certifications:	
EMI-EMC Compliance :- FCC Class C288A/ICES-003, Class A(FCC Part 15B), CE Class A(EN55022/24), C-Tick Class A (CISPR-22) , VCCI Class A(CISPR-22)	
Safety Compliance :- cUL, CB	
Immunity :- FCC, CE certification	

7) Internet & WAN Router:

Feature Requirements	**Compliance**
Hardware Architecture: Router should be mountable on 19" Rack	
Modular chassis	
Power supply 230 V AC	
Interface: 4 x 10/100/1000 MBPS Fast Ethernet Port	
2 x Open slots for Network Modules	
1 x Console port, 2 x External USB 2.0 High speed Port	
1 x Auxiliary port	
Memory: DDR 2 ECC DRAM - Minimum – 1 GB, however 2 GB expandability is preferable	
Inbuilt / Flash Memory - 256MB, upgradeable to 1GB or more	
Security: GRE and IP Sec 3DES/AES VPN for configuration of VPN tunnels.	
Encryption - IP Sec 3DES/AES	
NAT, PAT	
Access control - Multilevel	
Controlled SNMP Access using ACL on router to ensure SNMP access only	

Feature Requirements	Compliance
to identified NMS/EMS	
Controlled SNMP access through the use of SNMP with MD5 authentication.	
Multiple Privilege Levels for managing & monitoring	
Support for RMON 1 / 2 or equivalent groups as and when required	
Support for Remote Authentication User Service (RADIUS) and AAA	
PPP CHAP support. PAP (optional)	
Firewall protection along with VLAN	
Routing Protocols - RIPv1, RIPv2, OSPF V1 and v2, BGP4, VRRP / HSRP, HDLC Static Routes	
Route redistribution between any of the above protocols	
Protocols: PPP, Multi-link PPP	
Frame Relay	
IPv4 and IPv6 ready	
IP Accounting	
Packet & Byte Counts	
Start & End Time Stamp	
Input & Output interface ports.	
Type of service, TCP Flags & Protocol	
Source & Destination IP addresses	
Source & Destination TCP/UDP ports	
Management: Accessibility using Telnet, SSH, Console access.	
Easier Software upgrades through network, using FTP,TFTP, etc.	
SNMPv1, snmpv2/v3	
Configuration management through CLI.	
Event and system history logging functions shall be available.	

Feature Requirements	Compliance
Support for Syslog Server required	
QoS, FIFO, PQ, CQ, CBWFQ, WFQ, RED, WRED, DSCP, IP Precedence, RTS, RSVP,	
All necessary power cords, adapters, data cables, connectors, CDs, manuals, brackets accessories, wire managers, etc. should be provided	

8) 42U Rack:

19" 42U racks shall be used in the Data Centre for hosting the department applications of Police department of Madhya Pradesh. All the racks should be mounted on the floor with castor wheels with brakes (set of 4 per rack).

Feature Requirements	Compliance
19" Floor Standing Rack 42U (600 X 1000)	
Mounting accessories for required servers / equipment	
Cable Manager Horizontal - 4 No.	
Cable Manager Vertical 42 U – 2 Front & 2 Rear	
4 Fans with Fan tray and Safety Grill	
Power Distribution Box 6 (5 & 15 Amp) Socket Horizontal with surge protection -1 No.	
Power Distribution Box (5 & 15 Amp) Twelve Socket Vertical with surge protection - 2 No.	
Copper Earthing Strip	

9) UTP & Structured Cabling:

The cabling material shall be supplied, laid tested and commissioned in accordance with specifications and site requirements.

All the cabling shall run through PVC conduit / Casing Capping of suitable size of ISI standard. Separate PVC conduits or Casing Capping shall be used for electrical and data cabling.

Laying of Cables- Cables shall be laid by skilled and experienced workmen using adequate equipments to minimize stretching of the cable.

All terminations should be carried out according to the manufacturer's instructions and guidelines and standards of generic cabling systems. When terminating outlets, care must be taken to avoid damaging the copper cores when stripping back the outer sheathing.

Testing and Documentation: Testing of each node should be done as per manufacturer standards and the final report should be submitted.

UTP COMPONENTS: SI must make sure that the system should Meet or exceed TIA/EIA 568 B-2 specifications of Category-6 as a system. All performance parameters -Attenuation, Pair -to-Pair and power sum NEXT, Pair And Power sum ELFEXT, Return Loss and Delay skew should be tested for 100m Channel as well as 90m permanent Link. It should be a single OEM solution and should ensure optimum system performance. There should not be any Impedance mismatch problems among components of the cabling system. The complete system should be tested up to 600 MHz for all the test parameters to ensure the end-to-end system performance.

Specification:

Type	Details	Compliance (Yes/No)
Type	Unshielded Twisted Pair, Category 6, ANSI/TIA/EIA 568-B.2.1	
Conductors	24 AWG solid bare copper	
Insulation	Polyethylene/Polyolefin	
Jacket	Flame Retardant PVC	
Approvals	UL Listed	
	ETL verified to ANSI/TIA/EIA 568-B.2.1 Cat 6	
Operating temperature	-20 Deg. C up to +60 Deg. C	
Frequency tested up to	600 MHz	
Delay Skew	25ns-45ns / 100m MAX.	
Impedance	100 Ohms + / - 6 ohms	

10) Cat-6 Patch Cord (1-Meter)

Scope:

Scope of 1 meter Patch cord is to get connectivity between patch panels to switch. System Integrator has to provide proper connectivity via Cat-6 Patch Cord (1 Meter) and must make sure it will be proper dressed in rack and function properly.

Specification:

Type	Details	Compliance (Yes/No)
Length	3 Feet	
Conductor	24 AWG 7 / 32, stranded copper	
Cable Type	UTP CAT 6 ANSI/TIA/EIA 568-B.2.1	
Plug Protection	Matching colored boot to maintain bend radius	
Warranty	20-year component warranty	
Category	Category 6	
Terminals	Phosphor Bronze with gold plating	
Jacket	PVC	
Insulation	Flame Retardant	

11) Cat - 6 Patch Cord (2 Meters Length)

Scope:

Scope of 2 meters Patch cord is to get connectivity between IO to desktop/Printers. System Integrator has to provide proper connectivity via Cat-6 Patch Cord (2 Meters) and must make sure it will function without any interruption.

Specification:

Type	Details	Compliance (Yes/No)
Length	7 Feet	
Conductor	24 AWG 7 / 32, stranded copper	
Cable Type	UTP CAT 6 ANSI/TIA/EIA 568-B.2.1	

Plug Protection	Matching colored boot to maintain bend radius	
Warranty	20-year component warranty	
Category	Category 6	
Terminals	Phosphor Bronze with gold plating	
Jacket	PVC	
Insulation	Flame Retardant	

12) Firewall with VPN & IPS:

Feature Requirements	Compliance
The firewall should be an hardware appliance based unit	
UTM Firewall with Unrestricted users	
The unit should have minimum 1 GB or higher memory	
Firewall stateful throughput should be more than 5 GBPS	
Gateway Antivirus throughput should be more than 1 GBPS	
IPS throughput should be more than 2 GBPS	
VPN throughput should be more than 2 GBPS	
Unified Threat Management throughput should be more than 1 GBPS	
UTM should support minimum 20000 new Connections per second	
UTM should support more than 1500 site-to-site VPN Tunnels and more than 5000 VPN Client, Should be supplied with minimum 2000 bundled VPN Clients	
UTM Should support Active/Passive with State Synch and Active/Active UTM in HA Mode	
The UTM should have 8 Copper Gigabit Network Interface Ports, 1 Console Interface, 2 USB ports	
Should have LED's indicating Status (Power, Test, Alarm) LAN (Link, Activity) WAN (Link, Activity) DMZ (Link, Activity)	

Feature Requirements	Compliance
Unit should have minimum 16 Core Processor with specialized security processing	
It should not consist of any failure devices such as Hard Disk	
Should have additional Cryptographic Accelerator Processor offloading VPN computation from Main Processor	
Should have a Multi-Layered Protection Technology	
Should have upgradeable Firmware	
Should Have a Re-Assembly Free Deep Packet Inspection or equivalent feature	
Should have a stateful throughput of 1 Gbps or higher Bi-directional for Firewall	
Gateway Antivirus should be able to scan the 50+ Protocols including HTTP, FTP, SMTP, POP3 and IMAP,	
Should support the following and Standard protocols TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS	
Should have an integrated Intrusion Prevention System	
Should be able to Scan encrypted traffic and payload for any virus threats	
Should be able to provide Content Filtering services without the use of other software with more than 8 million site categorized	
Should support routing functionality like RIP and OSFP	
Should be able to add policy based routes on the appliance	
Should have no file size limitation for GAV/IPS scanning	
Should support Site-to-Site Auto Provisioning VPN	
Should support IKEv2 Secondary Gateway, IKEv2 Dynamic Client Support	
Should have Application Firewall for application Bandwidth Control, Access Control, Regulation of web traffic, email, email attachments and file transfers, scanning of files and documents for keywords and specified content, creation of custom IDS/IPS signatures	
Should support Single Sign-On for user authentication	
Should Inbound Load Balancing for redundancy or load balancing for multiple server applications or devices	

Feature Requirements	Compliance
Should support HTTPS Content Filtering	
Should support SSL Control for policies to control the establishment of SSL connections	
Should support Services Dashboard for global and local statistics of blocked network threats	
Should support Packet Capture to capture and examine the contents of individual data packets that traverse the firewall appliance for troubleshooting, diagnostics and general network activity, decreasing the time it take to investigate potential issues	
Should support Hardware Failover with State sync	
Should support Network Address Translation (NAT) over Virtual Private Network (VPN)	
Should support Clean Virtual Private Network (VPN) technology	
Should support 25000+ signature in the Gateway Antivirus (GAV)	
Should support Network Antivirus (NAV) from the hardware appliance	
Should support Address Resolution Protocol (ARP) binding functionality	
Should support Zone Security	
Should support object Based Management	
Should support SPAM blocking	
Should support VOIP protocol both SIP and H.323	
Should support policy based Network Address Translation (NAT)	
Should support WAN to WAN failover	
Should support Internet Service Provider (ISP) failover	
Should support Load Balancing in Round Robin and in accordance with Bandwidth & percentage	
Should support Hardware Failover / High Availability	
Should have Console based and Browser based management facility.	
The data transfer between the Management station and Firewall appliance should be encrypted.	

Feature Requirements	Compliance
The appliance would be IPv6 Ready	
Should support firewall modes like Nat mode, Bridge mode and transparent mode	
Should be able to log any traffic and activity on the unit	
Should be able to divert Logs on to log server and third party software integration should be possible.	
Should be able to generate reports with statistic such as User login, IP address, Intrusion, URL, Virus attacks etc.	

13) Software for Data Center & DR Center

Operating System and Database for Server

CAS (State) will be developed in two distinct technology stacks by the Software Development Agency at the Center. The details of the Technology Stacks are provided as **Annexure II Details of technology stack-CAS (Center) and CAS (State)** to this RFP. The SI is expected to bid with one of the technology stacks in response to this RFP. SI shall procure all necessary required software for DC & DR including Operating System, Database, and Other Software Licenses. All software licenses should be in the name of MP Police and should be a perpetual license, i.e. the software license should not expire after the contract period. The software Licenses should be comprehensive and no further licenses should be required for DC and DR operations. The software installed should necessarily be the latest version at the time of actual implementation. The SI shall procure all necessary updates /patches / bug fixes for this software during the project cycle. The SI will also implement the same from time to time as required after necessary approvals from MP Police / MPCOPS. Tuning of application, databases, third party software's, and any other components provided as part of the solution to optimize the performance will be the responsibility of SI. The SI shall also apply regular patches to the licensed software including the operating system and databases as released by the OEMs.

The SI shall also provide services for software license management and control. SI shall maintain data regarding entitlement for software updates, 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 MP Police / MPCOPS.

All the software licenses should be in the name of DGP, MP Police, Bhopal.

All Operating system, database and other software licenses for DC and DR shall be genuine, perpetual, full use and should provide patches, bug fixes, security patches and updates directly from the respective developer / manufacturer for the contract period. The CAS application will be

implemented at 1420 police locations from where various departmental users will access the Core Application Software on approximately 5000 desktop computers.

The software product used should have well defined product roadmap by the respective developer / manufacturer.

The proposed system software must provide indemnification and indemnification must cover patent claims, copy right claims, legal fees and damages claim. System integrator and /or developer/ manufacturer must protect the department from all such legal cost that may arise out of any claim by a third party alleging intellectual property infringement i.e. related to the software.

Bidder shall provide a comprehensive warranty that covers all components after the issuance of the final acceptance test of department. The warranty should cover all materials, licenses, services and support for both hardware and software. Bidder shall administer warranties with serial number of equipment during warranty period. Upon final acceptance of the MP Police / MPCOPS any manufacturer warranties will be transferred to the MP Police / MPCOPS at no additional charge. All warranty documentation (whether expired or not) will be delivered to MP Police / MPCOPS at the issuance of final acceptance certificate.

The bidder shall provide with a full use of database license during the project period for unrestricted users. Database should have received the security certification such as International common criteria for information technology security evaluation. Database should be quoted as per the CAS Stack Selected. The database software should provide the following capabilities:

a) Advance web based reporting
b) Data warehouse and analysis service
c) Complete ETL functionality
d) High Availability / Clustering Services
e) Tuning and Diagnostic Tools
f) Spatial Database capability
g) Database compression & encryption tools
h) Replication Technologies for Failover to Remote Site
i) High availability option without shared Disk / SAN

Note: System Integrator should quote the Database as per CAS Stack Selection.

Antivirus Software for Server and Desktop:

Feature Requirements	Compliance
Unified protection - from viruses, spyware, and other current integrated through one client agent	
Simplified administration - through central management to protect the infrastructure with greater efficiency	
Visibility and control - through insightful, prioritized security reports and a summary dashboard view, which enable administrator for visibility and control over malware threats	
Infrastructure Integration Capabilities 1. All Data must be stored Centrally in proposed Database Server and Reporting should be provided	
Malware Filtering Capabilities 1. Should support Integrated anti-virus/anti-spyware agent delivering real-time protection 2. Should support Static analysis and code emulation for addressing threats 3. Should support Event Flood Protection 4. Should support Integrated and Single foot printed State Assessment Scans to detect Vulnerabilities 5. Should support In-depth scanning of unknown malware by Dynamic Translation	
Manageability 1. The Solution Should support Centralized Monitoring of the integrated anti-malware engine, security state assessment technologies and policies alerts, and reports 2. Should support in-built Reporting for Below Items : a. Deployment Status: Number of machines up to date or not up to date with the latest signatures b. Top issues and issue history: Information about the top issues in their environment categorized by type along with the history of issues over time c. Top Threats and threat history: List of top threats, their severity and number of machines impacted. Should provide info on current status and trends d. Top vulnerabilities and vulnerability history: Through security state assessment checks, admin should be able to see the top vulnerabilities as well as history of vulnerabilities over time. The admin should also be alert to measure the security risk profile based on security best practices e. Top alerts and alert history: Should support Information about the key alerts impacting their environment (with the ability to drill down into more information), along with the history of alerts over time 3. It should be capable of providing customized alerts based on incidents and assets	

Email Security Software:

Email Security should contain the highest possible level of network protection from all inbound and outbound e-mail threats by leveraging a global end-to-end attack monitoring network. Center is providing **Q-Mail community based email solutions** to MPCOPS / MP Police for which Email Security system is required. The email security protection should include:

Feature Requirements	Compliance
Anti-spam with auto update feature	
Anti-phishing with auto update feature	
Anti-virus with auto update feature	
Policy management including Policy Rules for Users, Groups or All Users	
Connection management	
Compliance & content filtering	
Quick configuration with Streamlined interface	
Seamless LDAP / active directory integration	
Administrative quarantine	
Robust reporting	
Inbound and outbound e-mail management in the same system	
Unlimited domain support	
Allow / Deny All End-User Controls	
Per User Junk Boxes	
Single Sign-on	
Secure & Hardened OS with hardware Appliance	
19” Rack mount with Intel based minimum 2 GHz CPU, 2 GB RAM, 250 GB HDD	
Should support Clustering & Remote Clustering	

Enterprise management & Monitoring Solution (EMS):

ITEM	Compliance (Y/ N)
Basic Requirements: Solution should be inclusive with hardware, OS, patches, etc. ▪ Solution should provide for future scalability of the whole system without major architectural changes. ▪ Should be SNMP compliant. ▪ Filtering of events should be possible, with advance sort option based on components, type of message, time etc. ▪ Should support Web / Administration Interface. ▪ Should provide compatibility to standard RDBMS. ▪ Solution should be open, distributed, and scalable and open to third party integration. ▪ Should provide fault and performance management for multi-vendor TCP/IP networks.	
Security: ▪ Should be able to provide secured windows based consoles / secured web based consoles for accessibility to EMS. ▪ Should have web browser interface with user name and Password Authentication. ▪ Administrator/ Manager should have privilege to create/modify/delete user.	
Polling Cycle: ▪ Support discriminated polling ▪ Should be able to update device configuration changes such as re-indexing of ports	
Fault Management: ▪ Should be able to get fault information in real time and present the same in alarm window with description, affected component, time stamp etc. ▪ Should be able to get fault information from heterogeneous devices- routers, switches, servers etc. ▪ Event related to servers should go to a common enterprise event console where a set of automated tasks can be defined based on the policy. ▪ Should have ability to correlate events across the entire infrastructure components of DC and DR. ▪ Should support automatic event correlation in order to reduce events occurring in DC and DR. ▪ Should support advanced filtering to eliminate extraneous data / alarms in	

ITEM	Compliance (Y/ N)
Web browser and GUI. ▪ Should be configurable to suppress events for key systems/devices that are down for routine maintenance or planned outage. ▪ Should be able to monitor on user-defined thresholds for warning/ critical states and escalate events to event console of enterprise management system. ▪ Should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. ▪ Should have self-certification capabilities so that it can easily add support for new traps and automatically generate alarms. ▪ Should provide sufficient reports pertaining to asset and change management, alarms and availability of critical network resources as well as network response times for critical links. ▪ The tool shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network and system components. The current performance state of the entire network and system infrastructure shall be visible in an integrated console. ▪ Should provide an integrated event view for all the managed systems and networks along with the various threshold violations alarms in them. It should be possible to drill down into the performance and event views to execute context specific reports ▪ Should provide a variety of reports for troubleshooting, diagnosis, analysis and resolution purposes such as Trend reports, At-A-Glance reports, etc. It should also provide the capability to additional user-defined reports and customize existing reports. ▪ The system should allow defining baselines formulae for different set of infrastructure. It should allow user to define upper and lower threshold limits in a way wherein it almost burst threshold definition, duration threshold, and combination.	
Discovery: ▪ Should provide accurate discovery of layer 3 and heterogeneous layer 2 switched networks for Ethernet, LAN, and Servers etc. ▪ Manual discovery can be done for identified network segment, single, or multiple devices.	
Presentation: ▪ Should be able to discover links with proper color status propagation for complete network visualization. ▪ Should support dynamic object collections and auto discovery. The topology of the entire Network should be available in a single map.	

ITEM	Compliance (Y/ N)
▪ Should give user option to create his /or her map based on certain group of devices or region.	
Agents: ▪ Should monitor various operating system parameters such as processors, memory, files, processes, file systems etc. where applicable using agents on the servers to be monitored. ▪ Provide performance threshold configuration for all the agents to be done from a central GUI based console that provide a common look and feel across various platforms in the enterprise. These agents could then dynamically reconfigure them to use these threshold profiles they receive.	
System Monitoring: • Should be able to monitor/manage large heterogeneous systems environment continuously. Should monitor / manage following (based on Stack): ▪ Event log monitoring. ▪ Virtual and physical memory statistics ▪ Paging and swap statistics ▪ Operating system ▪ Memory ▪ Logical disk ▪ Physical disk ▪ Process ▪ Processor ▪ Paging file ▪ IP statistics ▪ ICMP statistics ▪ Network interface traffic ▪ Cache ▪ Active Directory / LDAP Services Should monitor following with statistics : ▪ CPU Utilization, CPU Load Averages ▪ System virtual memory (includes swapping and paging) ▪ Disk Usage ▪ No. of Nodes in each file system ▪ Network interface traffic ▪ Critical System log integration	
Infrastructure Services: ▪ IIS / Tomcat / Apache / Web server statistics ▪ HTTP service ▪ HTTPS service ▪ FTP server statistics ▪ POP/ SMTP Services ▪ ICMP services ▪ Database Services – Monitor various critical relational database management system (RDBMS) parameters such as database tables / table	

ITEM	Compliance (Y/ N)
spaces, logs etc.	
Application Performance Management: ▪ End to end Management of applications (J2EE/.NET based) ▪ Determination of the root cause of performance issues whether inside the Java / .Net application in connected back-end systems or at the network layer. ▪ Automatic discovery and monitoring of the web application environment ▪ Ability to monitor applications with a dashboard. ▪ Ability to expose performance of individual SQL statements within problem transactions. ▪ Monitoring of third-party applications without any source code change requirements. ▪ Proactive monitoring of all end user transactions; detecting failed transactions; gathering evidence necessary for problem diagnose. ▪ Storage of historical data is for problem diagnosis, trend analysis etc. ▪ Monitoring of application performance based on transaction type. ▪ Ability to identify the potential cause of memory leaks. **(Note: Application Security is not considered at EMS Level)**	
Reporting: ▪ Should able to generate reports on predefined / customized hours. ▪ Should be able to present the reports through web and also generate “pdf” / CSV / reports of the same. ▪ Should provide user flexibility to create his /or her custom reports on the basis of time duration, group of elements, custom elements etc. ▪ Should provide information regarding interface utilization and error statistics for physical and logical links. ▪ Should create historical performance and trend analysis for capacity planning. ▪ Should be capable to send the reports through e-mail to pre-defined user with pre-defined interval. ▪ Should have capability to exclude the planned-downtimes or downtime outside SLA. ▪ Should be able to generate variety of SLA Reports.	

ITEM	Compliance (Y/ N)
▪ Should be able to generate web-based reports, historical data for the systems and network devices and Near Real Time reports on the local management console. ▪ Should be able to generate the reports for Server, Application, infrastructure services, and Network devices in DC and DR environment.	
Availability Reports: ▪ Availability and Uptime – Daily, Weekly, Monthly and Yearly Basis ▪ Trend Report ▪ Custom report ▪ MTBF and MTTR reports	
Performance Reports: ▪ Device Performance – CPU and Memory utilized ▪ Interface errors ▪ Server and Infrastructure service statistics ▪ Trend report based on Historical Information ▪ Custom report ▪ SLA Reporting ▪ Computation of SLA for entire DC and DR Infrastructure ▪ Automated Daily, Weekly, Monthly, Quarterly and Yearly SLA reports.	
Data collection: ▪ For reporting, required RDBMS to be provided with all licenses. ▪ Should have sufficient Storage capacity should to support all reporting data	
Integration: ▪ Should be able to receive and process SNMP traps from infrastructure components such as router, switch, servers etc. ▪ Should be able integrate with Helpdesk system for incidents. ▪ Should be able to send e-mail or Mobile –SMS to pre-defined users for predefined faults. ▪ Should trigger automated actions based on incoming events / traps. These actions can be automated scripts/batch files.	
Network Management: ▪ The Network Management function must monitor performance across heterogeneous networks from one end of the enterprise to the other. ▪ It should proactively analyze problems to improve network performance. ▪ The Network Management function should create a graphical display of all discovered resources. ▪ The Network Management function should have extensive reporting facility, providing the ability to format and present data in a graphical and tabular display. ▪ The Network Management function should collect and analyze the data. Once collected, it should automatically store data gathered by the NMS	

ITEM	Compliance (Y/ N)
system in a database. This enterprise-wide data should be easily accessed from a central location and used to help with capacity planning, reporting, and analysis. ▪ The Network Management function should also provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment, WAN links and routers. ▪ Alerts should be shown on the Event Management map when thresholds are exceeded and should subsequently be able to inform Network Operations Center (NOC) and notify concerned authority using different methods such as pagers, emails, etc. ▪ It should be able to automatically generate a notification in the event of a link failure to ensure proper handling of link related issues. ▪ The Systems and Distributed Monitoring (Operating Systems) of EMS should be able to monitor: ➢ Processors: Each processor in the system should be monitored for CPU utilization. Current utilization should be compared against user-specified warning and critical thresholds. ➢ File Systems: Each file system should be monitored for the amount of file system space used, which is compared to user-defined warning and critical thresholds. ➢ Log Files: Logs should be monitored to detect faults in the operating system, the communication subsystem and in applications. The function should also analyze the files residing on the host for specified string patterns. ➢ System Processes: The System Management function should provide real-time collection of data from all system processes. This should identify whether or not an important process has stopped unexpectedly. Critical processes should be automatically restarted using the System Management function. ➢ Memory: The System Management function should monitor memory utilization and available swap space. ➢ Event Log: User-defined events in the security, system, and application event logs must be monitored.	
SLA Monitoring: ▪ The SLA Monitoring function of the EMS is by far the most important requirement of the DC/DR Project. The SLA Monitoring component of EMS will have to possess the following capabilities: ➢ EMS should integrate with the application software component of portal software that measures performance of system against the following SLA parameters:	

ITEM	Compliance (Y/ N)
• Response times of Portal; • Uptime of data center; • Meantime for restoration of Data Centre etc. ➢ EMS should compile the performance statistics from all the IT systems involved and compute the average of the parameters over a quarter, and compare it with the SLA metrics laid down in the RFP. ➢ The EMS should provide details of **uptime/downtime/availability** report details based on which penalties can be calculated. ➢ The SLA monitoring component of the EMS should be under the control of the authority that is nominated to the mutual agreement of Director, the partner so as to ensure that it is in a trusted environment. ➢ The SLA monitoring component of the EMS should be subject to random third party audit to vouchsafe its accuracy, reliability, and integrity.	
Reporting: ▪ The Reporting and Analysis tool should provide a ready-to-use view into the wealth of data gathered by Management system and service management tools. It should help generating variety of reports and the relevant information easily accessible to business pertaining to servers/ network devices being monitored. This information, should be presented in a variety of graphical formats can be viewed interactively. ▪ The tool should allow customers to explore the real-time data in a variety of methods and patterns and then produce reports to analyze the associated business and service affecting issues. ▪ The presentation of reports should be in an easy to analyze graphical form enabling the administrator to put up easily summarized reports to the management for quick action (Customizable Reports). The software should be capable of supporting the needs to custom make some of the reports as per the needs of the organization. ▪ Provide Historical Data Analysis: The software should be able to provide a time snapshot of the required information as well as the period analysis of the same in order to help in projecting the demand for bandwidth in the future.	
ITIL based Helpdesk System: ▪ Helpdesk system would automatically generate the incident tickets and log the call. Such calls are forwarded to the desired system support personnel deputed by the Implementation Agency. These personnel would look into the problem, diagnose and isolate such faults and resolve the issues timely. The helpdesk system would be having necessary workflow for transparent, smoother and cordial DC and DR support framework. ▪ The Helpdesk system should provide flexibility of logging incident manually via windows GUI and web interface. ▪ The web interface console of the incident tracking system would allow viewing, updating, and closing of incident tickets.	

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

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