E-GOVERNANCE

MISSION MODE PROJECT (MMP)

Crime and Criminal Tracking Network & Systems (CCTNS)

Request for Proposal

For Selection of System Integrator

For

Implementation, Commissioning and Maintenance of CCTNS

VOLUME – I :

FUNCTIONAL AND TECHNICAL SPECIFICATIONS

Released By :

MANIPUR POLICE

Manipur Police,

Government of Manipur

TABLE OF CONTENTS

LIST OF ANNEXURES

LIST OF ABBREVIATIONS

AFIS	Automated Fingerprint Identification System
AT	Acceptance Testing
ATMO	Assistant Technical Maintenance Officer
BOM	Bill of Material
BPR	Business Process Reengineering
CAS	Core Application Software
CBI	Central Bureau of Investigation
CC	Court Constable
CCIS	Crime and Criminals Information System
CCTNS	Crime & Criminal Tracking Network and Systems
CID	Criminal Investigation Department
CIPA	Common Integrated Police Application
CPMU	Central Program Management Unit
CrPC	Criminal Procedure Code
DCRB	District Crime Record Bureau
DGP	Director General of Police
DIG	Deputy Inspector General of Police
DRC	Disaster Recovery Centre
DY.SP	Deputy Superintendent of Police
EMD	Earnest Money Deposit
EMS	Enterprise Management System
FIR	First Information Report
FRS	Functional Requirement Specifications

FPB	Finger Print Bureau
FSL	Forensic Laboratory
GIS	Geographical Information System
GPS	Global Positioning System
GRP	Government Railway Police
HLD	High Level Design
IGP	Inspector General of Police
IIF	Integrated Investigation Forms
IO	Investigation Officer
IPC	Indian Penal Code
LAN	Local Area Network
LIMS	Lawful Interception Monitoring System
LLD	Low Level Design
MHA	Ministry of Home Affairs
MIS	Management Information System
MPLS	MultiProtocol Label Switching
MPR	Manipur Police Radio
NCR	Non-Cognizable Report
NCRB	National Crime Record Bureau
NeGP	National e-Governance Plan
NIC	National Informatics Centre
PCR	Police Control Room
PHQ	Police Headquarters
RFP	Request for Proposal
SAN	Storage Area Network
SCRB	State Crime Record Bureau

SDA	Software Development Agency
SDC	State Data Centre
SDPO	Sub-Division Police Office
SHO	Station House Officer
SI	System Integrator
SLA	Service Level Agreement
SOA	Service Oriented Architecture
SP	Superintendent of Police
SPMC	State Project Management Consultants
SPMU	State Program Management Unit
SRS	Software Requirement Specifications
SWAN	State Wide Area Network
VPN	Virtual Private Network
XML	Extensible Markup Language

GLOSSARY OF TERMS

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

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

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

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

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

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

• **"Successful Implementation / Go-Live"** will mean:
Successful deployment, commissioning and UAT of the CCTNS application modules implemented during the phase

o Site Preparation including civil works, creation of LAN, electrical works, etc. during that phase after verification and approval by Manipur Police or its constituted committees or representatives

o Successful Data digitization / migration after verification and approval by Manipur Police or its constituted committees or representatives

o Training and Certification of all the trainees, trained on the CCTNS application modules of that Phase

o Procurement, deployment and commissioning of the hardware at PHQ, Data Center, DR Site and other locations required to support the functioning of modules of that Phase

o Procurement, deployment and commissioning of the networking equipments and provisioning of desired connectivity required to support the functioning of modules of that Phase

o Achievement of the Service Levels as expected during that Phase

o Acceptance / Sign off from Manipur Police or its constituted committees or representatives

1. REQUEST FOR PROPOSAL DATA SHEET

SL. NO.	INFORMATION	DETAILS
1	RFP Reference No. and Date	14/3 (CCTNS-SI) 2011-CB
2	Non Refundable Tender Cost	Rs. 20,000/- (Twenty Thousand only) in form of Demand Draft in favour of "SP CID(Crime Branch), Manipur", payable at Imphal, Manipur
3	Sale of RFP Document	13th April,2011 to 22nd April 2011upto 4.00 PM
4	Earnest Money Deposit (EMD/Bid Security)	@ 2.5% of Bid Value in the form of Demand Draft in favour of "SP CID (Crime Branch), Manipur", payable at Imphal, Manipur (as per details in Sec. 2.2.9)
5	Last date and time for submission of written queries for clarifications	25th April 2011 up to 12.00 PM
6	Date, Time and Venue for Pre-bid Meeting	28th April 2011 at 3.00 PM at "CID Headquarters", Imphal, Manipur
7	Release of response to clarifications	4th May 2011
8	Last date, Time (deadline) and Venue for receipt of proposals in response to RFP notice	12th May, 2011 up to 12.00 PM at "CID Headquarters", Imphal, Manipur
9	Date, Time and Venue of opening of Technical Proposals received in response to the RFP notice	12th May, 2011 at 3.00 PM at "CID Headquarters", Imphal, Manipur
10	Place, Time and Date of Technical Presentations by the Bidders	At "CID Headquarters", Imphal, Manipur on 25th May, 2011 and 26th May, 2011, 11 AM onwards
11	Place, Time and Date of opening of Financial Proposals received in response to the RFP notice	To be intimated later
12	Contact Persons for queries	(i) "Shri. L.M.Khaute, IPS, Additional Director General of Police (Armed Police and Training), Manipur , Imphal" Ph. No. / Fax : 0385-2450575 Mobile : 09436021985 (ii) "Dr S. Ibocha Singh, IPS, SP CID (Crime

		Branch), Manipur, Imphal" Phone No. : 0385 - 2451501(O) Fax No. : 0385- 2451501 Mobile : 09436027465
13.	Addressee and Address at which proposal in response to RFP notice is to be submitted	Shri. L.M.Khaute, IPS, Additional Director General of Police (Armed Police & Training), Manipur, C/O. Crime Branch, CID Headquarters, Imphal, Manipur - 795001

2. INTRODUCTION

2.1 PROJECT BACKGROUND

Availability of relevant and timely information is of utmost necessity in conduct of business by Police, particularly in investigation of crime and in tracking & detection of criminals. Police organizations everywhere have been handling large amounts of information and huge volume of records pertaining to crime and criminals.

Information Technology (IT) can play a very vital role in improving outcomes in the areas of Crime Investigation and Criminals Detection and other functioning of the Police organizations, by facilitating easy recording, retrieval, analysis and sharing of the pile of Information. Quick and timely information availability about different facets of Police functions to the right functionaries can bring in a sea change both in Crime & Criminals handling and related Operations, as well as administrative processes.

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

2.2 BACKGROUND OF POLICE SYSTEMS IN INDIA

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

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

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

2.2.1 Crime and Criminals Information System (CCIS)

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

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

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

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

2.2.2 Common Integrated Police Application (CIPA)

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

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

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

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

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

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

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

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.

2.4 CCTNS IMPLEMENTATION FRAMEWORK

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

2.5 GOALS OF THIS REQUEST FOR PROPOSAL (RFP)

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

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

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

3. PROJECT OVERVIEW

3.1 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.

3.2 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.

3.3 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

3.4 DESIRED OUTCOMES FROM VARIOUS STAKEHOLDERS

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

Benefits to Citizens

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

Benefits to Police Department

i) Enhanced tools for investigation
ii) Centralized crime and criminal information repository along with the criminal images and fingerprints with advanced search capabilities
iii) Enhanced ability to analyze crime patterns, modus operandi
iv) Enhanced ability to analyze accidents and other road incidents
v) Faster turnaround time for the analysis results (crime and traffic) to reach the officers on the field
vi) Reduced workload of the police station back-office activities such as preparation of regular and ad-hoc reports and station records management
vii) Enhanced tools to optimize resource allocation for patrols, emergency response, petition enquiries, and other general duties
viii) A collaborative knowledge-oriented environment where knowledge is shared across the different regions and units
ix) Better coordination and communication with external stakeholder through implementation of electronic information exchange systems

Benefits to Ministry of Home Affairs (NCRB)

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

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

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

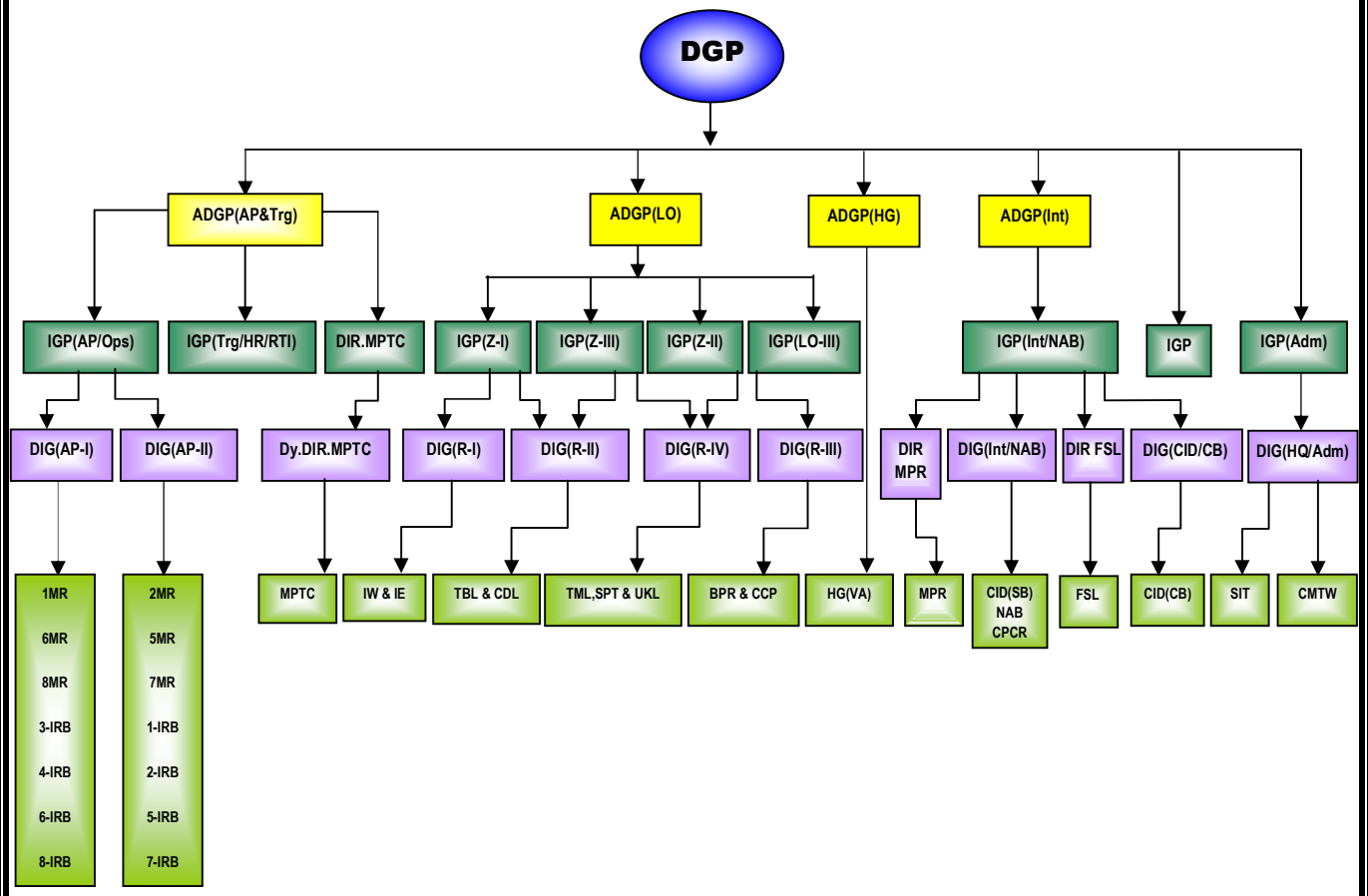
iv) The ability to respond faster and with greater accuracy to inquiries from the parliament, citizens and citizens groups; and to RTI queries.

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

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

4. STATE POLICE DEPARTMENT

4.1 ORGANIZATION STRUCTURE



Manpower Strength

The break-up of the police force in Manipur is provided below:

Break-up of Police Personnel in the State	
GROUP	**NO. OF PERSONNEL**
Group A – Senior Officers of SP rank and above	48
Group B – Officers of ASI rank and above	2,566
Group C – Personnel of Constable rank and above	14,164
TOTAL	**17,798**

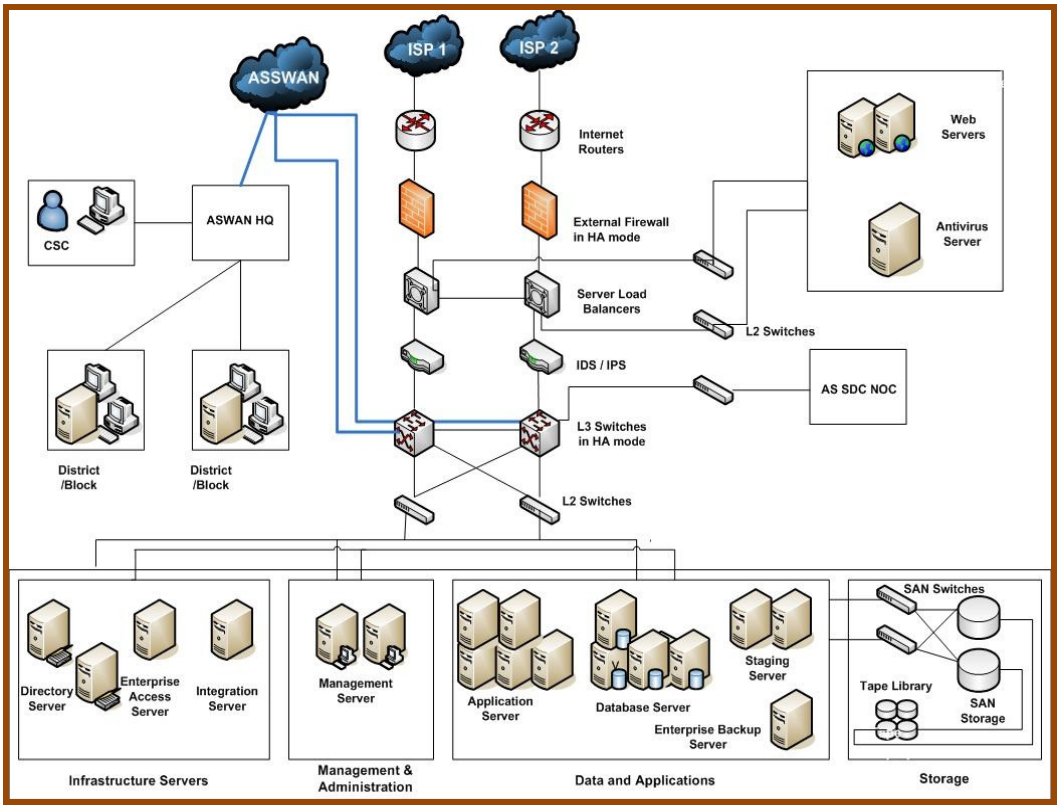
4.2. EXISTING LEGACY SYSTEMS

The various Software Applications currently installed at Manipur Police, their platforms and an assessment of their usages is summarized in the following table.

SL. NO.	APPLICATION SOFTWARE NAME	AREAS OF POLICE FUNCTIONING COVERED	DATE OF COMMISSIONING	PRESENT STATUS	REMARKS / COMMENT
1.	CCIS (Crime & Criminal Information System)	10(ten) districts including CID	2000	System working only in Imphal West District. Server machine for remaining 8 districts became defective since April, 2008.	However, data for daily crime reporting being sent through alternative means.
2.	Crime in India (Annual Report)	- do-	2000	Functioning	
3.	Monthly Crime Statistics	- do-	2000	Functioning	
4.	Accidental Deaths & Suicide	- do-	2000	Functioning	
5.	M.V.C.S. (Motor Vehicles Co-ordination Systems)	S.C.R.B, CID(CB), CID Head Quarter.	2005	Functioning	

4.3 EXISTING DATA CENTER INFRASTRUCTURE

Manipur SDC is to consolidate services, applications and infrastructure to provide efficient electronic delivery of G2G, G2C and G2B services. SDC infrastructure shall provide adequate space to house ICT assets of various departments within the state in an environment that meets the need for reliability, availability, scalability, security and serviceability. Various applications and some of the functionalities envisaged at the Manipur SDC include Secure Central Data Repository of the State, Core Application Servers, Service Delivery Gateway, Citizen Information/Services Portal, State Intranet Portal, Remote Management and Service Integration facility. Manipur SDC will act as a mediator and convergence point between open unsecured public domain and sensitive government environment. It will be equipped to host/ co-locate systems such as Web Servers, Application Servers, Database Servers, SAN, and NAS etc.



Coverage of the Project: SDC shall be connected through SWAN & Internet cloud, its services will be available throughout the state to various Govt. departments & agencies including Police Department.

Data Center Services : Manipur SDC is expected to provide following services and it would be the participating department's option to avail any or all services:

- Physical & rack space in the Data Center.
- Availability of power and cooling infrastructure and other facility as per SLA.
- Scalability in terms of availability of physical space, racks and supporting infrastructure.
- Foolproof security – locked server cabinets, with IP-based CCTV surveillance and hand key biometric access to all areas.
- 24x7 monitoring of the IT infrastructure.
- Server Management- Periodic system upgrades/updates, patch management, OS support, hardening etc.
- Security Management– physical as well as IT infrastructure security management including firewall Monitoring, configuration updates, Intrusion detection and prevention, antivirus, performing periodic audits etc.
- Database services– database provisioning & allocation.
- Storage Infrastructure inclusive of storage space, administration, and management services.
- Backup infrastructure and services.
- Mail and portal services.

The State Govt. of Manipur with the engagement of an empanelled vendor had prepared DPR for establishing SDC in Imphal. Also, the RFP for Design, Site Preparation, Supply, Installation, Commissioning, Maintenance and Operations of the State Data centre for a period of five years was published by the Department. Thereafter, LoI was issued to M/s Reliance Communications Infrastructure Ltd. and the target to complete the roll-out of SDC has been taken as 29 months.

4.4 EXISTING WAN INFRASTRUCTURE

Manipur State Wide Area Network

The Manipur State Wide Area Network is the core project of connectivity for all e-governance project in the State with an objective to ensure connectivity for all State Government departments/agency up to block level. The SWAN which is a 3 (three) tier network shall ensure minimum 2 Mbps connectivity up to the block level. It is specifically and independently built for the State with heterogeneous applications and Devices have common Network Standards & Security Policy as specified by GOI. The network is interoperable and the biggest advantage is that, it allows for partial or three-layer solutions, where the Networks overlap in some but not all places, or where an intermediate layer that speaks to both protocols is created.

Essential Features of the SWAN Infrastructure

- Inter-operability with NICNET at State Hqrs. and adherence to other Standards, Interconnect and Security policy Guidelines already circulated to the States.
- Wireless connectivity infrastructure required at Block Hqrs for connectivity to 'Common Service Centers' (CSCs).
- Network connectivity hardware at State Hqrs. PoP required to support connectivity and traffic load for the State Data Centre (SDC)
- Voice over IP phones to be made available at least one at each PoP
- Network items to support both IPv4 and IPv6 protocol for Horizontal Connectivity under NeGP.
- Bandwidth is up-gradable on demand as the network has deployed STM card.
- The total number of POPs - 160 nos
- Backup power arrangement and security provided in all POP locations

State Wide Area Network (SWAN) has been identified as one of the Mission Mode Projects under the National e-Governance Plan by Department of Information Technology, Govt. of India (DIT, GoI) to increase transparency and effectiveness for delivery of citizen services. This scheme envisages establishment of an intra-government network with a minimum of 2 Mbps connectivity from the State Headquarters to Block level through District/Sub-Division Headquarters for providing the connectivity to facilitate the rolling out of citizen-centric services under various Mission Mode Projects (MMPs). States have aggressively taken up implementation of this project and very shortly all States should be networked upto the block level creating the building block for:

- Integration of various existing stand-alone applications and provide effective interconnectivity
- Effective Voice and Video communication
- Data transfer needs between departments as also government to public
- Improved quality of decision-making and governance due to easy access of information
- Improve government response time to citizens from weeks to minutes
- Fast and reliable information flow –

1. Government to Government (G2G)
2. Government to Citizen (G2C)
3. Citizen to Government (C2G)
4. Government to Business (G2B)

Department of IT, Government of Manipur has established State Wide Area Network (SWAN) in Manipur. This network has Data, Voice and Video transmission facilities. The network shall be utilized for the inter-Departmental connectivity, multi-user and multi-service facilities, video conferencing, email, on-line application processing and query. SWAN shall enable better communication and information sharing to allow the officers to work more effectively, resulting in cohesive administration. The implementation of SWAN will cover strengthening of existing and future intranet at the State Secretariat, CM secretariat, Government Departments in the state capital, District Headquarters, Sub-Divisions and Block headquarters with the existing and proposed gateway infrastructure.

SWAN is a secured network for the state of Manipur and is based on VSAT and Leased Circuit. SWAN in Manipur has 42 PoPs located in State Headquarter, District Headquarters, Sub-divisional Headquarters and Block Headquarters.

The list of SWAN PoPs and type of connectivity (OFC / VSAT) is illustrated in following table:

Table 2 : Distribution of Manipur SWAN PoP

SL. NO.	NAME OF DISTRICT	PoP LOCATION	CONNECTIVITY TYPE
1	State Centre	NIC State Unit	OFC
2	Imphal West	SDO Wangoi	OFC
3	Imphal East	ADC Jiri	OFC
4		SDO Keirao Bitra	OFC
5		SDO Sawombung	OFC
6	Bishnupur	NIC Bishnupur	OFC
7		SDO Nambol	OFC
8		SDO Moirang	OFC
9	Thoubal	NIC Thoubal	OFC
10		SDO Lilong	OFC
11		SDO Kakching	OFC
12	Churachandpur	NIC Churachandpur	OFC
13		SDO Singhat	OFC
14		ADC Pherzawl	VSAT
15		SDO Thanlon	VSAT
16		SDO Henglep	VSAT
17		SDO Tipaimukh	VSAT
18		BDO Vangai Range	VSAT
19		BDO Sangaikot	VSAT
20	Senapati	NIC Senapati	OFC
21		ADC Kangpokpi	OFC
22		SDO Paomata	OFC
23		SDO Purul	OFC
24		SDO Saikul	OFC
25		SDO Saitu Gamphazol	OFC
26		SDO Tadubi	OFC
27	Ukhrul	NIC Ukhrul	OFC

28		SDO Chingai (N)	OFC
29		SDO Kasom Khullen (S)	OFC
30		SDO Kamjong	OFC
31		SDO Phungyar	VSAT
32		BDO Lungchong Maphei	VSAT
33	Tamenglong	NIC Tamenglong	OFC
34		SDO North Tamenglong (Tamei)	OFC
35		SDO Nungba	OFC
36		SDO West (Tousem)	VSAT
37		BDO Khoupum	VSAT
38	Chandel	NIC Chandel	OFC
39		SDO Moreh	OFC
40		SDO Chakpikarong	OFC
41		SDO Machi	VSAT
42		BDO Khenjoy	VSAT

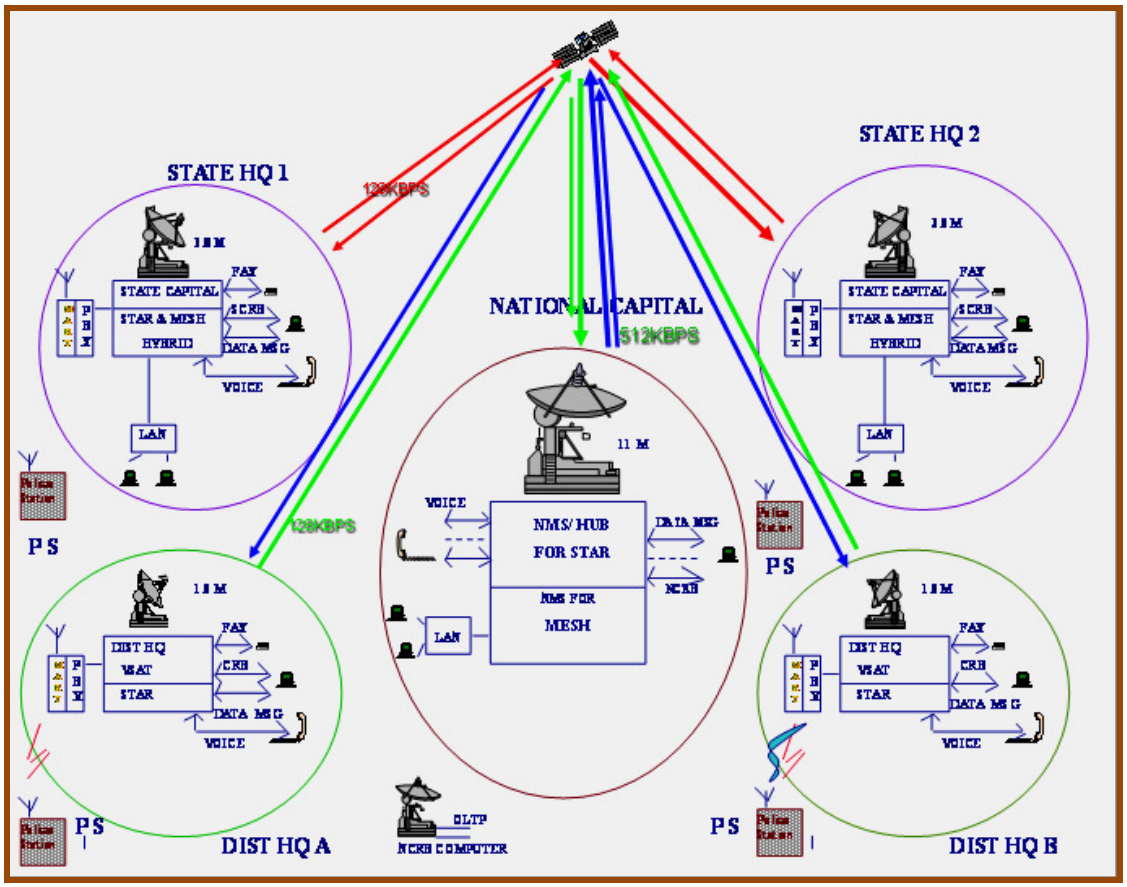
4.5 EXISTING CLIENT SITE INFRASTRUCTURE

Existing Network Information

POLNET is a satellite based wide area network for the modernization of Police Telecommunication of country. POLNET is an amalgamation of different latest VSAT technologies i.e. TDM/TDMA, SCPC/DAMA and DVB-S. It is a huge network consisting of about 1,000 V-SATs at each State Capital, District Head Quarter and selected locations of CPMF's (BSF, ITBP, CISF, CRPF, Manipur Rifles, SSB) and CPO's. At present POLNET caters to 961 no. of V-SAT's through a HUB installed in New Delhi with 11 m Antenna with necessary outdoor and indoor equipments to support total V-SAT Network of about 1,500 locations for Voice, Data, Fax facilities. Out of existing 961 V-SAT terminals, 41 V-SAT terminals of 3.8 m antenna size are installed at the State Capitals / UT and some of the CPOs locations based on Hybrid technology which can support both TDM / TDMA and SCPC / DAMA scheme for Star and Mesh connectivity, 811 TDM/TDMA V-SAT terminals with 1.8 / 2.4 m Antenna size installed at District Head Quarters of all States and UTs and other

important locations of CPMF's, MHA, NCRB, CPO's etc. The remaining 109 are broadband V-SAT terminals based on DVB-S technology installed at various locations of BSF and ITBP. The TDM/TDMA V-SAT works on double hop link through the Central Hub at New Delhi for communication with other sites. The connectivity from District Headquarters is being extended upto Police Stations / Police Posts through local Radio Network using MART (Multi Access Radio Telephone) system. POLNET network is also providing connectivity for interlinking NCRB computers to SCRB and DCRB computers provided to State/District Head Quarters for online transaction processing.

Exhibit 3 : Schematic Diagram of POLNET



In Manipur Police, POLNET connectivity is available at 9 districts at their Head Quarters through V-SAT. The status of each of the V-SAT connectivity is as follows:

Manipur Police Wireless

The Manipur Police Wireless unit is regarded as one of the best organizations and well equipped wireless unit in the North Eastern region.

CATEGORY	EQUIPMENT DETAIL	NUMBERS
VHF	(i) SIMOCO PRM 8019/20 L.V	232
	(ii) SIMOCO PRM 8020 H.V	73
	(iii) MOTOROLA GM 300 H.V	115
	(iv) ICOM F310 H.V	115
	(v) ICOM MS-2350 MONITORING SETS	50
	(vi) MOTOROLA GM 369 L.V	30
	(vii) ICOM F110 H.V	30
	(viii) ICOM F111	100
	(ix) ICOM REPEATER	11
	(x) MOTOROLA GR 300(R)	15
	(xi) SIMOCO PRR 8019 L.V. REPEATER	25
	(xii) HYT TM 610 H.V	182
	(xiii) ICOM F3 H.V	189
	(xiv) ICOM F3 G.T. H.V	198
	(xv) MOTOROLA GP 38 H.V	257
	(xvi) HYT TC 700 H.V	550
UHF	(i) HAND HELD XTS 3000 DTS SETS	40
	(ii) STATIC ASTRO SPECTRA DTS	76
	(iii) MOTOROLA FIX STATION SETS	4
HF	(i) BARRETT MS 530 -50 NOS	50
	(ii) TRC 80 -8 NOS	8
	(iii) MS 707 -10 NOS	10

SL. NO.	DISTRICT	POLICE STATION	MODE OF COMMUNICATION
	Bishnupur		
1.		Bishnupur	VHF (Lower Band)
2.		Nambol	-do-
3.		Moirang	-do-
4.		Loktak	-do-
5.		Kumbi	-do-
	Imphal West		
6.		City PS	VHF (Higher Band)

7.		Lamphel	-do-
8.		Singjamei	-do-
9.		Patsoi	VHF (Lower Band)
10.		Lamsang	-do-
11.		Sekmai	-do-
12.		Mayang Imphal	-do-
13.		Imphal West PS	VHF (Higher Band)
	Imphal East		
14.		Jiribam	VHF (Lower Band)
15.		Lamlai	-do-
16.		Heingang	-do-
17.		Porompat	-do-
	Thoubal		
18.		Thoubal	VHF (Lower Band)
19.		Lilong	-do-
20.		Yairipok	-do-
21.		Kakching	-do-
22.		Waikhong	-do-
23.		Sugnu	-do-
	Chandel		
24.		Chandel	VHF (Higher Band)
25.		Moreh	-do-
26.		Tengnoupal	-do-
	Senapati		
27.		Senapati PS	VHF (Lower Band)
28.		Mao	-do-

29.		Tadubi	-do-
30.		Kangpokpi	-do-
31.		Saikul	-do-
	Tamenglong		
32.		Tamenglong	VHF (Lower Band)
33.		Nungba	-do-
	Ukhrul		
34.		Litan	VHF (Lower Band)
35.		Jessami	-do-
36.		Chassad	-do-
37.		Sansak	-do-
38.		Ukhrul	-do-
	Churachandpur		
39.		Churchandpur	VHF (Lower Band)
40.		Singhat	-do-

Storage Infrastructure

SL. NO.	ITEMS	DETAILS	
1.	Data Center Availability	NIC Data Centre	Yes (State level)
		State Data Centre	Under implementation
		Police Data Centre	Yes (Manipur Police Computer Centre).
2.	Address of Data Centre Building	NIC Data Centre	Room No. 166, 3rd Floor- Ministers Block, New Secretariat, Imphal.
		Police Data Centre	Police Computer Centre, Jail Road,

			Imphal & CID(SB), HQ.
3.	Recommended by State/UT (for Data Center)	NIC Data Center/State Data Center/ Police Data Center.	NIC Data Centre, Manipur.

Infrastructure Analysis at Police Station Level

An analysis of the existing infrastructure at Police Station was tried to be assessed for which a format was created. The very purpose was to see whether IT hardware/assets proposed under CCTNS can be installed and functions smoothly. The report is given in the following table:

IT Hardware Availability & Requirement in Police Stations & Units:

Sl. No.	Zone	Range	District	Sub-Division	Police Station	Whether covered under CIPA (Yes/No)	Computers Available	No. of Computers Required	Printer required (Yes/No)	Multi Functional Device Required (Yes/No)	UPS Required (Yes/No)	Generator Required (Yes/No)	Port Switch Required (Yes/No)	Site Preparation Required (Yes/No)	Type of Connectivity Required
1.	IGP (Zone-I), PHQ Babupara, Imphal.	DIG (R-I), SP/IMPHAL (W) Office Complex, Imphal.	1. Imphal West District, Imphal.	1. SDPO Imphal, District Head Quarter, SP Imphal West Office Complex.	1. Imphal P.S, District Head Quarter, SP Imphal West Office Complex.	Yes	4 (Under CIPA Project)	4 (The hardware need replacement due to wear & tear)	Yes	Yes	Yes	Yes	Yes	Yes	Broadband
2.	-do-	-do-	-do-	-do-	2. City P.S, M.G. Avenue, Imphal.	Yes	4 (Under CIPA Project)	4 (The hardware need replacement due to wear &	Yes	Yes	Yes	Yes	Yes	Yes	-do-

								tear)							
3.	-do-	-do-	-do-	-do-	3. Imphal West Women P.S, SP Imphal West Office Complex.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
4.	-do-	-do-	-do-	-do-	4. Anti Human Trafficking Unit, Imphal West.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
5.	-do-	-do-	-do-	-do-	5.Special Juvenile Police Unit, Imphal West.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
6.	-do-	-do-	-do-	2.SDPO Singjamei, Kakwa	1. Singjamei P.S, Kakwa Imphal.	Yes	1	3	No	No	No	No	No	Yes	-do-
7.	-do-	-do-	-do-	-do-	2. Mayang Imphal P.S, Mayang Imphal.	No	3	1	No	Yes	No	Yes	No	Yes	-do-

8.	-do-	-do-	-do-	-do-	3. Wangoi P.S, Wangoi.	No	3	1	No	Yes	No	Yes	No	Yes	-do-
9.	-do-	-do-	-do-	2.SDPO Lamphel, Lamphel.	1. Lamphel P.S, Lamphel.	Yes	4 (Under CIPA Project)	4(The hardware need replacement due to wear & tear)	Yes	Yes	Yes	Yes	Yes	Yes	-do-
10.	-do-	-do-	-do-	-do-	2. Lamshang P.S, Taothong.	No	3	1	No	Yes	No	Yes	No	Yes	-do-
11.	-do-	-do-	-do-	-do-	3. Patsoi P.S, Patsoi Part-IV	No	3	1	No	Yes	No	Yes	No	Yes	-do-
12.	-do-	-do-	-do-	-do-	4. Sekmai P.S, Sekmai.	No	3	1	No	Yes	No	Yes	No	Yes	-do-
13.	-do-	-do-	2. Imphal East District,	1. SDPO Porompat, Porompat Imphal	1. Porompat P.S., Porompat.	Yes	4 (Under CIPA Project)	4(The hardware need replacement	Yes	Yes	Yes	Yes	Yes	Yes	-do-

			Imphal.	East.				due to wear & tear)							
14.	- do -	- do -	-do-	-do-	2. Heingang P.S., Heingang.	No	3	1	No	Yes	No	Yes	No	Yes	-do-
15.	- do -	- do -	-do-	-do-	3. Irilbung P.S., Irilbung.	No	3	1	No	Yes	No	Yes	No	Yes	-do-
16.	- do -	- do -	-do-	-do-	4. Andro P.S., Andro.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
17.	- do -	- do -	-do-	-do-	5. Women P.S., I/E.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
18.	- do -	- do -	-do-	-do-	5. Anti Human Trafficking Unit, Porompat	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
19.	- do -	- do -	-do-	SDPO Lamlai Imphal	1. Lamlai P.S.,	No	3	1	No	Yes	No	Yes	No	Yes	-do-

				East.	Napetpalli.										
20.	- do -	- do -	-do-	-do-	2.Thoubal Dam P.S., I/E.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
21.	- do -	- do -	-do-	-do-	3.Yaingangpokpi P.S., I/E.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
22.	- do -	- do -	-do-	-do-	4. Sagolmang P.S., Sagolmang.	No	1	3	No	No	No	Yes	No	Yes	-do-
23.	-do-	-do-	2. Imphal East District, Imphal.	2. SDPO Jiribam Imphal East.	1. Jiribam P.S, Jiribam.	No	3	1	No	Yes	No	Yes	No	Yes	-do-
24.	-do-	-do-	-do-	-do-	2. Borobeeka P.S.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
25.	IGP (Zone-II), PHQ Babupara, Imphal.	DIG (R-II), SP/Thoubal Office Complex, Khang	SP/ Thoubal Khangabok	1. SDPO Thoubal, Thoubal.	1.Thoubal P.S., Thoubal.	Yes	4 (Under CIPA Project)	4(The hardware need replacement due to wear & tear)	Yes	Yes	Yes	Yes	Yes	Yes	-do-

		abok.													
26.	- do -	- do -	-do-	-do-	2. Lilong, P.S., Lilong.	No	3	1	No	Yes	No	Yes	No	Yes	-do-
27.	- do -	- do -	-do-	-do-	3.Yairipok P.S., Yairipok	No	3	1	No	Yes	No	Yes	No	Yes	-do-
28.	- do -	- do -	-do-	-do-	4. Women P.S., SP Thoubal Office Complex.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
29.	- do -	- do -	-do-	-do-	5.Anti Human Trafficking Unit, Thoubal	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
30.	- do -	- do -	-do-	-do-	5. Heirok P.S., Heirok	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
31.	- do -	- do -	-do-	-do-	6. Nongpok Sekmai PS, Nongpok Sekmai	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-

32.	- do -	- do -	-do-	SDPO Kakching	1. Kakching P.S., Kakching.	No	1	3	No	No	No	No	No	Yes	-do-
33.	- do -	- do -	-do-	-do-	2. Pallel P.S., Pallel.	No	1	3	No	No	No	Yes	No	Yes	-do-
34.	- do -	- do -	-do-	-do-	3.Hiyanglam PS, Hiyanglam	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
35.	- do -	- do -	-do-	-do-	4, Khongjom PS, Khongjom	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
36.	- do -	- do -	-do-	2. SDPO Sugnu, Sugnu.	1. Sugnu P.S., Sugnu.	No	3	1	No	Yes	No	Yes	No	Yes	-do-
37.	- do -	- do -	-do-	-do-	2. Waikhong P.S., Waikhong.	No	3	1	No	Yes	No	Yes	No	Yes	-do-
38.	- do -	- do -	-do-	-do-	3.Wangoo PS, Wangoo	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
39.	IGP (Zone-II), PHQ Babupara,	DIG (R-III), 1st M.R.	SP- Bishnupur,	1. SDPO Bishnupur, Bishnupur	1. Bishnupur P.S, Bishnupur.	Yes	3 (Under CIPA Project)	4(The hardware need replace	Yes	Yes	Yes	Yes	Yes	Yes	-do-

	Imphal.	Complex, Imphal.	Bishnupur.	.				ment due to wear & tear)							
40.	- do -	- do -	-do-	-do-	2. Nambol P.S, Nambol	No	3	1	No	Yes	No	Yes	No	Yes	-do-
41.	- do -	- do -	-do-	-do-	3. Loktak P.S, Kom Keirak	No	3	1	No	Yes	No	Yes	No	Yes	-do-
42.	- do -	- do -	-do-	-do-	4. Women P.S, SP-Office, Bishnupur.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
43.	- do -	- do -	-do-	-do-	5. Anti Human Traffiking Unit, Bishnupur.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
44.	- do -	- do -	-do-	2. SDPO Moirang, Moirang.	1. Moirang P.S, Moirang	No	1	3	No	No	No	No	No	Yes	-do-
45.	- do -	- do -	-do-	-do-	2. Kumbi P.S,	No	3	1	No	Yes	No	Yes	No	Yes	-do-

					Kumbi.										
46.	- do -	- do -	-do-	-do-	3.Phougakchao PS, Phougakchao Ikhai	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
47.	- do -	- do -	-do-	-do-	4.Arong Nongmaikhong PS, Arong Nongmaikhong	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
48.	- do -	- do -	-do-	-do-	5.Keibul Lamjao PS, Keibul Lamjao	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
49.	IGP (Zone-II), PHQ Babupara, Imphal.	DIG (R-III), 1st M.R. Complex, Imphal.	SP- Churachan-dpur, Tuibong.	1. SDPO Churachandpur, Tuibong.	1. Churachan-dpur P.S, Tuibong.	No	1	3	No	No	No	No	No	Yes	-do-
50.	- do -	- do -	-do-	-do-	2. Singhat	No	1	3	No	No	No	Yes	No	Yes	-do-

					P.S, Singhat.										
51.	- do -	- do -	-do-	-do-	3. Churachan-dpur Women P.S, SP-Office, Tuibong.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
52.	- do -	- do -	-do-	-do-	4. Anti Human Trafficking Unit, SP-Office, Tuibong.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
53.	- do -	- do -	-do-	-do-	4. Sangai Kot PS, Sangai Kot	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
54.	IGP (Zone-II), PHQ Babupara, Imphal.	DIG (R-III), 1st M.R. Complex,	SP-Churachan-dpur, Tuibong.	1. SDPO Thanlon, SP-Office, Tuibong.	1. Parbung P.S., SP Office Tuibong.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-

		Imphal.													
55.	- do -	- do -	-do-	-do-	2. Thanlon P.S, SP Office Tuibong.	No	1	3	No	No	No	Yes	No	Yes	-do-
56.	- do -	- do -	-do-	-do-	3. Henglep P.S, SP Office Tuibong.	No	1	3	No	No	No	Yes	No	Yes	-do-
57.	IGP (Zone-II), PHQ Babupara, Imphal.	DIG (R-IV), Senapati.	SP-Tamenglong, Tamenglong.	1. SDPO Tamenglong, Tamenglong	1. Tamenglong P.S., Tamenglong	No	3	1	No	Yes	No	Yes	No	Yes	-do-
58.	- do -	- do -	-do-	-do-	2. Tamenglong Women P.S, SP-Office, Tamenglong	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
59.	- do -	- do -	-do-	-do-	3.Anti Human Trafficking Unit, SP-Office, Tamenglong	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-

60.	- do -	- do -	-do-	2. SDPO Tamei, Tamenglong	1. Tamei P.S, SP-Office, Tamenglong.	No	1	3	No	No	No	Yes	No	Yes	-do-
61.	- do -	- do -	-do-	3. SDPO Tousem, Tamenglong	1. Tousem P.S, SP-Office, Tamenglong.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
62.	- do -	- do -	-do-	4. SDPO Nungba, Nungba.	1. Nungba P.S, Nungba	No	1	3	No	No	No	Yes	No	Yes	-do-
63.	- do -	- do -	-do-	-do-	2. Noney P.S, Noney.	No	1	3	No	No	No	Yes	No	Yes	-do-
64.	- do -	- do -	-do-	-do-	3. Khoupum P.S, SP-Office, Tamenglong.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
65.	IGP (Zone-III), PHQ Babupara, Imphal.	DIG (R-II), Thoubal.	SP-Chandel, Chandel.	1. SDPO Chandel, Chandel.	1. Chandel P.S, SP-Office, Chandel .	No	3	1	No	Yes	No	Yes	No	Yes	-do-

66.	- do -	- do -	-do-	-do-	2. Chakpikarong P.S, Chandel.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
67.	- do -	- do -	-do-	-do-	3. Chandel Women P.S, Chandel.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
68.	- do -	- do -	-do-	-do-	4.Anti Human Trafficking Unit, Chandel.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
69.	- do -	- do -	-do-	2. SDPO Moreh, Moreh.	1. Moreh P.S, Moreh.	No	3	1	No	Yes	No	Yes	No	Yes	-do-
70.	- do -	- do -	-do-	-do-	2. Tengnoupal P.S, Tengnoupal	No	1	3	No	No	No	Yes	No	Yes	-do-
71.	- do -	- do -	-do-	-do-	3. Molcham P.S, Molcham.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
72.	- do -	- do -	-do-	-do-	4. Khengjoy PS, Khengjy	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-

73.	IGP (Zone-III), PHQ Babupara, Imphal.	DIG (R-IV), Senapati.	SP-Senapati, Senapati.	1. SDPO Senapati, Senapati.	1. Senapati P.S, Senapati.	No	1	3	No	No	No	No	No	Yes	-do-
74.	- do -	- do -	-do-	-do-	2. Chalwa PS, Chalwa	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
75.	- do -	- do -	-do-	-do-	3. Senapati Women P.S, Senapati.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
76.	- do -	- do -	-do-	-do-	4.Anti Human Trafficking Unit, Senapati.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
77.	- do -	- do -	-do-	2. Addl. SP Kangpokpi, Kangpokpi.	1. Kangpokpi P.S, Kangpokpi.	No	3	1	No	Yes	No	Yes	No	Yes	-do-
78.	- do -	- do -	-do-	-do-	2. Saikul P.S, SP Office, Senapati.	No	1	3	No	No	No	Yes	No	Yes	-do-

79.	- do -	- do -	-do-	-do-	3.Gamnom Sapermeina P.S, Gamnom Sapermeina.	No	3	1	No	Yes	No	Yes	No	Yes	-do-
80.	- do -	- do -	-do-	-do-	4. New Keitheelmanbi PS, New Keithelmanbi	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
81.	- do -	- do -	-do-	1. SDPO Mao, Mao.	1. Mao P.S, Mao.	No	1	3	No	No	No	Yes	No	Yes	-do-
82.	- do -	- do -	-do-	-do-	2. Tadubi P.S, Tadubi.	No	1	3	No	No	No	Yes	No	Yes	-do-
83.	- do -	- do -	-do-	-do-	3.Tungjoy PS, Tungjoy	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
84.	- do -	- do -	-do-	-do-	4.Purul PS, Purul	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
85.	- do -	- do -	-do-	-do-	5.Phaibung PS, Phaibung	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
86.	- do -	- do -	-do-	-do-	6.Willong PS, Willong	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-

87.	- do -	- do -	-do-	-do-	7. Dzuko PS, Dzuko	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
88.	- do -	- do -	SP-Ukhrul, View Land (Ukhrul)	1. SDPO Ukhrul, Wino Bazar, Ukhrul..	1. Ukhrul P.S, Wino Bazar, Ukhrul.	No	3	1	No	Yes	No	Yes	No	Yes	-do-
89.	- do -	- do -	-do-	-do-	2. Litan P.S, Litan.	No	3	1	No	Yes	No	Yes	No	Yes	-do-
90.	- do -	- do -	-do-	-do-	3. Somdal P.S, SP Office, Ukhrul.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
91.	- do -	- do -	-do-	-do-	4. Sanakeithhel PS, Sanakeithel	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
92.	- do -	- do -	-do-	-do-	5. Ukhrul Women P.S, SP Office, Ukhrul.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-

93.	- do -	- do -	-do-	-do-	6.Anti Human Trafficking Unit, SP Office, Ukhrul.	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
94.	- do -	- do -	SP-Ukhrul, View Land (Ukhrul)	2. SDPO Phungyar, SP Office, Ukhrul	1. Phungyar P.S, SP Office, Ukhrul..	No	1	3	No	No	No	Yes	No	Yes	-do-
95.	- do -	- do -	-do-	-do-	2. Shangsak P.S, Shangsak.	No	1	3	No	No	No	Yes	No	Yes	-do-
96.	- do -	- do -	-do-	-do-	3. Chassad P.S, SP Office, Ukhrul..	No	1	3	No	No	No	Yes	No	Yes	-do-
97.	- do -	- do -	-do-	-do-	4. Kasom-Khullen P.S, SP Office, Ukhrul..	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-
98.	- do -	- do -	-do-	2. SDPO	1. Chingai	No	Nil	4	Yes	Yes	Yes	Yes	Yes	Yes	-do-

				Chingai, SP Office, Ukhrul.	P.S, SP Office, Ukhrul..										
99.	- do -	- do -	-do-	3. SDPO Jeshami, SP Office, Ukhrul	1. JeshamiP.S, SP Office, Ukhrul..	No	1	3	No	No	No	Yes	No	Yes	-do-
100.	IGP(Int), CID Head Quarter, Imphal.	DIG(Int/NAB)	SP Narcotic Affairs & Border, Jail Road, Imphal.	Nil	Narcotic Affairs & Border P.S, Jail Road, Imphal.	No	3	1	No	Yes	No	Yes	No	Yes	-do-
101.	- do -	DIG(CB)	SP/CID (Crime Branch), Manipur	Nil	CID (Crime Branch) P.S, Imphal.	No	1	3	No	No	No	Yes	No	Yes	-do-

IT Hardware Availability & Requirement at Sub Divisional Police Offices

Sl. No.	Zone	Range	District	Addl.SP/Sub-Division	Computers Available	No. of Computers Required	Printer required (Yes/No)	Multi Functional Device Required (Yes/No)	UPS Required (Yes/No)	Site Preparation Required (Yes/No)	Type of Connectivity Required
1.	IGP (Zone-I), PHQ Babupara, Imphal.	DIG (R-I), SP/IMP(W) Office Complex, Imphal.	1. Imphal West District, Imphal.	Addl. SP (L&O), Imphal West SP Office , Imphal.	Nil	3	Yes	Yes	Yes	Yes	Broadband
2.	- do -	- do -	-do-	Addl. SP (Ops), Imphal West SP Office , Imphal.	Nil	3	Yes	Yes	Yes	Yes	Broadband
3.	- do -	- do -	-do-	Addl. SP (P), Imphal West SP Office , Imphal.	Nil	3	Yes	Yes	Yes	Yes	Broadband
4.	- do -	- do -	-do-	SDPO Imphal, Imphal West SP Office , Imphal.	Nil	3	Yes	Yes	Yes	Yes	Broadband

5.	- do -	- do -	-do-	SDPO Lamphel, Imphal.	Nil	3	Yes	Yes	Yes	Yes	Broadband
6.	- do -	- do -	-do-	SDPO Singjamei, Imphal.	Nil	3	Yes	Yes	Yes	Yes	Broadband
7.	- do -	- do -	-do-	DY.SP Traffic, Imphal West SP Office , Imphal.	Nil	3	Yes	Yes	Yes	Yes	Broadband
8.	- do -	- do -	-do-	DY.SP Reserve, Imphal West SP Office , Imphal.	Nil	3	Yes	Yes	Yes	Yes	Broadband
9.	- do -	- do -	-do-	DY.SP Interogation Cell, Imphal West SP Office , Imphal.	Nil	3	Yes	Yes	Yes	Yes	Broadband
10.	- do -	- do -	-do-	DY.SP (CDO-I), Imphal West SP Office , Imphal.	Nil	3	Yes	Yes	Yes	Yes	Broadband
11.	- do -	- do -	-do-	DY.SP (CDO-II), Imphal West SP Office , Imphal.	Nil	3	Yes	Yes	Yes	Yes	Broadband

12.	- do -	- do -	-do-	DY.SP (Ops), Imphal West SP Office , Imphal.	Nil	3	Yes	Yes	Yes	Yes	Broadband
13.	IGP (L&O-I), PHQ Babupara, Imphal.	DIG (R-I), SP/IMP(W) Office Complex, Imphal.	1. Imphal East District, Imphal.	Addl. SP(L&O)-Imphal East, Porompat.	Nil	3	Yes	Yes	Yes	Yes	Broadband
14.	- do -	- do -	-do-	Addl. SP(Ops)-Imphal East, Porompat.	Nil	3	Yes	Yes	Yes	Yes	Broadband
15.	- do -	- do -	-do-	Addl.SP Jiribam	Nil	3	Yes	Yes	Yes	Yes	Broadband
16.	- do -	- do -	-do-	SDPO-Porompat, Porompat.	Nil	3	Yes	Yes	Yes	Yes	Broadband
17.	- do -	- do -	-do-	SDPO-Jiribam, Jiribam.	Nil	3	Yes	Yes	Yes	Yes	Broadband
18.	- do -	- do -	-do-	SDPO-Lamlai	Nil	3	Yes	Yes	Yes	Yes	Broadband
19.	- do -	- do -	-do-	Dy.SP (CDO-I), Imphal East	Nil	3	Yes	Yes	Yes	Yes	Broadband

20.	- do -	- do -	-do-	Dy.SP (CDO-II), Imphal East	Nil	3	Yes	Yes	Yes	Yes	Broadband
21.	- do -	- do -	-do-	Dy.SP (CAR), Imphal East	Nil	3	Yes	Yes	Yes	Yes	Broadband
22.	- do -	- do -	-do-	Dy.SP (Ops), Imphal East	Nil	3	Yes	Yes	Yes	Yes	Broadband
23.	IGP (Zone-I), PHQ Babupara, Imphal.	DIG (R-II), SP/Thoubal Office Complex, Khangabok.	Thoubal District, Thoubal.	Addl. SP-Thoubal, Khangabok.	Nil	3	Yes	Yes	Yes	Yes	Broadband
24.	- do -	- do -	-do-	AddlSP-Kakching, Kakching.	Nil	3	Yes	Yes	Yes	Yes	Broadband
25.	- do -	- do -	-do-	SDPO-Thoubal, Thoubal.	Nil	3	Yes	Yes	Yes	Yes	Broadband
26.	- do -	- do -	-do-	SDPO-Sugnu, Kakching.	Nil	3	Yes	Yes	Yes	Yes	Broadband
27.	- do -	- do -	-do-	SDPO-Kakching, Kakching.	Nil	3	Yes	Yes	Yes	Yes	Broadband

28.	- do -	- do -	-do-	Dy.SP(CDO-I), Thubal	Nil	3	Yes	Yes	Yes	Yes	Broadband
29.	- do -	- do -	-do-	Dy.SP(CDO-II), Thoubal	Nil	3	Yes	Yes	Yes	Yes	Broadband
30.	- do -	- do -	-do-	Dy.SP(CAR), Thoubal	Nil	3	Yes	Yes	Yes	Yes	Broadband
31.	- do -	- do -	-do-	Dy.SP(Ops), Thoubal	Nil	3	Yes	Yes	Yes	Yes	Broadband
32.	IGP (Zone-III), PHQ Babupara, Imphal.	DIG (R-II), Thoubal.	Chandel District, Chandel.	Addl. SP(L&O)-Chandel, Chandel.	Nil	3	Yes	Yes	Yes	Yes	Broadband
33.	- do -	- do -	-do-	Addl.SP(Ops)-Chandel, Chandel.	Nil	3	Yes	Yes	Yes	Yes	Broadband
34.	- do -	- do -	-do-	SDPO-Chandel, Chandel.	Nil	3	Yes	Yes	Yes	Yes	Broadband
35.	- do -	- do -	-do-	SDPO-Moreh, Moreh.	Nil	3	Yes	Yes	Yes	Yes	Broadband
36.	- do -	- do -	-do-	Dy.SP(CAR)-Chandel.	Nil	3	Yes	Yes	Yes	Yes	Broadband

37.	IGP (Zone-II), PHQ Babupara, Imphal.	DIG (R-III), 1st M.R. Complex, Imphal.	Churachandpur District, Churachandpur.	Addl. SP-Churachandpur, Tuibong.	Nil	3	Yes	Yes	Yes	Yes	Broadband
38.	- do -	- do -	-do-	SDPO-Churachandpur, SP Office, Tuibong.	Nil	3	Yes	Yes	Yes	Yes	Broadband
39.	- do -	- do -	-do-	SDPO-Thanglon, SP Office, Tuibong.	Nil	3	Yes	Yes	Yes	Yes	Broadband
40.	- do -	- do -	-do-	Dy.SP(CAR)-Churachandpur.	Nil	3	Yes	Yes	Yes	Yes	Broadband
41.	IGP (Zone-II), PHQ Babupara, Imphal.	DIG (R-III), 1st M.R. Complex, Imphal.	Bishnupur District, Bishnupur.	Addl. SP(Ops)-Bishnupur, Bishnupur.	Nil	3	Yes	Yes	Yes	Yes	Broadband
42.	- do -	- do -	-do-	Addl.SP(L&O), Bishnupur	Nil	3	Yes	Yes	Yes	Yes	Broadband
43.	- do -	- do -	-do-	SDPO-Bishnupur, Bishnupur.	Nil	3	Yes	Yes	Yes	Yes	Broadband

44.	- do -	- do -	-do-	SDPO-Moirang, Moirang.	Nil	3	Yes	Yes	Yes	Yes	Broadband
45.	- do -	- do -	-do-	Dy.SP(CAR), Bishnupur	Nil	3	Yes	Yes	Yes	Yes	Broadband
46.	- do -	- do -	-do-	Dy.SP(CDO-I), Bishnupur	Nil	3	Yes	Yes	Yes	Yes	Broadband
47.	- do -	- do -	-do-	Dy.SP(CDO-II), Bishnupur	Nil	3	Yes	Yes	Yes	Yes	Broadband
48.	- do -	- do -	-do-	Dy.SP(Ops), Bishnupur	Nil	3	Yes	Yes	Yes	Yes	Broadband
49.	- do -	- do -	-do-	Dy.SP(Loktak Protection Force), Bishnupur	Nil	3	Yes	Yes	Yes	Yes	Broadband
50.	IGP (Zone-II), PHQ Babupara, Imphal.	DIG (R-IV), Senapati.	Tamenglong District, Tamenglong.	Addl. SP-Tamenglong, Tamenglong.	Nil	3	Yes	Yes	Yes	Yes	Broadband
51.	- do -	- do -	-do-	SDPO-Tamenglong, Tamenglong.	Nil	3	Yes	Yes	Yes	Yes	Broadband

52.	- do -	- do -	-do-	SDPO-Nungba, Nungba.	Nil	3	Yes	Yes	Yes	Yes	Broadband
53.	- do -	- do -	-do-	SDPO-Tousem, Tousem.	Nil	3	Yes	Yes	Yes	Yes	Broadband
54.	- do -	- do -	-do-	SDPO-Tamei, Tamei.	Nil	3	Yes	Yes	Yes	Yes	Broadband
55.	IGP (Zone-III), PHQ Babupara, Imphal.	DIG (R-IV), Senapati.	Senapati District, Senapati.	Addl. SP-Kangpokpi, Kangpokpi.	Nil	3	Yes	Yes	Yes	Yes	Broadband
56.	- do -	- do -	-do-	SDPO-Senapati, Senapati.	Nil	3	Yes	Yes	Yes	Yes	Broadband
57.	- do -	- do -	-do-	SDPO-Mao, Mao.	Nil	3	Yes	Yes	Yes	Yes	Broadband
58.	- do -	- do -	-do-	Dy.SP(CAR), Senapati	Nil	3	Yes	Yes	Yes	Yes	Broadband
59.	IGP (Zone-III), PHQ Babupara, Imphal.	DIG (R-IV), Senapati.	Ukhrul District, Ukhrul.	Addl. SP-Ukhrul, Ukhrul.	Nil	3	Yes	Yes	Yes	Yes	Broadband
60.	- do -	- do -	-do-	SDPO-Ukhrul, View Land (Ukhrul).	Nil	3	Yes	Yes	Yes	Yes	Broadband

61.	- do -	- do -	-do-	SDPO-Chingai, SP Office, Ukhrul.	Nil	3	Yes	Yes	Yes	Yes	Broadband
62.	- do -	- do -	-do-	SDPO-Phungyar, SP Office, Ukhrul.	Nil	3	Yes	Yes	Yes	Yes	Broadband
63.	- do -	- do -	-do-	SDPO-Jeshami, SP Office, Ukhrul.	Nil	3	Yes	Yes	Yes	Yes	Broadband
64.	- do -	- do -	-do-	Dy.SP(CAR), SP Office, Ukhrul.	Nil	3	Yes	Yes	Yes	Yes	Broadband
65.	IGP (Int.), Manipur, CID Head Qtrs. Imphal.	DIG(Int/NAB), Manipur, CID Head Qtrs. Imphal	SP CID (VIP Security), Maniur, CID Head Qtrs., Imphal.	Addl.SP/CID (VIP Security), Imphal.	Nil	3	Yes	Yes	Yes	Yes	Broadband
66.	- do -	- do -	SP CID (Spl. Branch), Maniur, CID Head Qtrs., Imphal.	Addl.SP CID(OSD), CID Head Qtrs.,	Nil	3	Yes	Yes	Yes	Yes	Broadband
67.	- do -	- do -	SP CID (Tech. & Adm), Maniur, CID Head Qtrs.,	Dy. SP/CID (Stablishment), CID Head Qtrs.,	Nil	3	Yes	Yes	Yes	Yes	Broadband

			Imphal.								
68.	- do -	- do -	-do-	Dy. SP/CID (Verification), CID Head Qtrs.,	Nil	3	Yes	Yes	Yes	Yes	Broadband
69.	- do -	- do -	-do-	Dy. SP/CID (Bomb Disposal), CID Head Qtrs.,	Nil	3	Yes	Yes	Yes	Yes	Broadband
70.	- do -	- do -	-do-	Dy. SP/CID (Political), CID Head Qtrs.,	Nil	3	Yes	Yes	Yes	Yes	Broadband
71.	- do -	- do -	-do-	Dy. SP/CID (FIC), CID Head Qtrs.,	Nil	3	Yes	Yes	Yes	Yes	Broadband
72.	- do -	- do -	-do-	Dy. SP/CID (OSD), CID Head Qtrs.,	Nil	3	Yes	Yes	Yes	Yes	Broadband
73.	- do -	- do -	-do-	Dy. SP/CID (Special Branch), CID Head Qtrs.,	Nil	3	Yes	Yes	Yes	Yes	Broadband
74.	- do -	- do -	-do-	Dy. SP/CID (Special	Nil	3	Yes	Yes	Yes	Yes	Broadband

				Branch), CID Head Qtrs.,							
75.	- do -	- do -	-do-	Dy. SP/CID (Special Branch), CID Head Qtrs.,	Nil	3	Yes	Yes	Yes	Yes	Broadband
76.	- do -	- do -	-do-	Dy. SP/CID (Special Branch), CID Head Qtrs.,	Nil	3	Yes	Yes	Yes	Yes	Broadband
77.	- do -	- do -	-do-	Dy. SP/CID (Special Branch), CID Head Qtrs.,	Nil	3	Yes	Yes	Yes	Yes	Broadband
78.	- do -	- do -	-do-	Dy. SP/CID (Special Branch), CID Head Qtrs.,	Nil	3	Yes	Yes	Yes	Yes	Broadband
79.	- do -	- do -	-do-	Dy. SP/CID (Special Branch), CID Head Qtrs.,	Nil	3	Yes	Yes	Yes	Yes	Broadband
80.	- do -	- do -	-do-	Scientific	Nil	3	Yes	Yes	Yes	Yes	Broadband

				Officer-I, CID Head Qtrs.,							
81.	- do -	- do -	-do-	Scientific Officer-II, CID Head Qtrs.,	Nil	3	Yes	Yes	Yes	Yes	Broadband
82.	- do -	- do -	SP DGCR, Imphal	Dy.SP DGCR, Imphal	Nil	3	Yes	Yes	Yes	Yes	Broadband
83.	- do -	DIG CID(CB), Manipur, CID Head Qtrs. Imphal	CID(Crime Branch), Maniur, CID Head Qtrs. Imphal.	Dy. SP/CID (SCRB).	Nil	3	Yes	Yes	Yes	Yes	Broadband
84.	- do -	- do -	-do-	Dy. SP (Organised Crime)CID Head Qtrs., Imphal.	Nil	3	Yes	Yes	Yes	Yes	Broadband
85.	- do -	- do -	-do-	Dy. SP (Economic Offences Wing)CID Head Qtrs., Imphal.	Nil	3	Yes	Yes	Yes	Yes	Broadband
86.	- do -	- do -	-do-	Dy. SP (Fingeer Print), CID Head Qtrs., Imphal.	Nil	3	Yes	Yes	Yes	Yes	Broadband

87.	- do -	Director Wireless	Joint Director (Communication), MPW	ATMO Imphal West	Nil	3	Yes	Yes	Yes	Yes	Broadband
88.	- do -	- do -	-do-	ATMO Imphal East	Nil	3	Yes	Yes	Yes	Yes	Broadband
89.	- do -	- do -	-do-	ATMO Bishnupur	Nil	3	Yes	Yes	Yes	Yes	Broadband
90.	- do -	- do -	-do-	ATMO Thoubal	Nil	3	Yes	Yes	Yes	Yes	Broadband
91.	- do -	- do -	-do-	ATMO Chandel	Nil	3	Yes	Yes	Yes	Yes	Broadband
92.	- do -	- do -	-do-	ATMO Churachandpur	Nil	3	Yes	Yes	Yes	Yes	Broadband
93.	- do -	- do -	-do-	ATMO Senapati	Nil	3	Yes	Yes	Yes	Yes	Broadband
94.	- do -	- do -	-do-	ATMO Ukhrul	Nil	3	Yes	Yes	Yes	Yes	Broadband
95.	- do -	- do -	-do-	ATMO Tamenglong	Nil	3	Yes	Yes	Yes	Yes	Broadband
96.	- do -	- do -	Joint Director (Adm.), MPW, Imphal	ATMO (Adm.) Imphal	Nil	3	Yes	Yes	Yes	Yes	Broadband
97.	IGP(Adm), PHQ, Imphal	DIG(HQ/Adm)), PHQ, Imphal	SP/SIT, Imphal	Dy.SP SIT-I, Imphal	Nil	3	Yes	Yes	Yes	Yes	Broadband

98.	-do-	-do-	-do-	Dy.SP SIT-II, Imphal	Nil	3	Yes	Yes	Yes	Yes	Broadband
99.	-do-	-do-	-do-	Dy.SP SIT-III, Imphal	Nil	3	Yes	Yes	Yes	Yes	Broadband
100.	-do-	-do-	-do-	Dy.SP SIT-IV, Imphal	Nil	3	Yes	Yes	Yes	Yes	Broadband
101.			SP CMTW Imphal	Addl.SP CMTW, Imphal	Nil	3	Yes	Yes	Yes	Yes	Broadband
102.	Director MPTC, Pangei	Dy.Director MPTC, Pangei		Addl.SP MPTC, Pangei	Nil	3	Yes	Yes	Yes	Yes	Broadband
103.	-do-	-do-		Dy.SP MPTC	Nil	3	Yes	Yes	Yes	Yes	Broadband
104.	-do-	-do-		Dy.SP MPTC	Nil	3	Yes	Yes	Yes	Yes	Broadband

IT Hardware Availability & Requirement at District Police Offices &Imphal-based SP level offices

Sl. No.	Zone	Range	District	Computers Available	No. of Computers Required	Printer required (Yes/No)	Multi Functional Device Required (Yes/No)	UPS Required (Yes/No)	Site Preparation Required (Yes/No)	Type of Connectivity Required
1.	IGP (Zone-I), PHQ Babupara, Imphal.	DIG (R-I), SP/IMP(W) Office Complex, Imphal.	Imphal West District, Imphal.	Nil	10 clients including 1 Server	Yes	Yes	Yes	Yes	Broadband
2.	-do-	-do-	Imphal East District, Imphal	Nil	10 clients including 1 Server	Yes	Yes	Yes	Yes	Broadband
3.	-do-	DIG (R-II), Thoubal	Thoubal District, Imphal	Nil	10 clients including 1 Server	Yes	Yes	Yes	Yes	Broadband
4.	IGP (Zone-II), PHQ Babupara, Imphal.	DIG (R-III), 1st MR Complex, Imphal.	Bishnupur Disttrict, Bishnupur	Nil	10 clients including 1 Server	Yes	Yes	Yes	Yes	Broadband

5.	IGP (Zone-II), PHQ Babupara, Imphal.	DIG (R-III), 1st MR Complex, Imphal.	Churachandpur District	Nil	10 clients including 1 Server	Yes	Yes	Yes	Yes	Broadband
6.	IGP (Zone-II), PHQ Babupara, Imphal.	DIG (R-IV), Senapati	Tamenglong District	Nil	10 clients including 1 Server	Yes	Yes	Yes	Yes	Broadband
7.	IGP (Zone-III), PHQ Babupara, Imphal.	DIG (R-IV), Senapati	Senapati District	Nil	10 clients including 1 Server	Yes	Yes	Yes	Yes	Broadband
8.	IGP (Zone-III), PHQ Babupara, Imphal.	DIG (R-IV), Senapati	Ukhrul District	Nil	10 clients including 1 Server	Yes	Yes	Yes	Yes	Broadband
9.	IGP (Zone-III), PHQ Babupara, Imphal.	DIG (R-II), Thoubal	Chandel District	Nil	10 clients including 1 Server	Yes	Yes	Yes	Yes	Broadband
10.	IGP(Int/NAB), CID HQ, Imphal.	DIG(Int/NAB)	SP/CID(SB)	Nil	10 clients including	Yes	Yes	Yes	Yes	Broadband

					1 Server					
11.	IGP(Int/NAB), CID HQ, Imphal.	DIG(Int/NAB)	SP/CID(VIP Security)	Nil	10 clients including 1 Server	Yes	Yes	Yes	Yes	Broadband
12.	IGP(Int/NAB), CID HQ, Imphal.	DIG(Int/NAB)	SP/CID(Tech & Adm)	Nil	10 clients including 1 Server	Yes	Yes	Yes	Yes	Broadband
13.	IGP(Int/NAB), CID HQ, Imphal.	DIG(Int/NAB)	SP/NAB	Nil	10 clients including 1 Server	Yes	Yes	Yes	Yes	Broadband
14.	IGP(Int/NAB), CID HQ, Imphal.	DIG(Int/NAB)	SP/DGCR	Nil	10 clients including 1 Server	Yes	Yes	Yes	Yes	Broadband
15.	IGP(Int/NAB), CID HQ, Imphal.	Director FSL, Pangei	Addl.Director FSL, Pangei	Nil	10 clients including 1 Server	Yes	Yes	Yes	Yes	Broadband
16.	IGP(Int/NAB), CID HQ,	Director Wireless	Jt.Director(Communication)	Nil	10 clients	Yes	Yes	Yes	Yes	Broadband

	Imphal.				including 1 Server					
17.	IGP(Int/NAB), CID HQ, Imphal.	Director Wireless	Jt.Director(Adm)	Nil	10 clients including 1 Server	Yes	Yes	Yes	Yes	Broadband
18.	IGP(Int/NAB), CID HQ, Imphal.	DIG/CID(CB), Imphal	SP/CID(CB)	Nil	10 clients including 1 Server	Yes	Yes	Yes	Yes	Broadband
19.	IGP(Adm), PHQ, Imphal.	DIG(HQ/Adm)PHQ, Imphal	SP(SIT)	Nil	10 clients including 1 Server	Yes	Yes	Yes	Yes	Broadband
20.	IGP(Adm), PHQ, Imphal.	DIG(HQ/Adm)PHQ, Imphal	SP(CMTW)	Nil	10 clients including 1 Server	Yes	Yes	Yes	Yes	Broadband
21.	IGP(Adm), PHQ, Imphal.	DIG(HQ/Adm)PHQ, Imphal	AIG Supertime	Nil	10 clients including 1 Server	Yes	Yes	Yes	Yes	Broadband

IT Hardware Availability& Requirement at Range Offices & Imphal-based DIG/Director level offices

Sl. No.	Zone	Range	Computers Available	No. of Computers Required	Printer required (Yes/No)	Multi Functional Device Required (Yes/No)	UPS Required (Yes/No)	Site Preparation Required (Yes/No)	Type of Connectivity Required
1.	IGP (Zone-I), PHQ Babupara, Imphal.	DIG (R-I), SP/IMP(W) Office Complex, Imphal.	Nil	4	Yes	Yes	Yes	Yes	Broadband
2.	-do-	-do-	Nil	4	Yes	Yes	Yes	Yes	Broadband
3.	-do-	DIG (R-II), Thoubal	Nil	4	Yes	Yes	Yes	Yes	Broadband
4.	IGP (Zone-II), PHQ Babupara, Imphal.	DIG (R-III), 1st MR Complex, Imphal.	Nil	4	Yes	Yes	Yes	Yes	Broadband
5.	IGP (Zone-II), PHQ Babupara, Imphal.	DIG (R-III), 1st MR Complex, Imphal.	Nil	4	Yes	Yes	Yes	Yes	Broadband
6.	IGP (Zone-II), PHQ Babupara, Imphal.	DIG (R-IV), Senapati	Nil	4	Yes	Yes	Yes	Yes	Broadband
7.	IGP (Zone-III), PHQ Babupara, Imphal.	DIG (R-IV), Senapati	Nil	4	Yes	Yes	Yes	Yes	Broadband
8.	IGP (Zone-III), PHQ	DIG (R-IV), Senapati	Nil	4	Yes	Yes	Yes	Yes	Broadband

	Babupara, Imphal.								
9.	IGP (Zone-III), PHQ Babupara, Imphal.	DIG (R-II), Thoubal	Nil	4	Yes	Yes	Yes	Yes	Broadband
10.	IGP(Int/NAB), CID HQ, Imphal.	DIG(Int/NAB)	Nil	4	Yes	Yes	Yes	Yes	Broadband
11.	IGP(Int/NAB), CID HQ, Imphal.	DIG(Int/NAB)	Nil	4	Yes	Yes	Yes	Yes	Broadband
12.	IGP(Int/NAB), CID HQ, Imphal.	DIG(Int/NAB)	Nil	4	Yes	Yes	Yes	Yes	Broadband
13.	IGP(Int/NAB), CID HQ, Imphal.	DIG(Int/NAB)	Nil	4	Yes	Yes	Yes	Yes	Broadband
14.	IGP(Int/NAB), CID HQ, Imphal.	DIG(Int/NAB)	Nil	4	Yes	Yes	Yes	Yes	Broadband
15.	IGP(Int/NAB), CID HQ, Imphal.	Director FSL, Pangei	Nil	4	Yes	Yes	Yes	Yes	Broadband
16.	IGP(Int/NAB), CID HQ, Imphal.	Director Wireless	Nil	4	Yes	Yes	Yes	Yes	Broadband
17.	Director MPTC	Dy.Director MPTC	Nil	4	Yes	Yes	Yes	Yes	Broadband
18.	IGP(Int/NAB), CID HQ, Imphal.	DIG/CID(CB), Imphal	Nil	4	Yes	Yes	Yes	Yes	Broadband

19.	IGP(Adm), PHQ, Imphal.	DIG(HQ/Adm)PHQ, Imphal	Nil	4	Yes	Yes	Yes	Yes	Broadband
20.	IGP(Adm), PHQ, Imphal.	DIG(HQ/Adm)PHQ, Imphal	Nil	4	Yes	Yes	Yes	Yes	Broadband
21.	IGP(Adm), PHQ, Imphal.	DIG(HQ/Adm)PHQ, Imphal	Nil	4	Yes	Yes	Yes	Yes	Broadband

IT Hardware Availability& Requirement at Zones /IG Offices & ADG & DG level offices

Sl. No.	Zone	Computers Available	No. of Computers Required	Printer required (Yes/No)	Multi Functional Device Required (Yes/No)	UPS Required (Yes/No)	Site Preparation Required (Yes/No)	Type of Connectivity Required
1.	IGP (Zone-I), PHQ Babupara, Imphal.	Nil	4	Yes	Yes	Yes	Yes	Broadband
2.	IGP (Zone-II), PHQ Babupara, Imphal.	Nil	4	Yes	Yes	Yes	Yes	Broadband
3.	IGP (Zone-III), PHQ Babupara, Imphal.	Nil	4	Yes	Yes	Yes	Yes	Broadband
4.	IGP (L&O-III), PHQ Babupara, Imphal.	Nil	4	Yes	Yes	Yes	Yes	Broadband
5.	IGP(AP&Ops), PHQ Babupara, Imphal.	Nil	4	Yes	Yes	Yes	Yes	Broadband

6.	IGP PHQ Babupara, Imphal.	Nil	4	Yes	Yes	Yes	Yes	Broadband
7.	IGP(Int/NAB), CID HQ, Imphal.	Nil	4	Yes	Yes	Yes	Yes	Broadband
8.	Director MPTC	Nil	4	Yes	Yes	Yes	Yes	Broadband
9.	IGP(Int/NAB), CID HQ, Imphal.	Nil	4	Yes	Yes	Yes	Yes	Broadband
10.	IGP(Adm), PHQ, Imphal.	Nil	4	Yes	Yes	Yes	Yes	Broadband
11.	ADGP(AP&Trg), PHQ, Imphal	Nil	4	Yes	Yes	Yes	Yes	Broadband
12.	ADGP(LO), PHQ, Imphal	Nil	4	Yes	Yes	Yes	Yes	Broadband
13.	ADGP(HG), PHQ, Imphal	Nil	4	Yes	Yes	Yes	Yes	Broadband
14.	ADGP(Int), PHQ, Imphal	Nil	4	Yes	Yes	Yes	Yes	Broadband
15.	DGP Manipur, PHQ, Imphal	Nil	10	Yes	Yes	Yes	Yes	Broadband

Existing Capacity Building Infrastructure (RTC, DTC & PTC)

Training Institution Type	No. of Training Institutions	District/Unit/Centre site preparation
District HQ (Imphal West, Imphal East, Thoubal, Bishnupur, Churachandpur, Chandel, Senapati, Tamenglong & Ukhrul)	9	9
Unit/Centre (CID SB, CB, DGCR & NAB)	4	4
RPCTC	0	0
SCRB, CID HQ Imphal	1	1
RTC/PTC(MPTC, Pangei)	1	1

N.B : Hardwares for training institutions have been procured separately under Capacity Building scheme.

5. CORE APPLICATION SOFTWARE (CAS)

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

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

5.1 CAS (CENTER)

CAS (Centre): CAS (Centre) would cater to the functionality that is required at the GOI level (by MHA and NCRB). CAS (Centre) would enable NCRB to receive crime and criminals' related data from States/UTs in order to organize it suitably to serve NCRB's requirements and to provide NCRB with the analysis and reporting abilities to meet their

objective as the central level crime and criminals' data repository of the nation. This would address the crime- and criminals-related information needs of MHA, NCRB, the Parliament, and central government ministries and agencies, citizens and citizen groups. CAS (Centre) also facilitates the flow if crime and criminals information across States/UTs on a need-basis. CAS (Centre) will be developed and deployed at NCRB. Also, CAS (Centre) is expected to interface with external agencies such as passports, transport authorities, etc.

Overview of Services for CAS (Center) :

i. State-SCRB-NCRB Data Transfer and Management

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

ii. Crime and Criminal Reports

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

iii. Crime and Criminal Records and Query Management

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

iv. Talaash Service

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

v. Person of Interest

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

vi. Registered Vehicle and Vehicle of Interest Service

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

vii. Publication Service

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

viii. NCRB Citizen Interface

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

ix. NCRB Interface for RTI

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

5.2 CAS (STATE)

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

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

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

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

- It will lay special emphasis on the functions at police stations with focus on usability and ease of use of the application
- It will be designed to provide clear and tangible value to key roles at the Police Station: specifically the SHO (Station House Officer), the IO (Investigation Officer) and the Station Writer.
- It will be event- and role-driven
- It will be content/forms-based, with customized forms based on requirements
- It will be a flexible application, event and role-driven system where actions on a case can be taken as required without rigid sequence / workflows
- It will eliminate the need for duplicate and redundant entry of data, and the need for repetitive, manual report preparation – this freeing valuable time and resources for the performance of core police functions
- It will be intelligent and help police perform their roles by providing alerts, highlighting key action areas, etc.
- Ability to view and exchange information amongst Police Stations, between Police Stations and other Police formations and with external entities including citizens
- Reporting and data requirements of higher offices must be met at the State Data Centre/SCRB level and not percolate to the police station level.
- Central facilitation and coordination; but primarily driven and owned by States/UTs where States/UTs can configure and customize the CAS for their unique requirements without the intervention of the central entity

Overview of Services for CAS (State)

i. Citizens Portal Service

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

ii. Petition Management Service

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

iii. Unclaimed/Abandon Property Register Service

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

iv. Complaint and FIR Management Service

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

v. PCR Call Interface and Management Service

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

vi. Investigation Management Service

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

vii. Court and Jail Interface and Prosecution Management Service

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

viii. Crime and Criminal Records and Query Management Service

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

ix. Police Email and Messaging Service

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

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

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

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

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

xii. State-SCRB-NCRB Data Transfer and Management Service

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

xiii. State CAS Administration and Configuration Management Service

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

xiv. User Help and Assistance Service

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

xv. User Feedback Tracking and Resolution Service

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

xvi. Activity Log Tracking and Audit Service

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

xvii. User Access and Authorization Management Service

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

DEVELOPMENT OF CCTNS CORE APPLICATION SOFTWARE (CAS)

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

CAS (State) would be built as a platform at NCRB addressing the core requirements of the Police Station to provide a basic framework to capture and process crime and criminal information at the police station while providing the States/UTs with the flexibility to build their state specific applications around it and in addition to it. CAS (State) will be provided to States and UTs for deployment. Each State/UT would customize the CAS according to their unique requirements and thereafter commission the same. A bulk of the functionality would

be added at States/UTs' discretion and would be added as extensions to the CAS (State) by the System Integrators (SI) chosen by the States/UTs.

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

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

ROLE OF SOFTWARE DEVELOPMENT AGENCY (SDA) IN SUPPORTING CAS

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

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

Each of these activities is detailed out below.

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

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

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

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

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

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

Technical Program Management of Implementation of CAS (State)

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

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

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

point of contact will be responsible for addressing queries from an SI and in meeting SLA targets (in responding to States/UTs' needs).

• *Helpdesk Support*: SDA shall provide Helpdesk support to the State Sis during customization, deployment and stabilization phases with 8 contact hours (during normal business hours of 10 AM to 6 PM), 6 days (Monday through Saturday, both included). The SDA shall deploy a team of at least 5 qualified and certified resources in NCRB to address the questions from the SIs.

• *Deployment Scripts*: The SDA shall develop the necessary deployment scripts to deploy CAS (State) in States/UTs and provide the same to State.

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

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

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

• 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.

6. SCOPE OF THE PROJECT

6.1 Geographical Scope

The locations across which the application and the bundle of services shall be rolled out (police stations, circle offices and other higher offices) during the implementation is as follows :

Phase I		**Phase II**	
PS/units	Higher Offices	PS/units	Higher Offices
47	118	54	34

During the first phase of the applications, CCTNS would be rolled out in the four valley districts covering around 47% of the PSs and 78% of the higher offices. The roll out would include installation and commissioning of hardware, connectivity, other infrastructure and associated services (such as handholding).

The district wise list of PSs / Units is provided below:

Sl. No.	**Name of Police Station**	**Name of District / Unit**
1.	Imphal PS	Imphal West – 10 P.Ss
2.	City PS	
3.	Singjamei PS	
4.	Lamphel PS	
5.	Sekmai PS	
6.	Wangoi PS	
7.	Mayang Imphal PS	
8.	Patsoi PS	

9.	Lamsang PS	
10.	Women PS	
11.	Porompat PS	Imphal East – 11 PSs
12.	Heingang PS	
13.	Lamlai PS	
14.	Irilbung PS	
15.	Jiribam PS	
16.	Sagolmang PS	
17.	Andro PS	
18.	Yangangpokpi PS	
19.	Borobekra PS	
20.	Thoubal Dam PS	
21.	Women PS	
22.	Bishnupur PS	Bishnupur – 9 PSs
23.	Moirang PS	
24.	Nambol PS	
25.	Kumbi PS	
26.	Loktak PS	
27.	Keibullamjao PS	
28.	Phougakchao (Ithai) PS	
29.	Arong Nongmaikhong PS	
30.	Women PS	
31.	Thoubal PS	
32.	Lilong PS	

33.	Yairipok PS	Thoubal – 13 PSs
34.	Kakching PS	
35.	Waikhong PS	
36.	Sugnu PS	
37.	Pallel PS	
38.	Heirok PS	
39.	Khongjom PS	
40.	Hiyanglam PS	
41.	Wangoi PS	
42.	Nongpok Sekmai PS	
43.	Women PS	
44.	Mao PS	Senapati – 14 PSs
45.	Senapati PS	
46.	Kangpokpi PS	
47.	Tadubi PS	
48.	Saikul PS	
49.	Gamnom Sapermeina PS	
50.	New Keithelmanbi PS	
51.	Willong PS	
52.	Dzuko PS	
53.	Tungjoi PS	
54.	Purul PS	
55.	Phaibung PS	
56.	Chalwa PS	

57.	Women PS	
58.	Moreh PS	Chandel – 7 PSs
59.	Tengnoupal PS	
60.	Molcham PS	
61.	Chakpikarong PS	
62.	Chandel PS	
63.	Khengjoi PS	
64.	Women PS	
65.	Churachandpur PS	Churachandpur – 7 PSs
66.	Singhat PS	
67.	Parbung PS	
68.	Henglep PS	
69.	Thanlon PS	
70.	Sangaikot PS	
71.	Women PS	
72.	Ukhrul PS	Ukhrul – 11 PSs
73.	Litan PS	
74.	Jessami PS	
75.	Somdal PS	
76.	Chingai PS	
77.	Kasom Khullen PS	
78.	Phungyar PS	
79.	Chassad PS	
80.	Shangsak PS	

81.	Sanakeithel PS	
82.	Women PS	
83.	Tamenglong PS	Tamenglong – 7 PSs
84.	Tousem PS	
85.	Nungba PS	
86.	Khoupum	
87.	Noney PS	
88.	Tamei PS	
89.	Women PS	
90.	NAB PS	NAB Manipur – 1 PS
91.	CID (CB)(EOW) PS	CID(HQ), Imphal – 1 PS
92.	Anti - Human Trafficking Unit	Imphal West – 1 Unit
93.	Anti - Human Trafficking Unit	Imphal East – 1 Unit
94.	Anti - Human Trafficking Unit	Thoubal – 1 Unit
95.	Anti - Human Trafficking Unit	Bishnupur – 1 Unit
96.	Anti - Human Trafficking Unit	Chandel – 1 Unit
97.	Anti - Human Trafficking Unit	Churachandpur – 1 Unit
98.	Anti - Human Trafficking Unit	Tamenglong – 1 Unit
99.	Anti - Human Trafficking Unit	Senapati – 1 Unit
100.	Anti - Human Trafficking	Ukhrul – 1 Unit

	Unit	
101.	Special Juvenile Police Unit	Imphal West – 1 Unit

The Higher Offices to be covered are given below :

Sl. No.	Name of Offices	Name of District
1.	SDPO Imphal	Imphal West
2.	SDPO Lamphel	
3.	SDPO Singjamei	
4.	DySP Traffic	
5.	DySP Reserve	
6.	DySP Interrogation Cell	
7.	DySP CDO-I	
8.	DySP CDO-II	
9.	DySP Ops	
10.	SDPO Prorompat	Imphal East
11.	SDPO Lamlai	
12.	SDPO Jiribam	
13.	DySP CDO-I	
14.	DySP CDO-II	
15.	DySP CAR	
16.	DySP Ops	
17.	SDPO Bishnupur	
18.	SDOP Moirang	

19.	DySP CAR	Bishnupur
20.	DySP CDO-I	
21.	DySP CDO-II	
22.	DySP Ops	
23.	DySP Loktak Protection Force	
24.	SDPO Thoubal	Thoubal
25.	SDOP Sugnu	
26.	SDPO Kakching	
27.	DySP CDO-I	
28.	DySP CDO-II	
29.	DySP CAR	
30.	DySP Ops	
31.	SDOP Mao	Senapati
32.	SDOP Senapati	
33.	DySP CAR	
34.	SDPO Moreh	Chandel
35.	SDPO Chandel	
36.	DySP CAR	
37.	SDPO Churachandpur	Churachandpur
38.	SDPO Thanlon	
39.	DySP CAR	
40.	SDPO Ukhrul	Ukhrul
41.	SDPO Chingai	
42.	SDPO Jessami	

43.	SDPO Phungyar	
44.	DySP CAR	
45.	SDPO Tamenglong	Tamenglong
46.	SDPO Tousem	
47.	SDPO Nungba	
48.	SDPO Tamei	
49.	DySP-I/CID (Verification)	CID (Special Branch)
50.	DySP-II/CID (State Bomb Disposal)	
51.	DySP-III/CID (Establishment)	
52.	DySP-IV/CID (Political)	
53.	DySP-V/CID (OSD)	
54.	DySP-VI/CID (FIC)	
55.	DySP-VII/CID (Special Branch)	
56.	DySP-VIII/CID (Special Branch)	
57.	DySP-IX/CID (Special Branch)	
58.	DySP-X/CID (Special Branch)	
59.	DySP-XI/CID (Special Branch)	
60.	DySP-XII/CID (Special Branch)	
61.	DySP-XIII/CID (Special Branch)	
62.	Scientific Officer –I	
63.	Scientific Officer –II	
64.	DySP-CID(SCRB)	CID(Crime Branch)
65.	DySP-CID(Economic Offence Wing)	
66.	DySP-CID(Organised Crime)	

67.	DySP-CID(Finger Print)	
68.	DySP-I/SIT	SIT
69.	DySP-II/SIT	
70.	DySP-III/SIT	
71.	DySP-IV/SIT	
72.	DySP-I/MPTC	MPTC
73.	DySP-II/MPTC	
74.	DySP (DGCR)	DGCR
75.	ATMO, MPW, Imphal West	MPW
76.	ATMO, MPW, Imphal East	
77.	ATMO, MPW, Bishnupur	
78.	ATMO, MPW, Thoubal	
79.	ATMO, MPW, Chandel	
80.	ATMO, MPW, Churachandpur	
81.	ATMO, MPW, Senapati	
82.	ATMO, MPW, Ukhrul	
83.	ATMO, MPW, Tamenglong	
84.	ATMO, MPW, Headquarters	
85.	Addl. SP (L&O) Imphal West	
86	Addl. SP (Ops) Imphal West	
87	Addl. SP (Prosecution) Imphal West	
88	Addl. SP (L&O) Imphal East	
89	Addl. SP (Ops) Imphal East	
90	Addl. SP (Jiribam) Imphal East	

91	Addl. SP (L&O) Bishnupur
92	Addl. SP (Ops) Bishnupur
93	Addl. SP (L&O) Thoubal
94	Addl. SP (Ops) Thoubal
95	Addl. SP (Kangpokpi) Senapati
96	Addl. SP (L&O) Chandel
97	Addl. SP (Ops) Chandel
98	Addl. SP (Churachandpur)
99	Addl. SP (Ukhrul)
100	Addl. SP (Tamenglong)
101	Addl. SP/CID(VIP Security) CID(Special Branch
102	Addl. SP/CID(OSD) CID(Special Branch
103	Addl. SP/CMTW
104	Addl. SP/MPTC
105	SP Imphal West
106	SP Imphal East
107	SP Bishnupur
108	SP Thoubal
109	SP Senapati
110	SP Chandel
111	SP Churachandpur
112	SP Ukhrul
113	SP Tamenglong
114	SP CID(Special Branch)

115	SP(VIP Security)
116	SP(Tech & Adm.)
117	SP CID(Crime Branch)
118	SP CMTW
119	SP NAB
120	SP SIT
121	SP DGCR
122	Joint Director (Administration) MPW
123	Joint Director (Communication) MPW
124	Addl. Director FSL
125	AIG (MPS Supertime post) PHQ
126	DyIGP (Range-I)
127	DyIGP (Range-II)
128	DyIGP (Range-III)
129	DyIGP (Range-IV)
130	DyIGP (AP-I)
131	DyIGP (AP-II)
132	DyIGP (ADM)
133	DyIGP (INT&NAB)
134	DyIGP (CID-CB)
135	Dy. Director (MPTC) (DIG rank)
136	Director (MPW)
137	Director (FSL)
138	IGP (Zone-I)

139	IGP (Zone-II)
140	IGP (Zone-III)
141	IGP (INT &NAB)
142	IGP (Ops , Armed , Provisioning)
143	IGP (Trg. HR, RTI)
144	IGP (ADM)
145	Director (MPTC)
146	IGP (LO-III)
147	IGP – Not posted
148	ADGP (L&O)
149	ADGP (HG)
150	ADGP (INT)
151	ADGP (AP&TRG)
152	DGP

The following implementation strategy shall be adopted phase-wise:

Phase I (Valley-based)			
PS / Units	**Number**	**Higher Offices**	**Number**
Imphal West P.S	10	SDPO	11
Imphal East P.S	11	Dy. SP	43
Thoubal	13	ATMO	5
Bishnupur	9	Sc. Officer	2
Imphal-based NAB & CB	2	Addl. SP	14
Imphal West AHTU & Special Juvenile Police Unit	2	SP	12
TOTAL	**47**	AIG	1

		JD	2
		AD/FSL	1
		DIGP	10
		Dir. MPW	1
		Dir. FSL	1
		IGP's	10
		ADGP's	4
		DGP	1
		TOTAL	**118**

Phase II (Hill-based)			
PSs / Units	**Number**	**Higher Offices**	**Number**
Chandel	7	SDPO	14
Churachandpur	7	Dy. SP	4
Tamenglong	7	ATMO	5
Senapati	14	Addl. SP	6
Ukhrul	11	SP	5
AHTU (Churachandpur, Chandel, Senapati, Ukhrul, Tamenglong, Imphal East, Thoubal, Bishnupur)	8	**TOTAL**	**34**
TOTAL	**54**		

6.2 Functional Scope

This section provides the detailed functional requirements that will be covered under the project. It contains functional requirements at the different levels of the organization/s covering police stations and higher offices. This section also lists the functionality that the state wants specifically for itself.

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

Sl. No.	CCTNS Modules	Functionality Requirements
1.	**Registration Module**	LOGIN • Login GENERAL PETITION SERVICES • Submit General Service Petition • Prepare Response for Service Petition PROPERTY INFORMATION • Maintain (Enter/Update/Delete) Unclaimed/Abandoned Property Information BASIC COMPLAINTS • Register Complaint • Complete Registration • Close Complaint
2.	**Investigation Module**	CRIME RELATED • Capture Crime Details Form • Capture Chance Finger Prints • Capture Investigation Details • Prepare Remand Report or Judicial Custody Report • Prepare Arrest Card • Prepare Property Seize Form EXTERNAL AGENCIES RELATED • Prepare FPB/FSL/PME/MLC Request form • Capture FPB/FSL/PME/MLC Response Reports • Prepare Inquest Report • Inquest Report Received from Magistrate • Transfer Case to Different PS or Agency EXTERNAL AGENCIES RELATED • IO Alerts for Finishing a Particular Activity Before the Stipulated Time • Alerts and MIS for Senior Officers HELP FOR IO • Help: View Information on the Support Agencies • Help: View Check List Related to a Type of Case SUPPORT SERVICES • Document Management • Generate Reports • Secure Access
3.	**Prosecution Module**	COURT INTERFACE

		• Submit Trial-day Update • Split Case in case of Trial at Different Courts • Order for Investigation/Re-investigation REPORTS • Alerts and MIS for Senior Officers SUPPORT SERVICES • Document Management • Generate Reports • Secure Access
4.	**Navigation Module**	CASE VIEW • Multiple Case View HOME PAGES • IO Home Page • SHO Home Page • Duty Officer's Home Page • Court Constable's Home Page • Station Writer's Home Page • SSP & Senior Officers' Home Page
5.	**Search Module**	QUICK SEARCH ADVANCED SEARCH
6.	**Configuration Module**	ADMIN FUNCTIONS • Configure Acts/Sections • Configure Additional Data Elements Specific to the State Acts/Sections • Configure Castes/Tribes • Configure Courts/FSL/FPB • Configure Templates • Configure Case-specific Service Levels • Configure Users
7.	**Citizen Interface Module**	COMPLAINT BASED REGISTRATION • Register Complaint and Receive/Acknowledge QUERY BASED INTERFACING • Conduct a Query PROPERTY INFORMATION • Apply for a NOC from the Police • Status Check on a NOC Application • Provide General Feedback/Comments to the Police

The database of CCTNS will have a handshake with databases of other agencies of the Criminal Justice System viz. Juvenile Justice, E-Courts, Passport Authorities, Immigration, Visa, Foreigner Registration & Tracking, Economic Offences, Cyber Crime, Forensic & Finger Print Bureau Workflow.

A) REGISTRATION MODULE

Registration comprises of functionalities which gathers/stores the information and decides their importance/priority. All of these functionalities are performed by police personnel mainly on the inputs from civilians.

Registration Module
Login
General Petition Services
Submit General Service Petition
Prepare response for Service Petition
Property Information
Maintain (Enter/Update/Delete) Unclaimed/Abandoned Property Information
Basic Complaints
Register Complaint
Complete Registration
Close complaint

i) Login

The system which is used by multiple users has access restrictions. The CCTNS system has a login page which takes the user to different function screen on basis of their role. This user decides to interact with the CCNTS system. The users allowed to interact with the system are the police staff with roles as SHO, IO, DO, SW, CC, DEO. The input is user name and password. On the basis of the role assigned to particular user the system display the functional screen.

On Successful login, the user is to taken to the following page:

a) If role is mapped to IO/SHO the user is taken to landing page for viewing case investigation and registration.

b) If role is mapped to Station writer the user is taken to landing page for viewing case investigation and registration.

c) If role is mapped to court constable the user is taken to landing page for viewing functionality for court cases.

d) If role is mapped to data entry operator the user is taken to Landing page for data entry.

ii) General Petition Services

Application

Citizens can submit General Petitions to the police station, which caters to different requirements of citizens where police interface or support is required for those requirements. This gets initiated when a citizen approaches a police station with a request. When citizen has a request, he can come to police station where his request (written, email, etc.) is attended and the proper action is taken. Police Personnel logs on to the system to enter the details. The entry is marked in register and the incoming entries are marked in Daily Diary. System saves the petition for the citizen and generates a unique number for the petition submitted. The petition is filed and assigned to police personnel. System tags the assigned police personnel to the unique number generated for the petition submitted by the citizen.

Prepare Response

This describes the sequence of steps to generate a response to those general petitions submitted by Citizens to the police station. Like no objection certificates. It caters to different requirements of citizens where police interface or support is required for those requirements. This is response to general petition submitted by a citizen. This data will be further used to

a) Generation of reports/certificate required by the citizen.

b) Sends notification to various authorities whose response is needed.

c) The output of the request is marked in Despatch register.

The police personnel navigate to the screen with the tasks on general petitions. He checks if all the information required has been provided. The personnel can then decide either to

a) Generate reports/certificate for the said petition. The system shows the user the interface for report generation and once the report is generated, returns to the main screen (Landing page).

b) Decide to assign the task to other person/authority. System sends a notification to the concerned authority or person. System returns to the main page (Landing page).

c) Cancel the process and the system returns to the landing page.

iii) Maintain Unclaimed/Abandoned Property Information

This facilitates capturing details of unclaimed or abandoned property. The first thing which is noted is whether the property is numbered or unnumbered. Accordingly (property is numbered or unnumbered) the details of the property are entered and further steps are taken. For example, a pamphlet is made about the attributes of the item(s) found. Details like acts and sections, local acts, section code, seizure place, seizure date/time, reported by, witness information and other property details are captured. The input is manual in terms of entering the details and the search is system search which results in item wise output. This consists of the following scenarios:

a) Information capture regarding property

b) Perform searches related to unclaimed or abandoned property

c) Associates unclaimed or abandoned property information to a case

d) If the match is found, the owner is traced and he is informed about the property. If the match is not found, a six month wait time is scheduled, if no one comes back in the six months' window, the auction is arranged and the property is sold and the entries are made accordingly.

The police personnel logs into the system to enter the details of the registration. The details of the property are to be entered or modified in the system. The police personnel navigate to the new case registration screen and fill in the required details i.e.

a) GD entry,

b) Date, time of incident

c) Place of incident

d) Investigation officer

e) Duty officer

f) Acts

g) Sections.

The following information about the property is also entered by the user

a) Property Category

b) Property Type

c) Description

d) Property Status

e) Value

f) Other details specific to property.

For automobile property the following details to be captured specifically:

a) Insurance Company

b) Insurance Date

c) Validity of the insurance

System captures (if required) human organs in property type i.e. Eye, Kidney, others. The user chooses property status out of the following statuses:

a) Involved in Crime

b) Stolen

c) Recovered

System assigns separate numbers viz.

a) Unclaimed Property Number

b) Investigative property number

Depending upon whether the property seized is unclaimed property or it is seized during investigation. The user opens the witness tablet and enters the following information:

a) Name with Alias

b) Sex

c) Parentage

d) Marital Status

e) Age (year of Birth)

f) Nationality information

g) Socio economic Status

h) Address

i) Jurisdiction

j) Other details specific to Witness

The user saves the data and System generates registration number if it saves the data for the first time else it just saves the data. If the user cancels, the system takes the user to complete registration. If the user closed the complaint, System mark the complaint as closed. If the user wants to search for a case, the personnel can start from the landing page or the advanced

search page. The system displays the registration page in the view mode and the user can do the following activities:

a) Choose to modify the following details:

i. Property Category

ii. Property Type

iii. Description

iv. Property Status

v. Value

vi. Other details specific to property.

b) Choose to associate the case with another case through the registration screen.

c) Checks if the waiting period has elapsed (registration date is 6 month prior to the current date), and marks the property as ready for auction.

iv) Register Complaint

This describes the sequence of steps to register a complaint submitted by citizens in the police station. In some other cases police may register an incident (police may do it on its own discretion). This may include complaints for crime such as thefts, robbery, murder or some disputes over property. It may also include some incidents like discovery of unclaimed property or unidentified dead body. This gets initiated by the police personnel who is in charge of registering complaints or have been designated by SHO. This is in response to complaint of a citizen. All the inputs are entered manually by the user. Citizen has filed a petition based on an incident that has already occurred and needs to be reported. The user (Police Personnel) logs onto the system and navigates to the screen meant for the recording the complaint and chooses a new case. User assigns acts, sections, & local Acts. The user also provides any information specific to the assigned acts/sections/local acts. System decides if a complaint is of type cognizable or noncognizable. It determines by the acts & sections (CrPC, IPC, & local) applied whether cognizable/non-cognizable. System captures if it is a juvenile crime. The user fills the Complaint Information and Case Specific information

a) Occurrence place/ date/ time/ location

b) Reported place/ date/ time/ location

c) Registration place/ date/ time/ location

d) Direction/distance from PS

e) Mode of information submission Oral, Written, Suo-Moto, Court, Senior Officer

f) Duty officer.

g) Preliminary inquiry officer

h) Investigation officer

The user fills in brief facts of complaint reported by the informer. The user also fills in the details about :

a) Victim(s) (if applicable)

b) Accused (if applicable)

c) Witness (if applicable)

System captures victim details in the standard format [There should be a provision of feeding the age in days for a newly born child]

System captures accused details are in the standard format

System captures witness details are in the standard format

User fills in the information about property

a) Property (Type, Lost/ Missing/ Stolen, Seized, Recovered, Abandoned, Involved in Crime)

b) User enters Insurance details in case of automobile property

c) Details: Type of property and specific information

d) User enters details of human organs in property type i.e. Eye, Kidney, others

e) Additional details in case of seizure

System captures property details are in the standard format.

Case specific information

a) Missing Person details in case of missing person case

b) If injured, MLC details

c) If death, MLC & PME details

d) If unidentified dead body, physical details (captured as victim's details)

e) If deserter, deserter details (captured as accused details)

f) If accident, vehicle and driver information

System captures case specific information

a) Missing Person details in case of missing person case

b) If injured, MLC details

c) If death, MLC & PME details

d) If unidentified dead body, physical details (captured as victim's details)

e) If deserter, deserter details (captured as accused details)

f) If accident, vehicle and driver information

g) System captures time of body found in case of un natural death

h) System captures (if required) zero MLC or zero UDR

i) System captures kind of weapon used in MLC

j) System captures the cause of un natural death

k) System captures date of desertion in case of deserter case.

l) In case of unnatural death case system captures number of photographs provided during post-mortem

m) In case of unnatural death case system captures that in case of dowry/custody death is videography captured or not?

n) In case of unnatural death case system captures whether fingerprints/impressions are preserved or the unclaimed dead body

o) In case of unnatural death case system captures whether viscera is preserved or not.

p) In case of unnatural death case system captures post-mortem registration number

User fills in the further details sub-category of the case for further analysis if possible. Ex: Petty Issues, Missing Items, Deaths, Accidents, Nuisance, Land Issues, Cheating, Financial Issues, Hurts, e-Community Issues, Suicides, Matrimonial, Property Offences, Family Disputes, Loss Of Property, Industrial Issues, Crime Against Women. The user is taken to the complete registration page.

If the user cancels the process, the system goes to the landing page.

Complete Registration

Complaint registration is critical function of a police station. This functionality will elucidate the different functions the user can perform after he/she has gone through the steps in registration. This will enumerate the options which are created after user is done with registration. The controlling user is either constable or data writer present at police station. This flow is the logical step that follows "Maintain Complaint". The data is stored in the system and complaint is segregated in different categories. If an Investigating Offices has to

be assigned it is done by higher office like SHO. An SHO can also assign some critical cases to himself. This flow will have six scenarios:

1. Save & quit
2. Save & Create FIR
3. Save & Create NCR
4. Save & Create Complaint Report (for other cases)
5. Generate Zero FIR (case or trial happens in the area of jurisdiction)
6. Generate final report of Juvenile Crime

A complaint has been initiated and the user (police personnel) has logged onto the system to enter the details. The User navigates to the screen to decide on the options for completing the registration process.

System provides the user with 6 options

1. Save & Quit
2. Save & Create FIR
3. Save & Create NCR
4. Save & Create Complaint report
5. Generate zero FIR
6. Generate final report for Juvenile crime

If the user chooses to 'Save & Quit', then the User can go through multiple iterations on the complaint (MPR/UDR/Deserter's Case) initiated. The user may export the report to a PDF, Word or Excel. The complaint is saved. If the user chooses "Save & Create FIR", then a FIR number is provided to the complaint. User can save and proceed to generate a report for FIR. The complaint is saved or submitted and is assigned to an investigation officer. The investigation process can be started. If the user chooses to "Save & Create NCR (Non cognizable report)", then User can save and generate an NCR. If the user chooses to "Save & Create Complaint Report", then User can save and generate a report for specific complaint type. If the user chooses to "Generate and Zero FIR", then System prompts user to update the status of Zero FIR generated by prompting user to enter the name of the Police Station to which FIR is assigned. User assigns the report to the relevant police station and fills in the details. System notifies the relevant police station. If the user chooses to "Save & Create Juvenile Crime Report", then User can save and generate a report for Juvenile Crime type as

per the Rule No. 11 of "The Juvenile Justice (Care and Protection of Children) Act, 2090 as amended in 2006". If the user chooses to quit without saving, then System does not save the changes made after login and returns to the previous screen (Case Specific Details form).

Close Complaint

This functionality will facilitate the closing of a complaint for those complaints which do not proceed for investigation. The input for this flow comes from Maintain Complaint form and after that when that particular complaint does not proceed to investigation and the Charge Sheet or Final Report (even for the cases which do not get investigated) is generated as an output right after the preliminary complaint. The owner of this flow is either the Police Constable or the Data Writer in the police station. If the user chooses to close complaint, then System assigns status 'closed' to the complaint. Save and close (without generating the report). If the user chooses to create report and close the complaint, then Systems saves the complaint, generates report and closes the complaint. If the user cannot close the complaint, if there is an erroneous situation (for example – the reason for closing the complaint is not given), then Pop up with the error message.

B) INVESTIGATION MODULE

When a complaint is registered by a complainant, it is taken forward by an Investigation Officer to conduct investigation activities and which involved building further to the information gathered during the registration phase. It mainly involves a defined processes bound to procedural methodologies elucidated by Indian law.

Investigation Module
Crime Related
Capture Crime Details Forms
Capture Chance Finger Prints
Capture Investigation Details
Prepare Remand Report or Judicial Custody Report
Prepare Arrest Card

Prepare Property Seizure Form
External Agencies Related
Prepare FPB/FSL/PME/MLC Request Form
Capture FPB/FSL/PME/MLC Response Reports
Prepare Inquest Report
Inquest Report received from Magistrate
Transfer case to different P.S/Agency
IO alerts for finishing a particular activity before stipulated time
Alert & MIS for Senior Officers
Reports
Prepare Final Report or Charge Sheet
Help for IO
View information on Support Services
View Checklist for a type of Case
Support Services
Document Management
Generate Reports
Secure Access
Support Services

i) Crime Related

Capture Crime Details Form

This will capture those details of a criminal case which are not captured during registration e.g. the details of crime that are gathered from the scene. Investigation Officer captures the crime details. The input is manual. As per the output new progress events are generated and the data is stored in to the system. The user logs onto the system with the designated role and a case (FIR/MPR/UDR) have been filed. The IO visits the place of occurrence of offence for the first time and records findings. Based on the role of the user navigates to the designated form. System displays the information captured through FIR/Any Other Report. User captures details of the permission granted by the court to proceed with the investigation.

System displays a form requiring the actor to enter the court name and the date that the permission was granted. These details only need to be filled in the case of an NCR. User enters the following details:

a) Select the date of Crime Details Capture.

b) Case Diary Number

c) Select and enter the details related to the sections (Major and Minor are common throughout the country)

Major Heads which comes under the previously entered Act and its Section

Minor Heads which comes under the previously entered Major Heads

Local involves the section or article for state or municipality.

d) Enter the methods which are used in the case and the special features related to the case. Depends on Sections selected. Methods need to be made more comprehensive (compare to CIPA) for each section so as to be able to cover all possible scenarios.

e) Select Place Type

f) Select Suspected Gangs

g) Enter Implements Used

h) Select Motive of Crime

i) If victim exists then capture victim details

j) If accused exists then capture accused details

k) If witnesses exists then capture witnesses' details

l) Enter description of place of occurrence

m) If the property is involved that is damage or stolen. User adds the property details in the property details form. Depends on Sections selected.

n) (Optional) User fills in the necessary details for the immovable property.

o) (Optional) User fills in the necessary details for the jewellery

p) (Optional) User fills in the necessary details for the automobile(s)

q) (Optional) User fills in the necessary details for the currency

r) (Optional) User fills in the necessary details for the explosives.

s) (Optional) User fills in the necessary details for the electronics.

t) (Optional) User fills in the necessary details for the Documents

u) (Optional) User fills in the necessary details for the Fire Arms.

v) (Optional) User fills in the necessary details for the drugs.

w) (Optional) User fills in the necessary details for the Cultural property.

x) (Optional) User fills in the necessary details for the other/miscellaneous property.

The user saves the data. System validates the data to check if the data is in the correct format. If the data is incorrect System prompts the user. The unfilled and mandatory data is highlighted. Any inconsistencies are also highlighted. If the data is correct System saves the data and notifies user.

Capture Chance Finger Prints

Whenever there is a crime the finger prints are taken from the scene. This finger prints are analysed by finger prints (FP) experts of police. This report is send to police station this is feed into the system. This describes the process of storing the finger print reports send to police station by the finger prints experts of police. The input here is the report from FP expert. For the output the information is stored in the CCTNS systems. The person responsible for entering the data can be the Police Constable, Data Writer or the Police Finger Print Expert. The user logs into the system with the designated role and the case (FIR/MPR/UDR) have been filed. User enters the chance finger print details:

1. Date of Capture

2. Captured By Scan finger print image and attach to a particular Finger Print detail.

System captures the finger print capture details entered by the police personnel. System captures the scanned image and displays a preview which is clickable and can be enlarged to see full image. Link finger print to accused and appear in the Accused Details section. Link finger print to victim and appear in the Victim Details section. User can capture two entries (default) for capturing of finger print details. System displays a form which has two default sections (forms) for entering finger print details. User can add more instances of finger print capture via an add button. User saves the details and quits. If the user quits without saving the use case details, System does not save the details edited after the last save action.

Capture Investigation Details

After a case is registered in the police station the investigation is carried out. This is normally a multistage process. The details may get updated several times. This enables the user to add

the details of the case and keep tracks of the progress of the case. The input is data entered manually or the link to pre-existing data in the system. User stores many different details:

1. Storing any new detail
2. Presenting charge sheet in court
3. Actions on the comments of authority

The persons responsible for entering the data are the SHO or the IO. The user logs into the system with the designated role and the case (FIR/MPR/UDR) have been filed. IO visits the place of occurrence of offence for the first time and records findings. Based on the role, the user navigates to the designated form and the System displays the information captured through FIR/Any Other Report. User adds the relevant details and saves the data. The details can be new information on

1. Case Status
2. Witness
3. Accused
4. Victim
5. Property
6. Motive
7. Place of occurrence
8. Changes in section through alteration memo

Progress event is generated and a log is maintained in case of a change. Relation of the surety with the accused will have to be captured in the case of accused being released on bail. The accused when proclaimed as an offender will require information regarding sender of information, sending date to gazette, date of publication etc. In the case of deserter cases information such as date of custody/arrest in addition to handling of accused to army should be captured under the accused section. Property status should include a "Miscellaneous" option for when it is not included in a crime and nor is it stolen. If the user wants to generate a charge sheet, then the user fills in the necessary details to generate the charge sheet and generate the charge sheet. If the user wants to add remarks on the case, System displays a text box for the display of comments. After actor adds the remark system saves the remark. These remarks may or may not be the response on the comments/remarks of senior officer/Authority. If the user chooses to select a case status for the current case being investigated, the System displays 4 options:

a) Details collected

b) Evidence Collected

c) Charge sheet created

d) Arrest made

Each of these statuses is mutually independent. If user selects the first 3 options, then The Case is updated with the status selected. If user selects the Arrest made option, then The System displays the following sub-statuses with details and number of accused under each sub status

a) Bail

b) Arrest

c) Fugitive

User selects a particular sub-option and updates this information. User saves and Charge sheet details are updated and charge sheet is generated and the data stored. If the user cancels, then the system returns to the state prior to this form.

Prepare Arrest Card

If any Arrest/Surrender takes place during investigation, the details are captured. These details are termed as arrest card. On the basis of evidence – sufficient evidence – cognizable offence – the arrest is made and hence an arrest card is prepared. This use case outlines the steps to prepare the arrest card. The input data is entered manually and the data stored. The output is the arrest card. Time, place of arrest is noted and when an arrest is made – the nearest relative of the arrested person is informed about the arrest. Subsequent to that, a personal search is conducted for the arrested person and if there are some items found, entry of those items is made in the memo. Daily diary entry is made for the arrest and other (associated) police stations are informed about the arrest. After this, the arrested person is produced in the court within 24 hours and can be taken in remand if required after that.

The persons responsible for entering the data are either the IO or the SHO. The user logs into the system with the designated role and the case (FIR/MPR/UDR) have been filed. IO visits the place of occurrence of offence for the first time and has recorded findings. Charge sheet

details have been updated and charge sheet is generated. User opens the relevant case and opens the Arrest Form associated with it and the System populates the basic data entered for the accused. User enters the arrest related info like

a) Date and Time of Arrest

b) Name of the police personnel who made the arrest

System stores the data on clicking the save button. CCTNS shall have to include the computer serial number of the accused (Currently missing from CIPA).

User enters the personal details of the arrested

a) Name

b) Father's Name

c) Age (Date of Birth)

d) Address

System stores the data on clicking the save button. User enters the details of the nearest relative informed

a) Name of the relative

b) Relation to the arrested

c) Address of the Relative

System stores the data on clicking the save button. User enters the personal search details about the arrested

a) Details of money found with arrested

b) Details of any objectionable material (arms, drugs, explosives etc)

System stores the data on clicking the save button. User enters the miscellaneous details about the arrested person and the System stores the data on clicking the save button. If the arrested person has to be presented before magistrate, the user enters the details and the system stores the data on clicking the save button.

If the arrested person has to be taken on remand, the user enters the details and the System stores the data on clicking the save button. If the user cancels, then the system returns to the state prior to this form.

Prepare Remand Report or Judicial Custody Report

This describes the sequence of steps to create a remand or a judicial custody report. An accused person when arrested or surrenders will have to be presented in front of a magistrate within a period of 24 hours. The magistrate can then decide the period during which the accused can be sent into police remand for questioning related to the ongoing investigations. The magistrate may also decide on sending the accused into the custody of the court (i.e. Jail) for providing adequate security or surety for grant of a bail in bailable offences and for a period which the court decides in nonbailable cases. The investigation officer can input details related to the decision of the court which relate to the accused and the current case being investigated. The input is manual and shall include details of the court's decision (i.e. Judicial Custody, Police Remand) in addition to the duration of the period during which the accused is to remain in custody. The output shall consist of the report which the user can export or print and shall serve as a reference for the ongoing investigation. The person responsible for entering the data is the IO. Accused is presented in front of a court during the course of the investigation of a case and is ordered to be taken into judicial custody or police remand. User with the designated role has logged into the system to update these details. The User navigates to the screen to update judicial custody or police remand related details. System displays a form with some fields pre-populated. e.g. Police Station, District, Investigation Officer, Date, Case Diary No etc. The system shall allow the user to update fields relating to the judicial custody or police remand whichever the case may be.

a) Custody type (Police remand or judicial custody)

b) Date on which accused was presented in front of the court

c) Name and type of court

d) Date up to which the accused is to remain in custody

e) Name of Jail

The name of the jail shall be enterable only if the accused is sent to judicial custody. User enters details relating to the court decision and saves this information. System updates remand/judicial custody information relating to the on-going investigation. If the User chooses to print the results displayed, the system shall make available a printer friendly format of the report for the user.

If the User chooses to export the report to a Spreadsheet or a PDF, the system shall export the

results in the format selected.

Prepare Property Seizure Form

During the process of investigation there are instances when the property is seized this may happen when the property is disputed, when it is used as an instrument in crime, to put pressure on accused. This form is used to note down the details. The police may seize the property in case of

a) If a property is found unclaimed.
b) If a crime is committed and
c) In case of a court of order

This flow outlines the steps to enter the relevant data in case a property is seized. The input data is entered manually which is equivalent to the recovery memo (created by police personnel). This data is stored in the system. Time, place of arrest is noted and when an seizure is made if there is a witness its details are also noted. Daily diary entry is made for the any seizure and other (associated) police stations are also informed. The persons responsible for entering the data are either the IO or the data writer. User successfully logs on to the system with the designated role and the Case (FIR/MPR/UDR) has been filed. IO records findings. User opens the relevant case and open the Property Seizure Form associated with it. System populates the basic data entered for the accused. User enters the seizure related info like

a) Date and Time of Seizure
b) Name of the police personnel who made the seizure
c) Place of seizure
d) Police station
e) Who is the owner of property

System stores the data on clicking the save button. User enters the property details of the arrested

a) Whether the proper is serializable or not
b) Type
c) Estimated Cost
d) Condition

e) Accused Details

f) Other details

System stores the data on clicking the save button. If the User enters the witness details, System stores the data on clicking the save button. Witness may be one or many. If the user cancels, then the system returns to the state prior to the form.

ii) External Agencies Related

Prepare FPB/FSL/PME/MLC/RTO/Excise Request Form

The flow describes the sequence of steps to create a request for cases which require the assistance of external agencies such as the Forensic Sciences Lab or the Finger Print Bureau in addition to hospitals, if a post mortem is warranted or if it is a Medico Legal case. An ongoing investigation might require the FPB to match a set of finger prints from the scene of the crime to ascertain the identity of the perpetrators. The investigations might also result in the seizure of property which shall be sent to the Forensic Sciences Lab for analysis. In the case of post mortems or medico legal cases the assistance of a hospital shall be required. Vehicles involved in an accident case might require verification from the RTO. In addition verifications from the Excise officer might be required in the case of Excise Cases. The User shall be able to create a specific type of request based on the requirement. The input is manual. The output shall consist of the request form, a hardcopy of which shall be sent to the concerned agency along with related artifacts/evidence. This request form is prepared on the order of SP or Magistrate. The flow consists of the following scenarios:

1. Request for Finger Prints Bureau (FPB)
2. Request for Forensic Sciences Lab (FSB)
3. Request for a Post Mortem Enquiry (PME)
4. Request for a Medico Legal Case (MLC)
5. Request for vehicle verification from RTO
6. Request for verification from Excise officer

The person responsible for entering the data is the IO. The investigation of a case by police personnel requires the assistance of an external agency. User successfully logs on to the system with the designated role to create a request for the case being investigated. The User navigates to the screen to create a FPB/FSL/PME/MLC request. System displays a form with

some fields pre-populated. e.g. Police Station, District, Investigation Officer, Date, Case Diary No etc. System provides the User 6 options

1. Request for Finger Prints Bureau (Default)
2. Request for Forensic Sciences Lab
3. Request for Post Mortem Enquiry
4. Request for Medico Legal Case
5. Request for RTO verification
6. Request for verification from Excise Department

If the user chooses "Request for Finger Prints Bureau (Default)", then User enters required information and saves it. System stores information relating to the request made to the FPB. If the user chooses to export the request form to a word document, or a PDF, the system shall export the request form in the format selected by the user. If the user chooses to print the request form displayed, the system shall make available a printer friendly format of request form. If the User chooses to create a request for the Forensic Sciences Lab (FSL), the system displays a form requesting for inputs including:

a) Information on property seized

b) Details of FSL the seized property is sent to

c) Name of officer through whom the property was sent

User enters required information and saves it. System stores information relating to the request made to the FSL. If the User chooses to create a request for a Post Mortem Examination (PME), the system displays a form requesting for inputs including:

a) Details of Hospital the dead body is sent to

b) Name of officer through whom the dead body was deposited

User enters required information and saves it. System stores information relating to the request made for a PME. If the User chooses to create a request for a Medico Legal Case (MLC), the system displays a form requesting for the following inputs:

a) Details of Hospital the MLC is sent to

b) Name of officer through whom the MLC was deposited in Hospital

User enters required information and saves it. System stores information relating to the MLC request. If the User chooses to create a request for RTO, the system displays a form requesting for inputs including:

a) Information on vehicles

b) Details of RTO the seized vehicle is sent to

User enters required information and saves it. System stores information relating to the request made to the RTO. If the User chooses to create a request for verification from the Excise department, the system displays a form requesting for inputs relating to the excise case at hand. User enters required information and saves it. System stores information relating to the request made to the Excise Department.

Prepare FPB/FSL/PME/MLC response reports

The flow describes the sequence of steps to create a response report after external agencies have sent across details of their findings related to the investigation. Police personnel could receive a fingerprints matching report from the FPB/NCRB, property analysis report from the FSL, post mortem report from the concerned doctor and a statement from the Injured person (when deemed fit by the doctor) in the case of medico legal cases. The User shall be able to create a specific type of response report based on the requirement. The input is manual. The output shall consist of the response report. The use case consists of the following scenarios:

1. Finger Prints Bureau (FPB) Response Report
2. Forensic Sciences Lab (FSB) Response Report
3. Post Mortem Enquiry (PME) Response Report
4. Medico Legal Case (MLC) Response Report
5. Vehicle verification RTO Response Report
6. Excise officer verification Response Report

The person responsible for entering the data is the IO. Police personnel receive inputs relating to an investigation from the external agencies. User successfully logs on to the system with the designated role to create a response report. The User navigates to the screen to create a FPB/FSL/PME/MLC response report. System displays a form with some fields pre-populated. e.g. Police Station, District, Investigation Officer, Date, Case Diary No etc. System provides the User 6 options

1. Finger Prints Bureau Response Report(Default)
2. Forensic Sciences Lab Response Report
3. Post Mortem Enquiry Response Report
4. Medico Legal Case Response Report
5. RTO verification Response Report

6. Excise Department verification Report

If the user chooses Finger Prints Bureau Response Report, User enters the required information and saves it. System stores information relating to the response report from FPB. If the User chooses to export the response report displayed to a word document, or a PDF, the system shall export the report in the format selected. If the User chooses to print the response report displayed, the system shall make available a printer friendly format of the report. If the User chooses to attached a scanned image of the actual report, the System shall store the scanned image of the report for later retrieval.

If User chooses to create a Forensic Sciences Lab (FSL) response report, the system displays a form requesting for inputs including:

a) Information on property seized

b) Details of FSL the seized property is sent to (defaults to entry made on request)

c) Brief description of the property analysis report received from the FSL

User enters the required information and saves it. System stores information relating to the FSL response report. If the User chooses to create a Post Mortem Examination (PME) response report, the system displays a form requesting for inputs including:

a) Details of Doctor who performed the PM

b) Date on which the PM was conducted

c) Brief description of the Cause of Death

User enters the required information and saves it. System stores information relating to the PME response report. If the User chooses to create a Medico Legal Case (MLC) response report, the system displays a form requesting for the following inputs:

a) Examination Date

b) Discharge Date

c) Statement (by the injured) Date

d) Brief description of injuries

User enters the required information and saves it. System stores information relating to the MLC response report. If the User chooses to create a RTO Vehicle Inquiry response report, the system displays a form requesting for the following inputs:

a) Verification Date

b) Vehicle verified (Y/N)

c) Details of findings

User enters the required information and saves it. System stores information relating to the RTO response report. If the User chooses to create a Excise verification response report, the system displays a form requesting for the following inputs:

a) Verification date

b) Excise officer

c) Verification details

User enters the required information and saves it. System stores information relating to the Excise verification response report.

Prepare Inquest Report

This flow elaborates the form details to be filled by investigation officer regarding the inquest report. Inquest report is prepared for any dead body found (humans and animals both). This flow facilitates Investigation officer to fill in the details which are required regarding sending of inquest report. The input form about inquest report sent is filled by IO. All the details are noted regarding the dead body like – if the person was hurt, what are the details of the clothing etc – called as Panchnama. The dead body is then sent to post-mortem. Output is closing of inquest report sent to magistrate progress event so that further changes are not possible. If the findings after the post-mortem are different than the conclusions beforehand, then using the alteration memo the changes are updated. The persons responsible for entering the data are either the IO or the SHO. User successfully logs on to the system with the designated role and the Case (FIR/MPR/UDR) has been filed. IO visits the place of occurrence of offence for the first time and has recorded findings. User lands on the page to fill inquest details and the System pops up the default case details. User enters the physical details

a) Details of the wound

b) Details of the clothes

c) Details of the personal belongings

If the dead body has been sent for post mortem, User enters the details in the system. If the report has been sent to the magistrate, User enters the details in the system. If the user cancels, the system returns to the state prior to the form.

Inquest Report Received from Magistrate

This flow elaborates the scenario when an inquest report (with magistrate's comments) is received by an investigation officer. This is for special circumstances – when magistrate creates the inquest report (like death in police or judicial custody) or death of lady within 7 yrs of marriage. Dead body sent to CMO for PM, then attached to case diary. The input is a commented report received from the magistrate. The output is a submitted 'inquest report received from a magistrate' progress event. The persons responsible for entering the data are either the IO or the SHO. User successfully logs on to the system with the designated role and the Case (FIR/MPR/UDR) has been filed. IO visits the place of occurrence of offence for the first time and has recorded findings. Inquest report form has been filled and sent to Magistrate. User lands on the page to fill inquest report details received from the magistrate. System pops up the default case details (and inquest details). User enters the details about the magistrate

a) Magistrate Code

b) Magistrate Name

User enters the details about the report

a) Report Date

b) Magistrate Remarks

User saves the data.

If the user cancels, the system returns to the state prior to the form.

Remarks from Officer

Officers may comment on the cases. Their remarks may be related to the progress of case or in the advisory capacity. The system will facilitate capturing the remarks of an officer who wants to oversee a case and comment or highlight a point for the case. The input is in form of a search parameter (usually a case number) and the output is edited form for a particular case. This use case can have different scenarios of an office remarking the case for various categories, for example critical, important or low priority. A circle officer finds that something is to done differently, or if he decides to take a different approach for a particular investigation. The persons responsible for entering the data are the IO or data writer. User successfully logs on to the system with the designated role and the Case (FIR/MPR/UDR) has

been filed. A case has been registered. User opens the relevant case to view its details and the System populates details already entered for the case. User after going through the details may add the comments (by clicking on add comments button) and saves them. System stores the data. The comments can be viewed by IO. An alert is sent to the IO. If the user cancels, System returns to the state prior to the form.

Transfer a case to different Police Station

This flow completes the logical transfer of a case from one police station to another police station. After certain stages of investigation are complete and it is ascertained that this particular case does not fall under the jurisdiction of the present police station involved. The input is entered by present investigation officer who fills the details required for completing the transfer of a case from one police station to other. Output results with the case being assigned to a certain police station and all the relevant papers being sent to different police station via officer. The persons responsible for entering the data are the IO or data writer.

User successfully logs on to the system with the designated role and the Case (FIR/MPR/UDR) has been filed. The registration is complete. Users open the relevant case and the System populates the basic data. User chooses the option to assign it to a different police station, System stores the data on clicking the save button. User enters the details needed for the transfer of case.

a) Date:

b) Transfer Type:

c) Reason:

d) To Investigation Officer:

e) To state:

f) District:

g) Police Station:

h) To Agency: (depending on case type)

System stores the data on clicking the save button. If the user cancels, System returns to the state prior to the form.

Alerts & MIS for Senior Officers

For the purpose of notify or getting approval, senior officers needed to be informed. For example if a senior officer is assigned a crucial case or if some grave crime has taken place in his area so he is notified through the alerts. This flow describes the required steps performed to generate alerts for senior officers The input is in the form of system assignments during course of investigation or registration. Output is an alert when a senior officer logs on to the system. The persons responsible for entering the data can be SHO, Senior Officers or any police staff. User successfully logs on to the system with the designated role and the Case (FIR/MPR/UDR) has been filed. IO records findings. User may set the dates the date for the task with a brief task description in the calendar. For court cases where the SHO/ Other police staff attention is needed the date with task list is stored with court appointment schedule by a third party. System notifies the User on its mobile devices on the dates mentioned. System displays the task to be performed on the Landing page. User can view the alerts on its landing page. If there is a serious offence or any information that primary user should be given. The secondary users set it in the system. System sets the alert on the User's landing page. System sends the notification on the mobile device. If the user cancels, System returns to the state prior to the form.

Alerts for IO: Finishing a particular activity before a stipulated time

An IO works on multiple cases simultaneously. Investing officer has to be informed of certain activities. IO must be made aware of deadlines to enable him/her finish certain tasks before stipulated timeframe e.g. filing a charge sheet. This flow generates the required alerts through system for an Investigation Officer The input for the flow are any triggers generated by events such as firing of charge sheet or an assignment of a duty which an IO has to perform (within a stipulated time). Output is an alert when the IO logs on to the system. Alerts are about crime in the area. The persons responsible for entering the data can be IO or any police staff. User successfully logs on to the system with the designated role and the Case (FIR/MPR/UDR) has been filed. IO records findings. User may set the dates the date for the task with a brief task description in the calendar. For court cases where the IO presence is needed the date with task list is stored with court appointment schedule by a third party. System stores the data. System notifies the User on its mobile devices on the dates mentioned. System displays the task to be performed on the Landing page. User views the

alerts on its landing page. If there is a serious offence or any information that primary user should be given. The secondary users set it in the system. System sets the alert on the User's landing page. System sends the notification on the mobile device. If the user is not present on the mobile device, System returns to the state prior to the form.

iii) Reports

Prepare Final Report or Charge Sheet

This flow generates the final report after investigation. There can be different types of final reports – one of them is Charge Sheet. Depending on the case type and on the findings in the investigation a certain type of Final Report is generated. The use case describes the steps for preparation of Final Report / Charge Sheet. According to sufficient evidence and findings of the investigation the final report is created. A case can be closed based on the fact that it has not progressed much and for three months' time it had been inactive. The input entered in form of case type and other details. Output results with generation of Final Report after which changes are not possible. The persons responsible for entering the data are the IO or data writer. User successfully logs on to the system with the designated role and the Case (FIR/MPR/UDR) has been filed. The registration is complete. Investigation process is complete. User opens the relevant case and view the case details including progress events. System populates the details of the case. User may adds/changes the details e.g. accused details. User adds the following while generating the charge sheet for first time

a) F.R Type:

b) Original/Supplement (replace by Supplement Number in subsequent charge sheets)

c) Court Name:

d) Court Type:

The user generates the report. If the user cancels, System returns to the state prior to the form.

iv) Help

View information on the Support Agencies

IO requires information on various sources to proceed on the case. Any help to guide him with information to define his responsibilities and interfaces and services available from

external agencies would save his time and help an IO to perform efficiently. Flow gets initiated by the IO who is in charge of investigation. IO asks for help on a particular case type. A help document is displayed. The persons responsible for entering the data can be SHO or IO. User successfully logs on to the system. User clicks on help link. System displays the options.

a) Case specific checklist

b) Information on support agencies

If the User chooses 'Case specific checklist', System displays the options for the type of cases. If the User chooses the support agency, System displays the help on support agency.

a) Contact information

b) Area of responsibility.

User closes the help window.

View checklist related for a type of case

Criminal cases are sensitive issues; IO needs to take care of lot of details. There are instances where accused does not meet the right judgement because of inconsistencies in technical details. Checklist for charge sheet and other legal documents will assist IO to perform more effectively. This flow gets initiated by the IO who is in charge of investigation. IO asks for checklist on a particular case type. A document is displayed. The persons responsible for entering the data can be SHO or IO.

User successfully logs on to the system.

User clicks on help link. System displays the options.

a) Case specific checklist

b) Information on support agencies

If the User chooses 'Case specific checklist', System displays the options for the type of cases. If the User chooses the type of case, System opens checklist for the particular type of case.

User closes the help window.

C) PROSECUTION MODULE

Police personnel are in constant touch with the courts; hence it is imperative that CCTNS provides a conduit which is to be used while interfacing with court. This option allows the user to enter/update/view information about prosecution going on for the particular

Registration Type. System court interface gives a Court Case (CC#) number based on the Charge sheet filed. After the acknowledgement of the Final Report (usually Charge sheet) from the police the court gives the CC number and then the trial is executed giving next hearing date etc. Going even beyond when the case comes up for trial the output from court is registered like:

_ Next hearing date

_ Who will be examined

_ What needs to be produced

_ Summons

_ Warrants

_ Bail petition by accused

_ Accused details

Prosecution Module
Court Interface
Submit Trail-Day Update
Split case in case of trial at different courts
Order for investigation / re-investigation
Reports
Alerts & MIS for senior officers
Support Services
Document Management
Generate Reports
Secure Access

i) Court Interface

Submit Trial Day Update

This flow captures the activities on the trial day and those activities get updated at the end of the day through the system. This use case captures the details and updates which are executed after a charge sheet is submitted to the court. A charge sheet number is issued to the court. It also follows when the case comes up for the trial.

1. Details about the court happenings are updated (like how many witnesses came – who did not come) etc.

2. Details about the next dates are entered like (when is the next date – what is the responsibility of the court constable on the next date

a. Sort by trial date

b. Collect evidence to be produced

c. Alert the witnesses/IO/victim on the upcoming date

d. Produce accused

e. Any summons left un-served

f. Any warrants left un-executed

g. Summons to be served

h. Warrants to be executed

i. Bail petitions

j. Court ruling or final result

k. Next trial date

l. Assign summons and status

m. Assign warrants and status

n. Stand on bail petition and status

o. Appeal to be filed or not?

The persons responsible for entering the data can be court constable or the duty officer. User successfully logs on to the system with the designated role. Charge sheet has been filed and charge sheet details have been updated in the system. Post Charge sheet Court Execution Orders – details have been updated and the case is running for the trial. User loads the page to capture charge sheet number. System prompts to enter FIR details. User enters the FIR number. System prompts to enter charge sheet details. User associates the charge sheet details to the FIR

a) Charge sheet Number

b) Charge sheet Issue Date

c) Next Hearing Date

System associates the particular FIR number to the entered Charge sheet details (number, date and next hearing date). User saves the above form. Charge sheet details gets saved (and associated with an FIR).

User moves to the Trial Day Update screen. User can search a particular FIR number. System loads that particular FIR details and it also loads related charge sheet numbers to the FIR. First it loads a particular charge sheet number and it shows the other charge sheet numbers in form of the drop down. User makes updates relating to the progress made on the trial. User makes updates relating to the progress made on the trial.

Information includes

a) Summons to be served

b) Warrants to be executed

c) Any summons left un-served

d) Any warrants left un-executed

e) Bail petitions

f) Court ruling or final result

g) Next trial date

h) Assign summons and status

i) Assign warrants and status

j) Stand on bail petition and status including forfeiture/default of security in case bail is accepted

k) Appeal to be filed or not?

The System is updated with this information related to the trial. Summons/Warrants when executed details such as name, address of the person /official should be captured. Summon/Warrants when issued by the Court should capture department to which it is issued. Summon/Warrants when executed should include remarks on action taken. If the trial has been postponed to Next Date, User enters the details:

a) Reason for postponing the date

b) The next date when trial will resume

If the FIR has to be associated with a different charge sheet, User chooses a particular charge sheet number (from the drop down). System loads the details of that particular charge sheet (for the FIR associated). User can fill the details in the lower pane of the trial day update page. System stores the data. User enters the data for the particular charge sheet – associated to a particular FIR and then saves and quits. System returns to the state prior to the form.

Split Case

This flow splits the case logically in the system. A case is generally split when some of the accused in a case are not apprehended. The accused who have been apprehended are taken through prosecution proceeding and a separate case is created for those that have not been apprehended. Separate charge sheets shall be created for the split case. Another scenario where a case could get split is when the trial is to take place at separate courts (e.g. Accused in a case includes a juvenile who shall be tried in a juvenile court). Input comes from various findings that emerge during the investigation process. For example if it is found that out of a few accused, one is not arrested and the rest are then the case shall be split so that the original case can be taken to its logical conclusion and the apprehended accused can be taken through a trial. Output is a new case or a new charge sheet for which a separate investigation or prosecution process kicks off. The persons responsible for entering the data are the police constable or the data writer. Some accused in a case have not been apprehended and the case is to be prosecuted hence warranting a splitting of the case. Accused in a single case are to be tried in different courts. User successfully logs into the system to split the case. User navigates to the screen in order to split a case. The system shall display a form with the following fields which are pre-populated Police Station, District, Investigation Officer, Case number etc. The system shall prompt the user to enter the FIR number. User enters the FIR number. System loads FIR details along with all related charge sheet numbers (in a drop down). User selects a charge sheet. System displays details of the charge sheet along with the list of accused. The user shall be able to split the case (i.e. charge sheet) by selecting the accused for which a separate charge sheet is to be created. User selects accused and splits case. System creates a new charge sheet number and associates it to the existing FIR. The accused selected shall now be associated with the new charge sheet.

Order for Reinvestigation/investigation

Court may order that a particular case must undergo reinvestigation or may give the permission for investigation. The details related to reinvestigation/investigation are sent to investigation officer. This flow describes the required steps performed to update the system when the court has order for reinvestigation of case of have given the permission for investigation. Input is data entered by the User and the case. Output is an alert and the related updates in the system. The persons responsible for entering the data can be court constable or

any police staff. User successfully logs on to the system with the designated role. Charge sheet has been filed and the case is being prosecuted. User navigates to details of case and set it for investigation. System displays the screen. User adds the following information to case details

a) Name of the Court

b) Court order detail.

c) Court order date.

d) Court order received on date.

e) "Investigation handed over to" Investigating Officer details

System notifies the concerned officers. System changes the status of the case to "Under investigation". System displays the task to be performed on the investigative officer landing page. User closes the window and stops the flow. System returns to the state prior to the form.

ii) Reports

Alerts & MIS for Senior Officers

Senior officers need to be informed and have to receive alerts and events related to cases that are currently being prosecuted in the courts. For example a senior officer shall have to receive alerts on crucial cases related to some grave crimes that have taken place in his area and that are currently being prosecuted. The input is in the form of cases that are currently being prosecuted. Output is an alert when a senior officer logs on to the system. The persons responsible for entering the data are SHO, Senior Officers or Any police staff. User successfully logs on to the system with the designated role. Charge sheet has been filed and the case is being prosecuted. User may set the dates the tasks with a brief task description in the calendar. For court cases where the SHO/ Other police staff attention is needed the date with task list is stored with court appointment schedule by a third party. System stores the data. System notifies the User on its mobile devices on the dates mentioned. System displays the task to be performed on the Landing page. User views the alerts on its landing page. User closes the window and stops the flow. System returns to the state prior to the form.

D) NAVIGATION MODULE

Navigation comprises of functionalities which are present to the staff members as per their different roles. It describes the interface the system provides to the staff once they log into the system and the options present to each one of them.

Navigation Module
Case View
Multiple Case View
Home Pages
Station Writer Home Page
SHO Home Page
Duty Officer's Home Page
Court Constable's Home Page
SSP & Senior Officer's Home Page

i) Case View

Multiple Case View

A case can have several stages i.e. open case, closed case, re-opens cases, disposed case, unresolved case and case pending trial. A multiple view is needed for the summary of such cases in a single page. The flow describes the navigation from and to multiple case views. The user see in the summary the number of open case, closed case, re-opens cases, disposed case, unresolved case as per his role and user id after the login. User then navigates to the relevant screen using the hyperlinks on that page. The system displays the page for generating reports with the following criteria to select:

1. FIR No.
2. Select Area
3. Category
4. Date Range
5. Yearly/Monthly/Weekly

When the user clicks on the Generate Report, the result should be in the form of statistics and drill down should be allowed for the user to deep dive into the details. The reports should contain the following columns:

1. Till Last Month

2. This Month
3. Completed
4. Pending

The following types of cases will be shown as part of the report:

1. Open Cases
2. Closed Cases
3. Re-Opened Cases
4. Disposed Cases
5. Un-Resolved Cases

ii) Home Pages

IO Home Page

Once the IO logs into the system, he/she see the cases and various status and pending tasks. This use case elaborates on that process. This flow gets initiated by the IO who is in charge of doing investigation in response to complaint of a citizen. After login, IO sees the page from where he view the list of cases also those under trials, under investigation, re-opened case. User can also view the task he/she had set in calendar, the court appointments and the administration related tasks. Here the user may fill in the details manually to search. The use case branches to another use cases for investigation and search. The user has successfully logged onto the system with the designated role. The user navigates to the landing page of the IO. The following tabs are shown to the user:

1. Case List
2. Under Investigation
3. Under Trial
4. Re-Opened Cases
5. Calendar
6. Court Appointment Schedule
7. Administration

The user can choose any of the cases from the tabs and drill down to see the details for that case. A link should be provided to the following pages:

1. New Case Registration

2. General Service Request

A section should be provided where the user should be able to view alerts and upcoming events. The basic search and quick reports functionality should be available on the landing page. A button for advanced search should also be present in case the user wants to use that feature.

SHO Home Page

Once the SHO logs into the system, he/she see the cases and various status and pending tasks. This use case elaborates on that process. This flow gets initiated by SHO to view case based summary. After login SHO sees the page from where he can view the list of cases i.e. under trial cases, under investigation cases in his police station. User can also view the task he/she had set in calendar, the court appointments, the administration related tasks and the reports. Here the user may fill in the details manually to search. The use case branches to another use cases for investigation and search. The user has successfully logged onto the system with the designated role. The user navigates to the landing page of the SHO. The following tabs should be present:

1. Under Investigation
2. Under Trial
3. Calendar
4. Court Appointment Schedule
5. Administration
6. Report Summary

The user can choose any of the cases from the tabs and drill down to see the details for that case. A link should be provided to the following pages:

1. New Case Registration
2. General Service Request

A section should be provided where the user should be able to view alerts and upcoming events. The basic search and quick reports functionality should be available on the landing page. A button for advanced search should also be present in case the user wants to use that feature.

Duty Officer Home Page

Once the DO logs into the system, he needs the capability to register a complaint. This flow elaborates on that process. This flow gets initiated by DO to view the case summary. After login DO sees the page from where he can a register a case.

The user has successfully logged onto the system with the designated role. The user navigates to the landing page of the Duty Officer. The system shows the case registration page to the user. The user can enter the following details

1. Registration Date
2. Registration Time
3. IO Name
4. IO Code
5. GD Entry Number
6. Mode of Information
7. Date of Occurrence
8. Time of Occurrence
9. Place of Occurrence
10. Direction from PS
11. Distance from PS
12. Brief Fact about the case
13. Case Type
14. Act
15. Local Act
16. Section

The user saves and submits the information or chooses to reset the page.

A link should be provided to the following pages:

1. New Case Registration
2. General Service Request

A section should be provided where the user should be able to view alerts and upcoming events. The basic search and quick reports functionality should be available on the landing page. A button for advanced search should also be present in case the user wants to use that feature.

Station Writer Home Page

Once the station writer logs into the system, he/she needs the capability to generate reports and add data relevant to cases. This flow gets initiated by station writer to view the case summary. After login station writer sees the report summary. He/She may generate the crime report. He may navigate to a particular case to update it. The user has successfully logged onto the system with the designated role. The user navigates to the landing page of the Station Writer Home Page. The system displays the page for generating reports with the following criteria to select:

1. FIR No.
2. Select Area
3. Category
4. Date Range
5. Yearly/Monthly/Weekly

When the user clicks on the Generate Crime Report, the result should be in the form of statistics and drill down should be allowed for the user to deep dive into the details. The reports should contain the following columns:

1. Till Last Month
2. This Month
3. Completed
4. Pending

The following types of cases will be shown as part of the report:

1. Case Pending Arrests
2. Registered Cases
3. Charge Sheets
4. Court Disposal
5. Warrants
6. Summons
7. General Service Request

The user can choose to reset the fields. The user should also be able to navigate to Search and Advanced Search Pages from the landing page.

Court Constable Home Page

Once the court constable logs into the system, he/she has the duty to keep the track of the updates related to court proceedings. This flow elaborates on that process. This flow gets initiated by court constable to view the court appointment schedule. He/She also views the summary of charge sheet filed, case disposed by court, summons and warrants. Court constable is able to navigate to other pages that require updates to be recorded from the court i.e. warrants, summons, bail petitions, court notices, trial day updates, prosecution related updates. The user has successfully logged onto the system with the designated role. The user navigates to the landing page of the Court Constable Home Page. The system shows the user the following buttons to navigate to the respective pages:

1. Capture Charge Sheet Number
2. Trial Date Update
3. Arrest
4. Warrants
5. Summons
6. Court Notices
7. Bail Petitions

The user gets to view the following tabs on his home page:

1. Court Appointment Schedule
    a. Court
    b. Date & Time of Trial
    c. FIR No
    d. Case Description
    e. Activity
2. Report Summary
    a. Till Last Month
    b. This Month
    c. Completed
    d. Pending

The report summary will be shown for the following categories:

1. Charge Sheets
2. Court Disposal

3. Warrants
4. Summons

The user will have the choice to drill down to the particular case from the statistical data shown in the report.

SSP & Senior Officer's Home Page

Once the SSP or a senior officer logs into the system, he/she see the cases and various status and pending tasks. This flow elaborates on that process. This flow gets initiated by SSP or Senior Officer to view the summary of cases based on junior officer or type of cases. After login Senior Officer sees the page from where he can navigate to links i.e. open case, closed case, re-opened case, resolved case and disposed cases assigned to officers junior to him/her.

The user has successfully logged onto the system with the designated role. The user navigates to the landing page of the SSP & Senior Officer Home Page. The system displays the following button to the user to navigate to the respective pages:

1. Open Cases
2. Closed Cases
3. Re-Opened Cases
4. Resolved Cases
5. Disposed Cases

The user will have the facility to do basic search or can click on the advanced search button for more options for search. The system displays the page for generating reports with the following criteria to select:

1. FIR No.
2. Select Area
3. Category
4. Date Range
5. Yearly/Monthly/Weekly

When the user clicks on the Generate Report, the result should be in the form of statistics and drill down should be allowed for the user to deep dive into the details. The reports should contain the following columns:

1. Till Last Month
2. This Month

3. Completed
4. Pending

The following types of cases will be shown as part of the report:

1. Case Pending Arrests
2. Registered Cases
3. Charge Sheets
4. Court Disposal
5. Warrants
6. Summons
7. General Service Request

E) SEARCH MODULE

Police personnel are often required to retrieve case related information for review or updates. The CCTNS provides them with basic and advanced search capabilities that enable the quick retrieval of information on-demand. The ability to query on cases related to crime, accused details, modus operandi etc, provides the required flexibility and quick turnaround time that police personnel can benefit from. The ability to save and retrieve queries is also built into the system and this helps to reduce the number of keystrokes required.

Search Module
Search
Quick Search
Advanced Search

i) Quick Search

The flow describes the Quick search capabilities provided by the CCTNS system to an user which will enable the concerned to retrieve cases based on less comprehensive search criteria as compared to the Advanced Search functionality. The input is manual. The output shall consist of a list of cases pertaining to the criteria entered and is customizable by the user. The User shall be able to select a case to view its details. User successfully logs on to the system

with the designated role. The User navigates to the screen to search for a case(s). The System displays a form requesting the user for the following inputs

a) FIR No

b) Date Range

c) Beat Area

d) Interval (Year/Month/Week)

e) Type of case

User enters search criteria and executes search. The system shall display results which match the search criteria entered. The view shall default to that selected by the user (i.e. Suspect/Case). If the User chooses to change the view on the results page, The system shall switch between views depending on the view (Suspect/Case) selected. If the User chooses to save a query, System displays a form that enables an user to save a query. The User shall be prompted to enter a name and a path for the query that he wants to save. If the User chooses to export the results displayed to a word document, Spreadsheet or a PDF, The system shall export the results in the format selected by the user. All pages shall be exported and not only the current page (i.e. Pagination present). If the User chooses to print the results displayed, the system shall make available a printer friendly format of the results for the user. All pages shall be printed and not only the current page (i.e Pagination present). If the User chooses to view the details of a specific case, System lands to case details page. If the User chooses to reset the page to default, System refreshes page with search criteria set to default. All previously entered fields are wiped out.

Advanced Search

The flow describes the Advanced Search capabilities provided by the CCTNS system to an user which will enable the concerned to retrieve case s based on the type of crime, accused details, modus operandi and property details. e.g. IO or SHO decides to retrieve cases tied to a particular type of crime (murder, theft etc). The User (SHO/IO) enters a search criteria based on the option (Crime, Property etc) selected and shall also be provided the ability to store and load custom queries for easy retrieval. The input is manual. The output shall consist of a list of cases pertaining to the criteria entered and is customizable by the user. The User shall be able to select a case to view its details. The persons responsible for using the system

are SHO or IO. User successfully logs on to the system with the designated role. The User navigates to the screen to search for a case(s). System provides the User 5 options

a) Criminal Detail (Default)

b) Suspect Detail

c) Victim Detail

d) Modus Operandi

e) Property Detail

The system shall display the search criteria for the Criminal Detail option on page load. Most fields in the search criteria section shall be presented as a combo box providing the ability to search on multiple values for a single field. System shall provide the ability to execute a query based on search criteria entered on multiple options. If the User chooses to execute a search using the Criminal Detail option, the system shall display the search criteria for the Criminal Detail option on page load. Most fields in the search criteria section shall be presented as a combo box providing the ability to search on multiple values for a single field. A user shall have the ability to select multiple fields from an Available list. The user shall also be able to view results by Suspects or by Cases. If the User chooses to execute a search using the Suspect Detail option, the system shall display the search criteria for the Suspect Detail option on page load. Most fields in the search criteria section shall be presented as a combo box providing the ability to search on multiple values for a single field. A user shall have the ability to select multiple fields from an Available list. The user shall also be able to view results by Suspects or by Cases. If the User chooses to execute a search using the Victim Detail search criterion, the system shall display the search criteria for the Victim Detail option on page load. Most fields in the search criteria section shall be presented as a combo box providing the ability to search on multiple values for a single field. A user shall have the ability to select multiple fields from an Available list. The user shall also be able to view results by Suspects or by Cases. If the User chooses to execute a search using the Modus Operandi search criterion, The system shall display the search criteria for the Modus Operandi option on page load. Most fields in the search criteria section shall be presented as a combo box providing the ability to search on multiple values for a single field. A user shall have the ability to select multiple fields from an Available list. The user shall also be able to view results by Suspects or by Cases. If the User chooses to execute a search using the Property Detail search criterion, the system shall display the search criteria for the Property

Detail option on page load. Most fields in the search criteria section shall be presented as a combo box providing the ability to search on multiple values for a single field. A user shall have the ability to select multiple fields from an Available list. The user shall also be able to view results by Suspects or by Cases. If the User chooses to view a previously stored query, System refreshes page with search criteria set to values defined in the query. The user shall be able to make edits if required. If the User chooses to delete a previously stored query, System shall provide the user to ability to browse through previously stored queries and delete them. If the User chooses to preview the query, System shall display a summary of the search criteria selected or entered by the user on a different form. The screen shall have the following sections:

a) Criminal Detail

b) Suspect Detail

c) Victim Detail

d) Modus Operandi

e) Property Detail

When the User enters search criteria and executes search, the system shall display results which match the search criteria entered. The view shall default to that selected by the user (i.e. Suspect/Case).

If the User chooses to change the view on the results page, the system shall switch between views depending on the view (Suspect/Case) selected. If the User chooses to save a query, System displays a form that enables an user to save a query. The User shall be prompted to enter a name and a path for the query that he wants to save. If the User chooses to export the results displayed to a word document, Spreadsheet or a PDF, the system shall export the results in the format selected by the user. All pages shall be exported and not only the current page (i.e. Pagination present). If the User chooses to print the results displayed, the system shall make available a printer friendly format of the results for the user. All pages shall be printed and not only the current page (i.e Pagination present). If the User chooses to view the details of a specific case, System lands on to case details page. If the user executes a search without entering fields marked as mandatory, the system shall prompt the User to enter the mandatory fields and then execute a search. Search criteria previously entered shall remain intact.

F) CONFIGURATION MODULE

Configuration comprises of functionalities necessary for the administration to maintain the system on daily basis. They keep the data updated as per the needs of police department. They are in charge of providing data and functionalities to police staff based on their roles. This section describes the interface which the system provides to the administration staff once they log into the system.

Configuration Module
Admin Functions
Configure acts/sections
Configure additional data elements specific to the state acts/sections
Configure MO/Property-Types/Castes/Tribes/…
Configure Police Organization Structure (Districts, Ranges, Police Stations,..)
Configure Courts/FSL/FPB/…
Configure Templates
Configure Case-specific Service Levels
Configure Users

i) Configure acts/sections

The admin needs to manage and update the data periodically. Admin may add new acts and sections. Admin may delete the acts and sections. This flow gets initiated by the admin who is in charge of keeping the acts and sections updated as per the laws especially local laws. The data is manually entered into the system by the user. After the user saves the data the changes are reflected to the users. The admin are not allowed to make changes to the data (acts/sections) provided by the centre. User successfully logs on to the system with the administrator's role. The User navigates to the screen to make changes to Acts/Sections. The System displays a screen and prompts the user for the following inputs

a) Act Number

b) Section Number(s)

The System also provides the ability to add or delete an Act or Section. The Act number is a mandatory input where as the Section Number is an optional input. The User enters an Act number and optionally the Section number and chooses to add it. The System shall be updated with the new Act/Section(s). The system shall check to ensure that there are no changes being affected to existing Acts/Sections. The User enters an Act number and

optionally the Section number and chooses to delete it. System requests the user for confirmation to proceed with the deletion. The User confirms that he wants to proceed with the deletion. System deletes the Act/Section. The User enters an already existing Act number and optionally the Section number and chooses to add it. System shall throw an exception informing the user that he cannot proceed with the addition.

ii) Configure additional data elements specific to the state acts/sections

The admin needs to manage and update the data periodically. Admin may add new data elements specific to the state acts/sections. This flow gets initiated by the admin who is in charge of keeping the data elements acts and sections updated as per the laws especially local laws. New objects/ data elements may be added on the request of specific police stations. The data is manually entered into the system by the user. After the user saves the data the changes are reflected to the users. The admin are not allowed to make changes to the data specified by the centre. User successfully logs on to the system with the administrator's role. The User navigates to the screen to make changes to the data elements pertaining to Acts/Sections. The System displays a screen and prompts the user for the following inputs

a) Act Number

b) Section Number(s)

The Act number is a mandatory input where as the Section Number is an optional input. The User enters an Act number and optionally the Section number and executes a search. The System shall display the data elements pertaining to the Act number and the Section number entered. The user shall have the ability to add/delete data elements tied to the Act/Section. If the User chooses to add data elements, System displays a form that enables the user to add additional data elements. The User adds the data elements. System adds the additional data elements to the Act/Section. If the User selects data elements and deletes them, System deletes selected data elements tied to the Act/Section.

iii) Configure Property-Type/Castes/Tribes

The admin needs to manage and update the data periodically. Admin may add new Property-Type/Castes/Tribes. Admin may delete the Property-Type/Castes/Tribes. It is necessary to meet the demands posed by new cases and ever changing scenarios. This flow gets initiated by the admin as they are in charge of keeping the master tables for Property-

Type/Castes/Tribes updated as per the need of police. The data is manually entered into the system by the user. After the user saves the data the changes are reflected to the users. The admin are not allowed to make changes to the data (acts/sections) provided by the centre. User successfully logs on to the system with the administrator's role. The User navigates to the screen to manage and update data pertaining to Castes/Tribes etc. The System displays the following options:

a) Property-Type

b) Castes

c) Tribes

The system shall provide the ability to add/delete data tied to the options mentioned above. When the User selects a particular option, System displays the data currently tied to the particular option. If the User chooses to add data elements to the option, System displays a form allowing the user to add additional fields to an option. The User adds the elements to the option. The System is updated with this information and the data elements are added. If the User selects data elements from the option and deletes them, System is updated with this information and the data elements are deleted.

iv) Configure Police Organisation Structure (District Ranges Police Stations)

The admin needs to manage and update the data periodically. Admin may make changes to the police organisation structure as proposed by the local authorities. This use case gets initiated by the admin. New locations like districe, beats etc can be added. They may add beats or add new locations within the beat. They may also change the jurisdiction of district police ranges. They may add new roles for the station and assign them the functionalities. These are the changes which have to keep the system in sync with the actions of local governing bodies or the necessities presented due to some cases. The data is manually entered into the system by the user. After the user saves the data the changes are reflected to the users. The admin are not allowed to make changes to the data specified by the centre. User successfully logs on to the system with the administrator's role The User navigates to the screen to make changes to the police organisation structure. The system displays the following options

a) Update roles/functionalities for the station

b) Update Beat Information

c) Update jurisdiction

If the User chooses to update the roles/functionalities tied to the station, System displays the list of roles tied to the police station. The System shall provide the ability to add/delete roles. If the User chooses to Add a role, System shall display a form enabling the user to add a new role. If the User selects a particular role, The System shall display a form with the list of functionalities tied to the particular role. The System shall provide the ability to add/delete responsibilities. If the User chooses to Delete a role, System shall ask for confirmation before proceeding with the deletion. If the User chooses to update Beat Information, System shall request the user to enter the following information:

a) Beat Number

b) Beat Name

The System also provides the ability to add/delete a Beat. If the User executes a query on the Beat Number and Beat Name, System displays information about the beat such as the locations currently tied to the beat. The System shall provide the ability to add/delete locations from the beat. If the User chooses to add a beat, System displays a form requesting the user to enter a Beat Number and an appropriate Name for the beat they want to add. If the User chooses to delete a beat, System displays a form requesting to user to enter a Beat Number and an appropriate Name for the beat they want to delete. If the User chooses to update information related to jurisdiction, System shall display a form listing the current police stations/circles/districts etc in their jurisdiction. Granularity shall depend on jurisdiction. The System shall provide the ability to make additions/deletions to the list being displayed. If the User makes additions/deletions in the jurisdiction list, System is updated with this information.

v) Configure Court/FSL/FPB

The admin needs to manage and update the changes related to external agencies such as court, FSL, FPB, etc periodically. New agencies need to be updated as per the jurisdiction of the changes in their attributes (.e.g. addresses, names). This flow gets initiated by the admin they maintain the master tables that stored the data related to external agencies i.e. court, FSL, FPB. They may enter delete or change the details such as (names, addresses, and contact person) as per the changes taken place in local bodies. The data is manually

entered/changed into the system by the user. After the user saves the data the changes are reflected to the users. The admin are not allowed to make changes to the data specified by the centre. User successfully logs on to the system with the administrator's role. User navigates to configuration module of the Court/FSL/FPB. System displays the option to

a) Add a Court.

b) Add a FSL

c) Add a FPB

If the user chooses to add a court, User fill in the details of Court

a) Name of the Court

b) Name of Judge

c) Joining and End dates

d) Address

User stores the court. System goes to the previous screen. If the user chooses to add FSL, User fill in the details of FSL

a) Name of the FSL

b) Name of concerned person

c) Address

User stores the FSL. System goes to the previous screen. If the user chooses to add FPB, User fill in the details of FPB

a) Name of the FPB

b) Name of concerned person

c) Address

User stores the FPB details. System goes to the previous screen.

vi) Configure Templates

The admin needs to manage and update the templates needed for different procedural purposes. Admin may add new templates. Admin may delete the old templates. This flow gets initiated by the admin as they maintain the different templates needed in different procedures and for different case types. They may enter delete or change the templates as per the directive of local governments or standard guidelines. The data is manually entered into the system by the user. After the user saves the data the changes are reflected to the users. The admin are not allowed to make changes to the data specified by the centre. User

successfully logs on to the system with the administrator's role. User navigates to configuration template. System displays the option to

a) Add a template.

b) Modify a template

c) Delete a template

If the user chooses to Add a Template, User fills in the details of template. These templates are the documents that are used in the normal operation of police station. These templates are only for those functionalities not supported by the System. They are primarily for interfacing with other entities e.g. Other police station for information sheet, For sending reports to CBI, for interfacing with hospital in cases of injuries. System displays the details that are needed to be entered into the system. User stores the template. System goes to the previous screen. If the user chooses to Delete a Template, System deletes the template. If the user chooses to Modify a Template, System stores the modified template.

vii) Configure Case-specific Service Levels

The admin needs to manage and update the data periodically. Admin may add service levels/standards/benchmarks for a case type. This flow gets initiated by the admin they are in charge of maintaining the service levels for different case types. They may enter delete or change the service agreements as per the directive of local governments. The data is manually entered into the system by the user. After the user saves the data the changes are reflected to the users. The admin are not allowed to make changes to the data specified by the centre. User successfully logs on to the system with the administrator's role. User changes the service level agreement for a case type.

viii) Configure Users

The admin needs to manage and update the other user's data periodically. It is need to keep the system updated as per the change happening with respect to human resources. This flow gets initiated by the admin they are in charge of maintaining the user accounts in the system. Admin may

a) Add or delete a user

b) Reset the password of user

c) Change the role of the user

The data is manually entered into the system by the user. After the user saves the data the changes are reflected to the users. User successfully logs on to the system with the administrator's role. User navigates to configuration module of the user. System displays the option to

a) Add a user

b) Delete a user

c) Change role of user

d) Resets the password

If the user chooses to Add a User, User fill in the details of User

a) Name

b) ID or PIS code

c) Role

d) Date of enlistment

e) Caste

f) Educational Qualification

g) Raker Year

System displays the details of the user that are needed to be entered into the system. PIS code should be at least 12 characters. User stores the data. System goes to the previous screen. If the user chooses Delete User, System asks for the ID and name. User fills in the ID and Name and then confirms to the system. System asks for confirmation and then mark the user as deleted. If the user chooses Change Role of User, System asks for the ID and name. User fills in the ID and Name and then confirms to the system. System asks for confirmation and then Change the role. If the user chooses Reset Password, System asks for the ID and name. User fills in the ID and name. System asks for the new passwords. User fills in the new password and confirms it. System updates the password for the user.

G) CITIZEN INTERFACE MODULE

Citizen Interface Module
Complaint Based Registration
Register Complaint and Receive Acknowledgement
Query Based Interfacing

Conduct a Query
Property Information
Apply for a NOC from the Police
Status check on a NOC application
Provide general feedback/comments to the Police

i) Complaint Based Registration

Register Complaints and Receive Acknowledgement

This flow enables citizens to register non emergency complaints online, and receive an electronic format acknowledgement that police has received the complaint and will get back to the citizen within a stipulated time. Citizens also get the copies of the case documents which they have filed with the Police station. Citizens can get the copies of FIR/MC/PME after giving the credentials online and they can view and take the print out.

1. Register non-emergency complaints and receive acknowledgement
2. View status on the complaint filed (FIR, non FIR etc.)
3. Get copies of the case documents (FIR, MC, PME etc)
4. Submit evidence and updates on the complaints

ii) Query Based Interfacing

Conduct a Query

The purpose of this flow is to give citizens a handle to operate upon the wish of seeking information. Citizens can conduct a query based on the type of complaint they have of the type of the information they seek. This use case helps citizens conduct following types of queries:

1. Query on process of registering complaints, investigation updates, summons, warrants, appearance as witnesses, and other procedures for which citizen comes in contact with the police
2. On Missing Persons
3. On status of a case
4. On Stolen Property (including vehicles)
5. On Unclaimed/Abandoned Property (including vehicles)

6. On Most Wanted Persons in the area
7. On crime profile/statistics of an area.
8. Query on information on the police station trends, crime maps to the citizens
9. Query on information on filing false FIR/complaint

iii) Property Information

Apply for an NOC from the Police

The citizens need to apply for different kind of No Objection Certificates (NOCs). This interface gives them a control of applying for those NOCs online. This flow describes the required steps performed how a citizen can apply to an NOC online.

Seek Status of an NOC Request

For the NOCs applied, a citizen may seek the status in which his request is. This flow gives the handle to the citizen by which he can seek the status of the NOC online. This use case describes the required steps performed by citizens who are going to seek the status for their NOCs.

Request for escalation on a complaint.

Provide the General Feedback/Comments to the Police

At times citizens may have some feedback for police personnel/processes/incidents. This flow enables citizens to provide this feedback online to the department.

1. This use case describes the required steps performed to submit the feedback to the Police.
2. Submit intelligence, information to police (anonymous information).
3. Register complaint against Police.

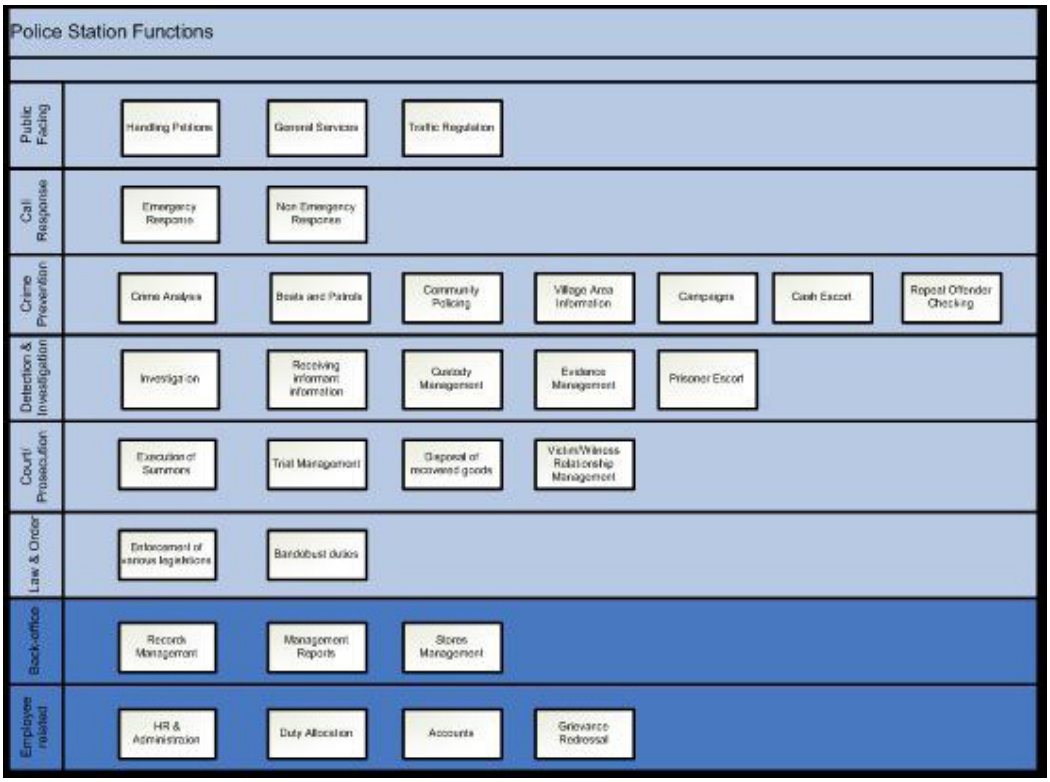
Brief Description of Police Station Process

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:



Functions in a Police Station

Traffic Management

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

Emergency Response Management

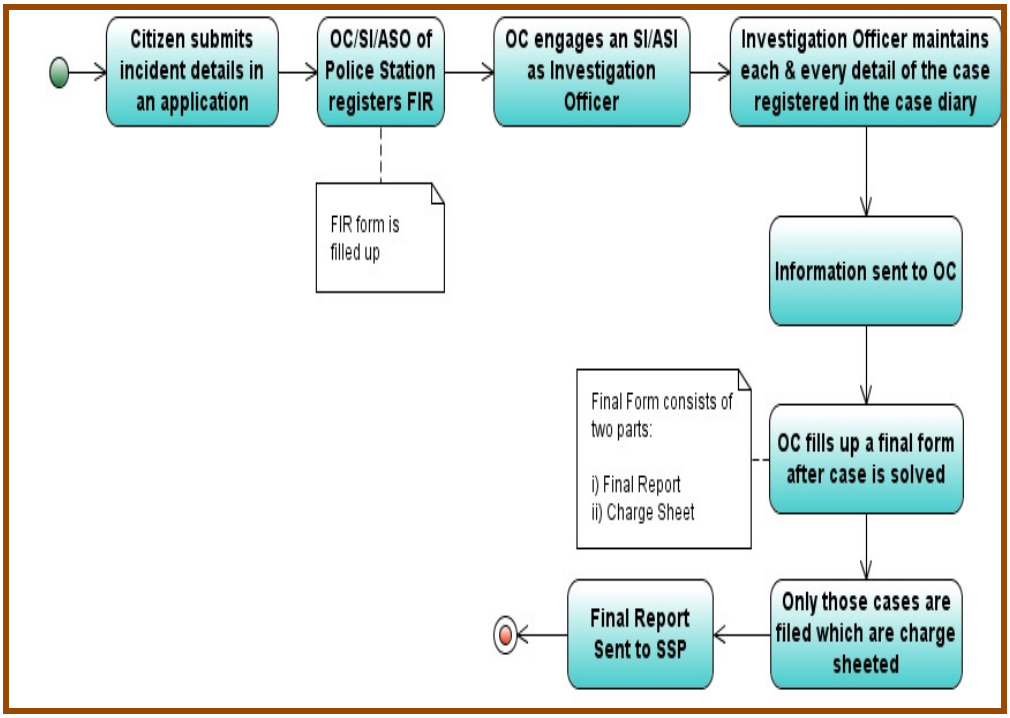
The control room of the police department serves as the focal point in the initiation and response of resources to the immediate citizen need for service. The primary function of the emergency response wing of the police department is to respond to citizen calls for assistance. It is critical that the department responds to calls for assistance in the shortest possible time, with the appropriate resources and with the most accurate information available in order to meet the public safety. In order to achieve a minimum turnaround time from the time the call is received to the time an emergency responder is sent for service, the control room personnel should be provided with easy interfaces to capture the caller information and access to caller details, incident location and the nearest available emergency responder. Efficient and timely responses to emergency calls are critical in building up the confidence of public in the police department. Information systems can play a major role in improving the efficiency and the effectiveness of the functioning of the control room and field units while responding to emergencies. There are multiple stakeholders in an emergency response scenario, right from the caller or victim making the call to report the incident to the call receivers and dispatchers manning the control room to the emergency responders visiting

the caller at his/her location. While the patrol officers may be the first responders, the police station takes charge of the incident after the first response for further enquiry and investigation.

FIR Process:

Primary Actors:	Citizen, OC/SI/ASI
Secondary Actors:	IO/DY.SP/ SP
Description:	FIR Process followed in Thana
Trigger:	Citizen submits application w.r.t. FIR
Pre Conditions:	Citizen must submit application with incident on white paper to the Police Station
Post Conditions:	1. Final Report sent to SP
Normal Flow:	1. Citizen submits application with incident details to Police Station 2. OC/SI/ASO of Police Station registers FIR by filling the FIR form 3. The OC engages an SI/ASI as Investigation Officer 4. Investigation Officer maintains each & every detail of the case registered in the case diary 5. Information sent to OC 6. OC fills up a final form after case is solved which as two parts: • Final Report • Charge Sheet 7. Only those cases are filed which are Charge Sheeted 8. Final report sent to SSP
Average time taken to complete the process	7-15 days

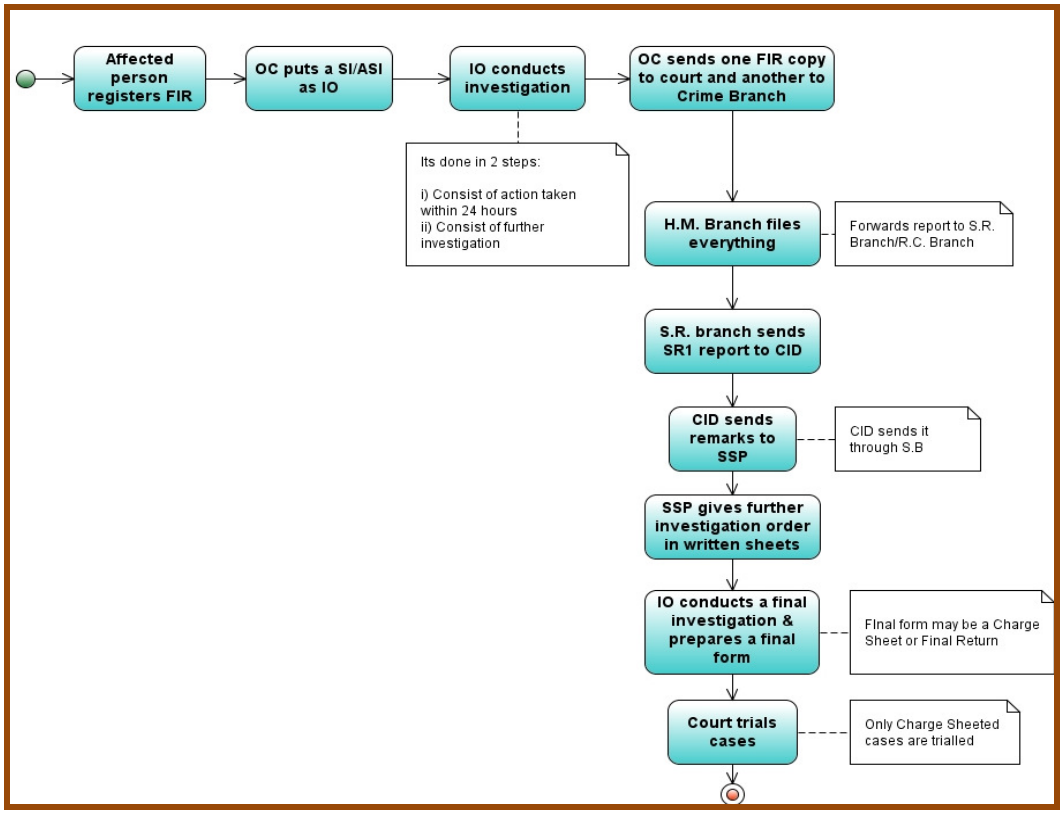
Process Flow Diagram for FIR:



Investigation Process:

Primary Actors:	Affected Person, Investigation Officer, SP/ SSP Office
Secondary Actors:	Officer in Charge (PS), CID, S.B Branch, Court etc.
Description:	Investigation of crimes committed & punishment of criminals
Trigger:	Registration of FIR by Affected Person
Preconditions:	1. Affected person must lodge a FIR
Post conditions:	1. Trial of Cases is done by courts
Normal Flow:	1. Affected person registers FIR in the nearest Thana 2. Officer in Charge (Thana) puts section against the registered FIR and assigns an ASI/SI as Investigation Officer (IO) 3. Investigative Officer (Thana) conducts investigation in 2 steps: a. 1st step - consists any action taken within 24 hrs b. 2nd step – consists further investigation

	4. Officer in Charge (Thana) sends one FIR copy to concerned court & sends other FIR copy to Crime Branch 5. H.M. Branch puts everything in register. Decides RC or SR and based on the decision & sends report to SR branch or RC Crime Branch 6. SR branch sends special report (SR1) to CID/DC 7. CID Send remarks through SB to SSP Office (Crime Branch) 8. SSP Office (Crime Branch) gives further investigation orders in written sheet 9. The Investigative Officer (Thana) investigates and when he reaches a conclusion he returns the case in FF (final form) through Officer in Charge (Thana) to court/crime branch. Returned cases may be of 2 type's: • Charge sheet – needs trial by court. • FR (final return) – case closed 10. Court trials only charge sheeted cases
Av. Time taken for an investigation	4-6 months

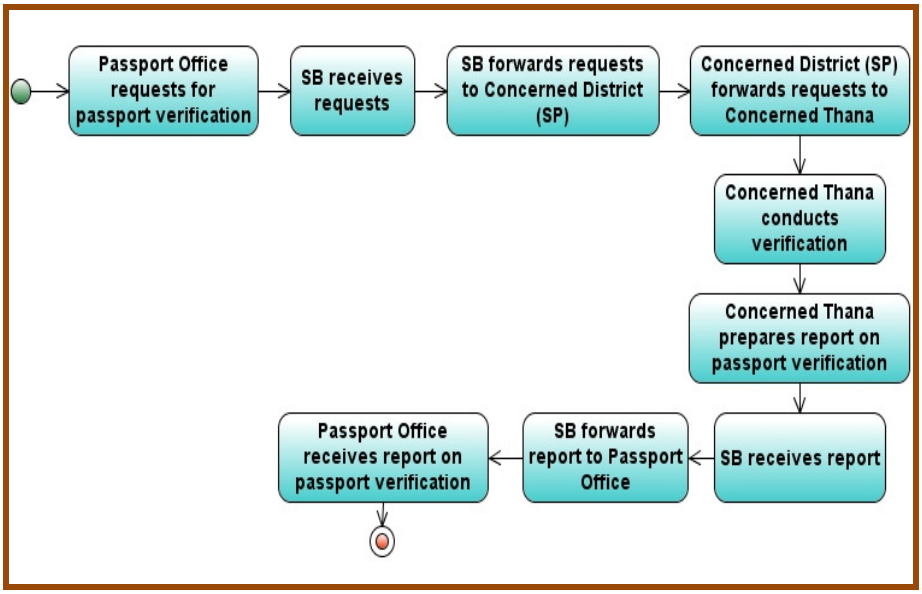


Passport Verification:

Primary Actors:	Passport Office, Concerned Thana
Secondary Actors:	SB, Concerned District (SP)
Description:	Passport Verification
Trigger:	Passport Office requests for passport verification
Preconditions:	1. Passport Office requests for passport verification
Normal Flow:	1. Passport Office requests for passport verification 2. SB receives requests 3. SB forwards requests to Concerned District (SP) 4. Concerned District (SP) forwards requests to Concerned Thana 5. Concerned Thana conducts verification 6. Concerned Thana prepares report on passport verification

	7. SB receives report 8. SB forwards report to Passport Office 9. Passport Office receives report on passport verification
Average time taken	1-2 months of time

Process Flow Diagram for Passport Verification:

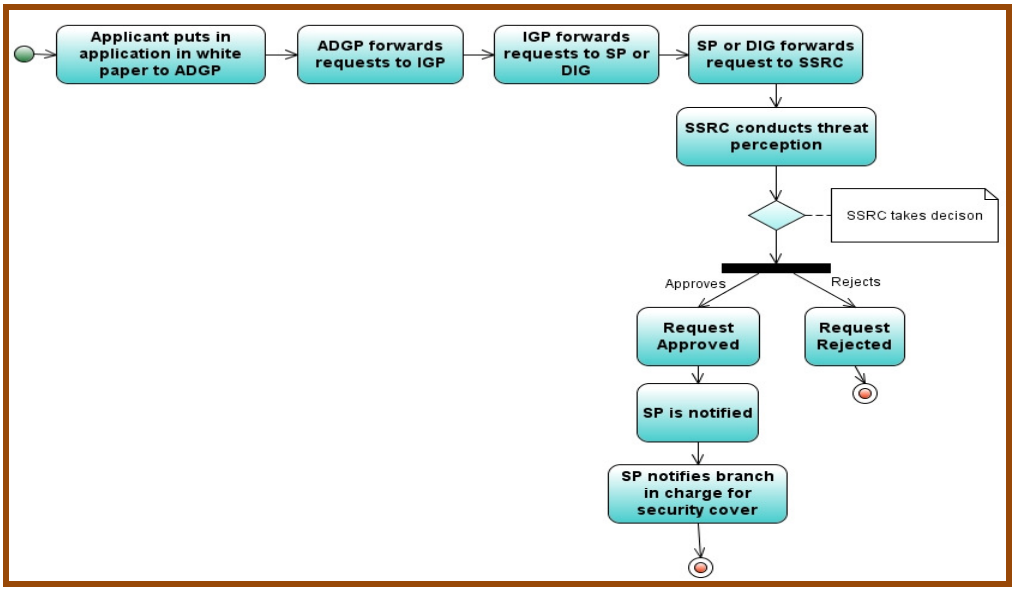


Providing Security

Primary Actors:	Applicant, SB
Secondary Actors:	SP/DIG/ IGP
Description:	Providing Security
Trigger:	Applicant puts in application in white paper/verbal order from Higher
Preconditions:	1. Applicant puts in application in white paper
Normal Flow:	1. Applicant puts in application in white paper to ADGP

	2. ADGP forwards requests to IGP 3. IGP forwards requests to SP or DIG 4. SP or DIG forwards request to SSRC 5. SSRC conducts threat perception 6. If approved, SP is notified 7. SP notifies branch in charge for security cover 8. Applicant receives security
Alternative Flows:	1. Payment if required is provided to Special Branch 2. For VIP security, information is passed from Delhi & SP arranges for security
Average time	1. For normal cases 7-15 days 2. For VIP 1-3 days

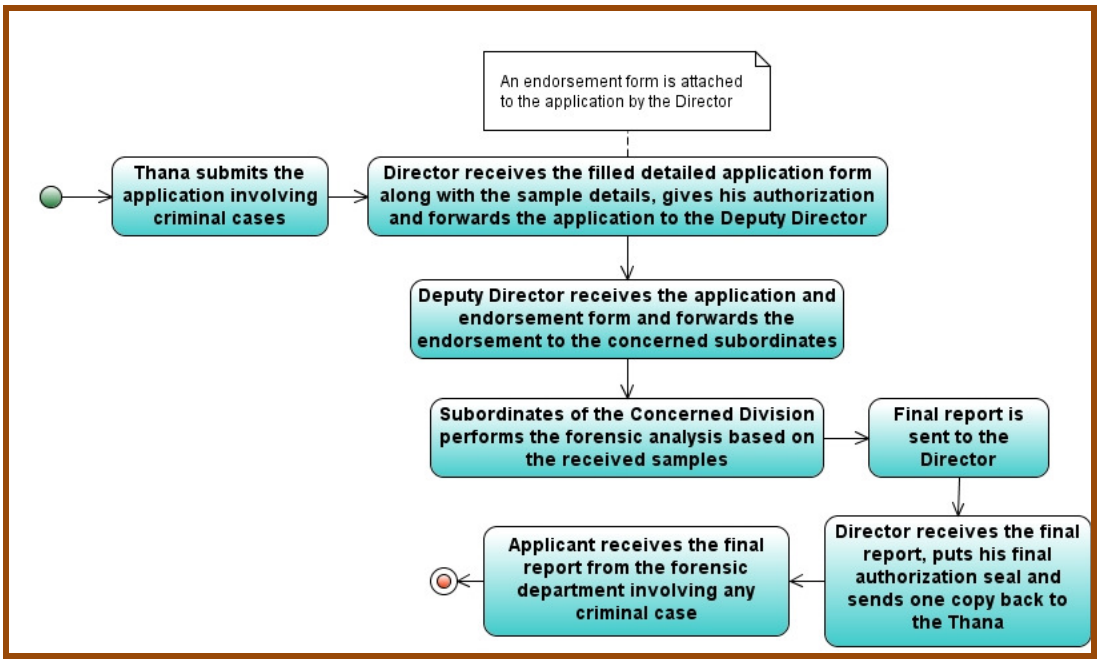
Process Flow Diagram for Providing Security:



Investigation aid to Police (G2G)

G2G Services	Application for Forensic help for faster investigation in Administration of Justice
Primary Actors:	Thana/ SP office
Secondary Actors:	Forensic Lab
Description:	To provide with the Forensic lab report for govt./court or private body with the final report of cases involving medical, criminal, toxicological etc
Trigger:	Application regarding the case including blood samples, DNA format etc. with all required details
Preconditions:	1. Application must be submitted by Thana/PS
Normal Flow:	1. Thana submits the application involving criminal cases in a white paper containing details of date, subject, questions and queries along with all the details of blood samples, DNA format, evidences on the crime spot etc. 2. The Director receives the filled detailed application form along with the sample details, gives his authorization and forwards the application to the Deputy Director of Format(Concerned Division) with an endorsement form 3. The Deputy Director receives the application and endorsement form and forwards the endorsement to the concerned subordinates 4. The Subordinates of the Concerned Division performs the forensic analysis based on the received samples 5. They send final report to the Director 6. The Director receives the final report, puts his final authorization seal and sends one copy back to the Thana 7. The Applicant receives the final report from the forensic department involving any criminal case
Average time taken	30-60 days

Process Flow Diagram for Investigation Aid:



7. SCOPE OF WORK SUMMARY & TIMELINES

Following table details the key project milestones and the deliverables to be submitted by the selected bidder at each milestone:

Sl. No.	Project Activity	Deliverables	Timelines (T - from date of signing of contract)
1	Project Planning	i. Detailed Project Plan for Implementation of the Project ii. Risk Management and Mitigation Plan iii. Manpower Deployment Plan	T
Study and Design			
2	System Study – study the legislation, business processes and organization design of Manipur Police along with relevant reports such as PIM	iv. A comprehensive System Study document v. Updated/ vetted FRS report including list of additional features that would result in further improvement in the overall application performance for consideration of the department vi. A comparative report on the extent of functionality currently available in the vendor's application (CAS provided by Centre) other applications/ COTS products and with the FRS for CRP vii. Detailed integration and interfacing model viii. Change/Reference document including all the changes or deviations from the base version of the CAS(State)/ FRS of other modules	T + 8 Weeks
3	Detailed assessment of functional requirements and MIS requirements		
4	Finalization/ Vetting of FRS		

5	Preparation of System Requirement Specification report and Software Requirement Specification report	ix. System Requirement Specification Report and Software Requirement Specification reports meeting all the Business, Functional and technical requirement of Manipur Police and incorporating all the functional specifications, standards provided by the NCRB, Manipur Police specific requirements and different integration points with CAS (Centre), external agencies and other applications of Manipur Police x. List of additional features proposed in complete CCTNS Application xi. CAS (State) Implementation document w.r.t. Configuration, Customization, Extension and Integration as per Manipur Police's requirements	

6	Preparation of Solution Design documents	A detailed Design document including: xii. Technical Architecture Document (Application, Network, and Security) xiii. High Level Design (including but not limited to) a. Application architecture documents b. ER diagrams and other data modelling documents c. Logical and physical database design d. Data dictionary and data definitions e. Application component design including component deployment views, control flows, etc. xiv. Low Level Design (including but not limited to) a. Application flows and logic including pseudo code b. GUI design (screen design, navigation, etc.) c. Database architecture, including defining data structure, data dictionary as per standards laid down by GoI/ GoM xv. CCTNS Application Test Plans and Test Cases	T + 10 Weeks
7	Site Survey	xvi. A site survey report detailing the current status of each site and the enhancements to be made at each site (s) based on the State's requirement and the guidelines of MHA, NCRB	T + 10 Weeks

8	IT infrastructure sizing	xvii. Final BoM with Technical specifications for the IT Hardware, Network and other IT Infrastructure Requirements xviii. Report on the reusability of existing infrastructure xix. Hardware procurement & Deployment plan	T + 11 Weeks
9	Others	xx. Data Migration Strategy and Methodology	T + 11 Weeks
10	Commissioning and operationalization of IT infrastructure at Data Centre and DR		T + 11 Weeks
Implement {This shall only begin after CAS (State) has been received from NCRB, MHA} – T1			
11	Study and analyze the CAS (State) system as received from NCRB against the requirements of Manipur Police and conduct Conference Room Pilot (CRP) based on the requirement specifications	xxi. Feedback Report based on CRP I and CRP II	T1 + 4 Weeks
12	Finalization of requirement specifications	xxii. Final FRS, SRS and other requirements with all the Solution Design documents	T1 + 6 Weeks
13	Configuration & Customization of CAS (State) and development of additional modules		T1 + 14 Weeks
14	Integration with CAS (Centre)		T1 + 14 Weeks

15	Data migration and digitization of historical data		T1 + 14 Weeks
16	Migration of CIPA and CCIS Police Stations/ non-CIPA and CCIS Police Stations/ Higher Offices to CCTNS		T1 + 15 Weeks
17	Testing of configured & deployed solution (CAS) and additional functionalities		T1 + 16 Weeks
18	Site preparation at Pilot Phase Client site locations		T1 + 18 Weeks
19	Procurement, Commissioning and Operationalizing the IT infrastructure at Pilot phase Police locations		T1 + 20 Weeks
20	User Acceptance and Testing of Pilot Phase implementation		T1 + 20 Weeks
21	User Training on Pilot Phase CCTNS Solution		T1 + 22 Weeks
22	Pilot rollout in two districts	xxiii. Report on amendments / enhancements / modifications made based on inputs of Manipur Police	T1 + 22 Weeks
23	Go-Live of Pilot	xxiv. Pilot phase Acceptance from Manipur Police xxv. Pilot phase Go-Live Report including	T1 + 24 Weeks

24	Improvement of application according to the experience of Phase I	a. Data Migration report for Pilot phase b. Performance and Load Testing Report for Pilot phase	T1 + 24 Weeks
25	CCTNS Solution customization for Phase II and integrating with external agencies		T1 + 32 Weeks
26	Site preparation at Phase II Client locations		T1 + 42 Weeks
27	Procurement, Commissioning and Operationalizing of IT infrastructure at Phase II Client locations		T1 + 42 Weeks
29	Capacity Building and Change Management		T1 + 44 Weeks
30	User Training on complete CCTNS Solution		T1 + 44 Weeks
31	State wide rollout of Phase II	xxvi. Report on amendments / enhancements / modifications made based on inputs of Manipur Police / Third Party's Acceptance Testing for State-wide Roll-Out	T1 + 45 Weeks
32	3rd party Acceptance testing, audit and certification of complete CCTNS Solution	xxvii. Third Party Acceptance Testing Certificate	T1 + 48 Weeks
33	SLA and Performance Monitoring Plan	xxviii. Detailed plan for monitoring of SLAs and performance of the overall system	Before "Go-Live"

34	Go-Live for complete CCTNS Solution	xxix. Go-Live Acceptance from Manipur Police xxx. Report on roll-out across State including a. Site Preparation and Infrastructure Deployment Report across State b. Manpower Deployment Report c. Data Migration Report including Test Plans and Test Results for Data Migration d. Training Delivery Report e. Overall Test Report	T1 + 50 Weeks
Post Implementation - Operation and Maintenance			**5 Years since the "Go-Live" of Complete CCTNS Solution**
35	Handholding support		For next 6 months from "Go-Live of each of the phases - Pilot and complete CCTNS solution respectively"
36	Project Operation and Maintenance	xxxi. Fortnightly Progress Report on Project including SLA Monitoring Report and Exception Report xxxiii. Project Quality Assurance report xxxii. Details on all the issues logged	5 Years from the date of "Go-Live" of Complete CCTNS Solution

8. SCOPE OF SERVICES DURING IMPLEMENTATION PHASE

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

- Project planning and management
- Configuration Customization and Extension (New Modules) of CAS (State) and Integration with CAS (Center) and External Agencies. CAS (State) will be developed in two distinct technology stacks by the SDA at the Center. The SI is expected to bid with one of the technology stacks in the response to this RFP. SI shall procure all the necessary underlying solution components required to deploy the CAS (State) solution for Manipur.
- Site preparation at the Higher Office locations (Circle offices, Range offices, Zones, State Crime Branch, CID, SDPOs, District HQ, Addl. SP Office, Economic Offences Wing, FPB, FSL, Cyber FSL, Communication & Technical Services branch and PHQ.
- IT Infrastructure at the Client site locations (Police Stations, Circle offices, Range offices, Zones, State Crime Branch, CID, SDPOs, District HQ, Addl. SP Office, Economic Offences Wing, FPB, FSL, Cyber FSL, Communication & Technical Services branch and PHQ).
- Network connectivity
- Data migration and Digitization of Historical Data
- Migration of CIPA and CCIS Police Stations / Higher Offices to CCTNS
- Change Management
- Capacity building
- Handholding Support
- Support to 3rd party acceptance testing, audit and certification

In implementing the above, the SI shall strictly adhere to the standards set by the MHA, NCRB, and State.

The project will be managed out of State Nodal Offcer's office in State HQ. At all points in the execution of the project, key senior resources including the project manager must be based at State Nodal Officer's office in State HQ.

8.1 Project Planning and Management

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

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

a. Create an organized set of activities for the project

b. Establish and measure resource assignments and responsibilities

c. Construct a project plan schedule including milestones

d. Measure project deadlines, budget figures, and performance objectives

e. Communicate the project plan to stakeholders with meaningful reports

f. Provide facility for detecting problems and inconsistencies in the plan

g. During the project implementation the SI shall report to the State Nodal Officer, on following items:

   (i) Results accomplished during the period;

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

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

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

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

h. Progress reports on a fortnightly basis

i. Interventions which the SI expects to be made by the State Nodal Officer and/or actions to be taken by the State Nodal Officer before the next reporting period;

j. Project quality assurance reports

k. As part of the project management activities, the SI shall also undertake:
   i. Issue Management to identify and track the issues that needs attention and resolution from the State.
   ii. Scope Management to manage the scope and changes through a formal management and approval process
   iii. Risk Management to identify and manage the risks that can hinder the project progress

The Project plan prepared by the SI would be reviewed by the Governance Structure in the State and approved by the Committee on the advice of the State Mission Team and State Project Management Unit.

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

Requirements Traceability Matrix

The SI would ensure that developed solution is fully compliant with the requirements and specifications provided in the RFP such as functional, non-functional and technical requirements. For ensuring this, the SI shall prepare a Requirement 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. Project documents include but are not limited to the following:

- Detailed Project Plan
- Updated/vetted FRS
- SRS document
- HLD documents (including but not limited to)
    - Application architecture documents
    - ER diagrams and other data modeling documents
    - Logical and physical database design
    - Data dictionary and data definitions
    - Application component design including component deployment views, control flows, etc.
- LLD documents (including but not limited to)
    - Application flows and logic including pseudo code
    - GUI design (screen design, navigation, etc.)
- All Test Plans
- Requirements Traceability Matrix
- Change Management and Capacity Building Plans
- SLA and Performance Monitoring Plan
- Training and Knowledge Transfer Plans
- Issue Logs

The SI shall submit a list of deliverables that they would submit based on the methodology they propose. The SI shall prepare the formats/templates for each of the deliverables upfront

based upon industry standards and the same will be approved by State prior to its use for deliverables.

All project documents are to be kept up-to-date during the course of the project. The SI shall maintain a log of the internal review of all the deliverables submitted. The logs shall be submitted to State Nodal Officer on request. All project documentation shall conform to the highest standards of software engineering documentation.

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

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

on project milestones by the Nodal Officer and other Supervisory Officers of CCTNS.

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

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

The SI shall procure and commission the required infrastructure (software, servers) for Project Management Tool, Configuration Management Tool and Issue Tracker tool and

maintain the same through the duration of the project. These tools along with the servers on which they are deployed will become property of the State and will be used by State even beyond the contract period.

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

8.2 CONFIGURATION, CUSTOMIZATION, AND EXTENSION (NEW MODULES) OF CAS (STATE) AND INTEGRATION WITH CAS (CENTER) AND EXTERNAL AGENCIES

System Study, Design, Application Development and Integration

The SI shall carry out a detailed systems study to refine the Functional Requirements Specifications provided as Annexure to this RFP and formulate the System Requirements Specifications (SRS) incorporating the functional specifications and standards provided by the NCRB and the state-specific requirements. The SI shall also study CAS-State and CAS-Center being developed at NCRB and / or already running application in Manipur during the system study phase. The study should also include different integration points of CAS state with external agencies as per state requirement. The SRS preparation shall take into account the BPR

recommendations suggested by the NCRB / State. The SI should also prepare a detailed document on the implementation of CAS (State) with respect to configuration, customization and extension as per the requirement of state. The SI would also prepare a change/reference document based on changes or deviations from the base version of the CAS (State) with appropriate references to all the artifacts /documents provided by NCRB / State.

1. Conduct of System Study at selected locations.
2. Preparation of System Requirements Specifications (SRS) for additional

functionalities and different integration points with CAS (Center) and External agencies.

3. Preparation of CAS (State) implementation document with respect to Configuration, Customization and extensions as per the requirement of state.
4. Preparation of the Solution Design
5. Solution Development and/or Customization and/or Configuration and/or Extension as required
6. Development of reports
7. Formulation of test plans and test cases for additional functionalities and different integrations with external agencies including CAS (Center)
8. Change/Reference document include all the changes or deviations from the base version of the CAS (State)
9. Testing of the configured solution (CAS) and additional functionalities.

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

Creation of Test Plans

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

High Level Design (HLD)

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

Detailed (Low Level) Design (LLD)

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

Application Development and Unit Testing

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

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

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

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

Configuration of CAS (State)

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

1. Developing Local Language Interfaces and Support
2. Configuring users
3. Configuring Police Stations / Higher Offices
4. Configuration of the UI as required by the State

The collection and validation of the data required for the configuration of the CAS (State) shall be the responsibility of the SI.

Setup of Technical Environment at State Headquarters

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

Regression, Integration, System and Functional Testing

After successful unit testing of all components, the SI would conduct full-fledged integration testing, system testing and functional testing in accordance with the approved Test Plans for

the configured/customized CAS (State), additional functionalities and also integration with CAS (Center) and external agencies. This would include exhaustive testing including functional testing, performance testing (including load and stress), scalability testing and security testing. Functional testing will be led by the SI's experts.

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

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

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

Test Reports

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

Test Data Preparation

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

User Acceptance Testing (UAT)

Test Plans for UAT would be prepared by the SI in collaboration with the State Mission Team /SPMU domain experts. The SI will plan all aspects of UAT (including the preparation

of test data) and obtain required assistance from State Headquarters to ensure its success. State Mission Team/SPMU will assemble representatives from different user groups based on inputs from the SI and would facilitate UAT. The SI would make the necessary changes to the application to ensure that CAS successfully goes through UAT.

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

8.3 SITE PREPARATION AT POLICE STATIONS AND HIGHER OFFICES

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

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

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

8.4 INFRASTRUCTURE AT THE CLIENT SITE LOCATIONS

The premises for offices will be provided by the department at respective locations. The list of Police Stations, Circle offices, and other locations where the infrastructure is required is

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

At each such location the following shall be carried out.

1. Supply of the hardware, software, networking equipments, UPS, DG set to the location as per the requirements
2. Redundant Network Connectivity - Ensuring last mile connectivity and testing.
   (At some locations SWAN may be available. SI shall ensure there is redundancy in the connection)
3. Installation, Testing and Commissioning of UPS, DG-Set
4 Physical Installation of Desktops, Printer, Scanner, /MFD, Switch- Connecting peripherals, devices, Plugging in
5. Operating System Installation and Configuration
6 Installation of Antivirus and other support software if any\
7. Configuring the security at the desktops, switch and broadband connection routers
8. Network and browser Configuration
9. Test accessibility and functionality of CCTNS application from the desktops
10. Ensuring all the systems required are supplied, installed, configured, tested and commissioned and declaring the site to be operational.

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

Indicative Hardware Bill of Material for PSs & Units under CCTNS Project:

The table below provides a detailed break up of hardware required for CCTNS Project.

Items	Quantity			
	Hardware per P.S	**No. of P.S/units under CCTNS**	**Total requirement**	**Remarks**
Client Systems (Preloaded with MS Windows 7 Pro, MS Office 2007 Pro. Plus or latest ver. & Antivirus)	4	101	301	**24** computers of 6 CIPA PSs @ 4 computers per PS to be replaced; for 5 PSs of CIPA **15** computers @ 3 per PS to be procured, for 15 PSs of CIPA **15** computers @ 1 computer per PS to be procured and for 17 PSs of CIPA **51** computers @ 3 computers per PS to be procured. For the remaining 49 PSs/Units **196** computers @ 4 computers per PS/Unit to be procured.
HDD 160 GB (external)	4	101	404	
Duplex Laser Printer	1	101	101	
UPS for 120min backup	1	101	55	46 UPS already provided for 46 CIPA PSs. 55 UPSs to be provided for the remaining 55 PSs.
2 KVA Generator set	1	101	96	96 generators@ 1 generator per PS to be provided for 96 PSs. 5 Generators already provided for 5 CIPA PSs.
8 Port Switch	1	101	49	Port Switch 52 CIPA PSs had already been provided
Fingerprint Reader	1	101	101	
Digital Camera	1	101	101	
Electronic Pen	1	101	101	
Operational Expenses (paper / toner)	1	101	101	

Indicative Site Preparation Requirements for P.Ss / Units under CCTNS

Sl. No.	Item	No. of Locations
a.	Creation of LAN (with creation of LAN nodes, laying UTP cables, structured cabling, patch panels, cable cripping, installing RJ-45, etc.)	101
b.	Workstations with allied furniture	101
c.	Earthing, Electric Cabling & adequate no. of power points	101

Indicative Hardware Bill of Material for Higher Offices

Higher Offices	No. of PC required (Preloaded with MS Windows 7 Pro. OS, MS Office 2007 Pro. Plus or latest ver. & Antivirus)	No. of Offices	Total no. of Computers	UPS	MFP	8 port Switch	Site Preparation	OPEX (paper / toner)
SDPO/DY.SP/ATMO/Sc. Officer	3	84	252	84	84	84	84	84
Addl.SPs	3	20	60	20	20	20	20	20
SPs/JD(MPW)/AD FSL/AIG	10	21	210	63	21	42	21	21
DIGPs/Dir.MPW/Dir.FSL	4	12	48	12	12	12	12	12
IGPs/Dir. MPTC	4	10	40	10	10	10	10	10
ADGPs	4	4	16	4	4	4	4	4
DGP	10	1	10	3	1	2	1	1
Total		**152**	**636**	**196**	**152**	**174**	**152**	**152**

Total No. of PC's to be procured 301 + 636 = 937

Indicative Site Preparation Requirements for Higher Offices

	Item	No. of Locations
a.	Flooring	152
b.	Wall Finishing and Painting	152
c.	Roller Blinds	152
d.	Ceiling Mounted Light fixtures	152
e.	4 mm thick Glass for door renovation	152
f.	Workstations with allied furniture	152
g.	Cabinets	152
h.	Earthing, Electric Cabling & adequate no. of Power points	152
i.	Creation of LAN (with creation of LAN nodes, laying UTP cables, structured cabling, patch panels, cable cripping, installing RJ-45, etc.)	152

8.5 NETWORK CONNECTIVITY FOR POLICE STATIONS, HIGHER OFFICES, AND DISTRICT TRAINING CENTERS

The Networking solution of CCTNS project shall be based on a Hybrid Model which will consist of SWAN operated by State under SWAN scheme and Data network operated by 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 State. BSNL shall also provide connectivity on MPLS VPN network for aggregated bandwidth at SDC for the locations connected on VPNoBB, WiMax and VSAT network and also provide connectivity for SDCs at SHQs to the National Data Centre of NCRB. Further BSNL shall provide MPLS VPN network for connecting SDC and DRC of the State.

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 SDC for the locations connected on VPNoBB, WiMax and VSAT network.

e) Provisioning of MPLS connectivity between SDC and DRC.

f) Provisioning of MPLS connectivity between NDC and SDC.

g) Maintaining the network including hardware supplied for minimum period of 3 years.

Role of System Integrator : The SI shall coordinate with BSNL and Manipur Police Department 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.

i. Site preparation at all locations for establishment and installation of networking and connectivity solution.

ii. 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.

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

iv. 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 Master Service Agreement.

v. The Police Stations and Higher Offices which are within the proximity of SWAN PoP 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 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.

SI shall also coordinate with State CCTNS Nodal Officer 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.

8.6 DATA MIGRATION & DATA DIGITIZATION

Data Migration

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

The SI shall perform the data digitization & migration from manual and/or the existing systems to the new system. The Data digitization & migration to be performed by the SI shall be preceded by an appropriate data migration need assessment including data quality assessment. The Data migration strategy and methodology shall be prepared by SI and approved by State. Though state is required to provide formal approval for the Data Migration Strategy, it is the ultimate responsibility of SI to ensure that all the data sets which are required for operationalization of the agreed user requirements are digitized or migrated. Any corrections identified by state or any appointed agency, during Data Quality Assessment and Review, in the data digitized/ migrated by SI, shall be addressed by SI at no additional cost to STATE. So far as the legacy data is concerned, they are either available as structured data in the IT systems that are currently used by state for related work or in the form of paper documents (Cases Documents and Police Station Registers). Almost all of such data items relevant for a Police Station are maintained at the same Police Station.

Data Migration Requirements

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

Scope of Data Migration

A one-time digitization effort to migrate the data of last ten years across the police stations into the system is required. It is observed that normally an FIR with detail case history contains more than 40-50 pages and these pages are mostly handwritten in vernacular languages. Utmost care shall be adopted during the process of digitations of these records into the system as any error in the process will create trouble for investigating officers / court etc.

Phase I would include the digitization of 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 data from the police stations records rooms (police registers).

Cost Estimate for Digitization				
Sl. No.	**Register / Form Name**	**Number of Records**	**Unit Cost (Rs.)**	**Total Cost**
1.	FIR	1,00,000	27	27,00,000

Digitization of historical data would help the police department maximize benefits from features such as Search and Reporting and is would significantly enhance outcomes in the areas of Crime Investigation, Criminals Tracking, servicing the requests of citizens and other groups, etc. The digitization exercise would be carried out by the state level SI.

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

Recommended Methodology of Data Migration

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

1. Analysis

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

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

2. Transformation

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

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

3. Data Take–On

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

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

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

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

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

m) Migrate from staging servers to production servers

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

Additional Guidelines for Data Migration

1. SI shall migrate/convert/digitize the data at the implementation sites of state.
2. SI shall formulate the "Data Migration Strategy document" which will also include internal quality assurance mechanism. This will be reviewed and signed–off by state prior to commencement of data migration.
3. SI shall incorporate all comments and suggestions of state in the Data Migration Strategy and process documents before obtaining sign–off from state.
4. SI shall perform mock data migration tests to validate the conversion programs.
5. SI shall ensure complete data cleaning and validation for all data migrated from the legacy systems to the new application.
6. SI shall validate the data before uploading the same to the production environment.
7. SI shall generate appropriate control reports before and after migration to ensue accuracy and completeness of the data.
8. SI shall convey to state in advance all the mandatory data fields required for functioning of the proposed solution and which are not available in the legacy

systems and are required to be obtained by state.

9. In the event state is unable to obtain all the mandatory fields as conveyed by SI, SI shall suggest the most suitable workaround to state. SI shall document the suggested workaround and sign-off will be obtained from state for the suggested workaround.
10. SI shall develop data entry programs / applications that may be required for the purpose of data migration in order to capture data available with / obtained by state in non – electronic format.
11. SI shall conduct the acceptance testing and verify the completeness and accuracy of the data migrated from the legacy systems to the proposed solution.
12. State may, at its will, verify the test results provided by SI.

Data Digitization

In addition to the above, SI would also be carrying out the digitization of historical criminal data during Pilot Phase which will include the digitization of 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 data from the police stations records rooms (from police registers).

Digitization of historical data would help the police department maximize benefits from features such as Search and Reporting and is would significantly enhance outcomes in the areas of Crime Investigation, Criminals Tracking, servicing the requests of citizens and other groups, etc.

Recommended Methodology of Data Verification

Effective data verification is the most important step in the migration/ digitization of data. Selected SI will support the Manipur Police Department in carrying out the data verification in a time bound manner and evolve a mechanism for data validation at various levels. An illustrative mechanism is given below:

• The manually processed Integrated Investigation Forms (1 to 7)/ Case File for a particular case would be given to the SI and will be checked for data completeness and consistency (lack of blank fields, correct data type per field, etc.) by the SI .

• Once the data is entered, digitized IIF forms (1 to 7)/ reports will then be checked/verified from the System for the particular case and shall be compared with the manually processed Case File, whereas In case of migrated data, IIF forms will be checked against the report generated from CIPA system for any particular case. Errors detected at this stage will be corrected by SI at no cost to the department.

• Corrected System generated Case File and its data will then be matched for verification against the existing manual records/ digitized records in CIPA application in Police Station. Further, system generated Case File will go through various levels of verification, starting from the Police Station to District level, District to Range and State level.

• This type of data verification by the District SP or State CCTNS Nodal Officer will be done through Data Verification Workshops where the records are brought, verification done (against the system generated Case Files) and the issues are flagged within a definite time frame. SI shall be responsible for conducting such a workshop and shall formally inform project nodal officer in writing well in advance for data verification workshop. SI shall also be responsible for incorporating and implementing changes proposed in these workshops at no additional cost to the department. These workshops shall work as User Acceptance Testing for Data Migration and Data Digitization. However overall System Acceptance testing shall be different from this testing and SI shall provide all the support required for ensuring quality of data entry/ data digitization/ data migration, wherever required.

There should also be a mechanism to incorporate those Police transactions that have taken place during the digitization of data phase. ***Correction facilities available in the software should be monitored to detect and discourage its misuse.***

Once this process is complete, the corrected data will be re-entered in the system and the records for which disputes have not been resolved will be flagged in the system so that this will not be bottleneck in the system going live. However, SI shall seek approval for flagging such data and point out the same during workshops. In case approval is not provided by

Manipur Police on the unresolved data entry, the same shall be counted for penalty calculations. Beyond this exercise, SI should be responsible for correcting the data entry found erroneous by the Department or its designated representatives at no additional cost to the Department. Manipur Police may at its discretion levy penalties for erroneous data entry as per penalty terms defined in the Service Level Agreement.

8.7 MIGRATION OF CIPA AND CCIS POLICE STATIONS / HIGHER OFFICES TO CCTNS

The SI is also responsible for migrating the Police Stations and Higher Offices currently operational on CIPA and CCIS to CCTNS as part of the CCTNS implementation in the State. SI shall validate the data in the CIPA systems and migrate the data to CCTNS.

8.8 CHANGE MANAGEMENT

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

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

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

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

the awareness and communication initiatives, workshops, and provide feedback to the District and State Mission Teams.

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

- Group I: Identify the key senior officers (ADGP, IG, DIG) responsible for Crime, Law and Order, who are directly impacted by the CCTNS with respect to receiving/analyzing the reports through CCTNS.
- Group II: Identify a few of the key officers (IG, DIG, DCP, ACP, SP) in charge

of a zone/range/district/sub-division who are directly impacted by the CCTNS with respect to reviewing the police station performance through CCTNS, reviewing the reports generated by the system, carrying out the required analysis using CCTNS and providing the necessary guidance to the officers at the cutting edge.

- Group III: Identify a few of the key officers (SHO, SI, ASI) in the Police Stations and Higher Offices who will use CCTNS for police station management, filing the necessary investigation forms, and utilize the basic and advance search features of CCTNS to facilitate their investigation process.
- Group IV: Identify a few of the key officers/constables (Station Writers, Court Duty, Head Constables) in the Police Stations and Higher Offices who will use CCTNS for capturing the data/investigation forms, generating the reports and utilize the basic and advance search features of CCTNS to service the general service requests and aid in investigation process.

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

Stakeholder Analysis / Impact Assessment

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

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

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

The SI would be responsible for the following activities:

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

Other Requirements:

- SI shall cover all the identified stakeholders and stakeholder groups identified in all the higher offices, State Headquarters, District Headquarters, SCRB, DCRB and Police Stations.
- SI will recommend additional Stakeholder or Stakeholder Groups – Internal and External who need to be covered under this activity.

- SI shall also cover the extended teams and should not limit to the direct identified stakeholders
- SI shall come up with innovative ways of stakeholder engagement in addition to the video conferencing, one on one meeting and teleconference
- SI shall ensure that the stakeholder engagement activity is a continuous activity and buy-in and commitment of the stakeholders are key drivers for the success of this project
- SI shall make recommendations to best manage this process
- SI shall also develop Job Aids, an important component of sustaining the change by ensuring that there is enough support material available to maintain the performance of the transformed workforce. A job aid is a repository for information, processes, or perspectives that is external to the individual and that supports work and activity by directing, guiding, and enlightening performance. Since job aids are external to the individual and would be applicable to those set of activities which are complex and difficult to memorize. For example, in the beginning stage, searching of records in the CAS might require a Job Aid. However, as the time progresses and user becomes more thorough and comfortable with the new system Job Aids for such activities may no longer be required. Also, for more complex activities such as generating a MIS report from the system might require a Job Aid for a much longer duration. These Job Aids must be revised on periodic basis.

Assess change readiness

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

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

Assessing change readiness will help the change team to:

- Pinpoint where risks are likely to occur
- Clarify issues associated with CCTNS
- Identify potential responses to change
- Identify and target where change activities are most needed

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

SI shall conduct 4 Cycles of Change Readiness Survey:

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

Sl. No.	Activities	Details	Frequency
1	Develop Change Readiness Survey approach	• SI shall be responsible for developing the objectives, scope, and process for change measurement • SI shall also finalize the target audience, timelines, method of change measurement	One time activity
2	Develop and Configure Change Measurement Survey/ Instrument	• SI shall develop or configure an appropriate change measurement instrument that is convenient for audience and easy to assimilate for CM Team • SI shall configure the change measurement instrument based on	Recurring Activity (at least four times in two years)

		the requirements of the project	
3	Select Sample Audience and Administer the survey	• SI shall select the sample for the survey and should ensure that the targeted audience is a fair mix representing all State Offices, solutions and all levels of the organization. • SI shall be responsible for administering the survey- paper based or electronic, as the case may be.	One time activity followed by review of sample audience for each subsequent cycle
4	Analyze reports and devise corrective action plan	• Analyze the result of the survey and generate survey reports (Higher Office-wise, State Headquarters - wise, District Headquarters - wise and Police Station-wise) to be shared with respective leadership team • Identify the key patterns that emerge out of the survey for all groups of stakeholders	Once for each survey
5	Share the result with the leadership and refresh change management plan	• SI shall share the results of each survey with audience identified by State's Nodal Agency and validate the corrective action plan with their inputs. • SI shall refresh the Change Management Plan with new	Once for each survey

		interventions in consultation with State's Nodal Agency's Change Management Plan	

Other Requirements:

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

Develop the Change Management plan

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

Implementation of Change Management Plan

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

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

Communication and Awareness

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

will be delivered, what information will be communicated, who communicates, and the frequency of the communications.

Communication & Awareness campaigns will be conducted throughout the duration of the implementation of the CCTNS project across the State/ UT at Project, Program level as well as for General awareness.

Sl. No	Activities	Details	Frequency
1	Develop and Validate detailed Communication plan	• SI shall facilitate an exploration of specific objectives; i.e., who must understand what, by when, and why with respect to the project, to ensure successful uptake of the project. • SI shall prepare a detailed communication plan for the program in line with the implementation timelines of each solution • SI shall ensure that all the impacted audience is covered in the communication plan and the most appropriate mode of communication is being used to deliver the messages to the target audience • These key audiences are not the only ones who will receive information, but their demographics will shape the strategy in terms of message and vehicle selection.	Once

2	Develop Communication Content	• SI shall be responsible for developing the content for communication material in English, Hindi and vernacular language. • SI shall ensure that the communication is simple, continuous and consistent.	Recurring Activity over the entire duration of the SI
3	Deliver Communication Events	• Prior to implementing the plan, the SI shall obtain the necessary sign-offs from State on the Communication Strategy & plan and make necessary changes as recommended by State. • SI shall determine who needs to approve communications prior to dissemination, who is responsible for distributing the message, and who is responsible for ensuring that those accountable for specific elements of the plan follow through on their responsibilities.	Recurring Activity (once a month) over the entire duration of the SI
		• SI shall organize the communication events or interventions for the target audience. • SI shall ensure consistency between messages delivered via different interventions, since the engagement of a key individual stakeholder or stakeholder group is an integrated effort, aiming at the same objective.	

4	Measure Effectiveness of Communication and Update Change Management Plan	• After implementing the communications program, SI shall seek feedback on and measure the impact of the communications program. • SI shall evaluate the effectiveness of the communication by electronic or paper based survey or focused group discussion and develop an action plan to improve the effectiveness of communication • SI shall refresh the Change Management Plan in consultation with **State's Nodal Agency's** Change Management Plan • Through feedback, SI shall assess which messages have been delivered most clearly; which vehicles are most effective; and whether the appropriate target audiences have been identified. Based on such assessment, SI shall update the communication strategy & plan and shall ensure that objectives of communication program are ensured, which further should lead to successful uptake of system.	Once in a Six Month

Other Requirements:

- SI shall work with the identified internal change agents (identified from the District and State Mission Teams) for all the Communication and Awareness

Programs

- SI shall utilize existing channels of communication and at the same time use innovative methods of communication for effectiveness
- SI should ensure that the communication messages are consistent, continuous and easy to understand and wherever possible in vernacular medium using all available channels
- The SI shall conduct Communications & Awareness Campaigns for each Technology Solution offered in CAS (State) being implemented through various means – Print, Electronic, Face to Face, Audio/Visual etc.
- SI shall align communication content, timing and delivery to the deployment phases/plan of each solution.

Change Management Workshops

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

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

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

8.9 CAPACITY BUILDING

Identification of Trainers (Internal)

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

Identification of Trainers (Police Training Colleges)

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

Identification of Trainees

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

- Group I: Identify the key senior officers (ADGP, IG, DIG) responsible for Crime, Law and Order who are directly impacted by the CCTNS with respect to receiving/analyzing the reports through CCTNS.
    - Role-based training will be carried out for these officers at suitable location in the State Headquarters by the System Integrator

- Group II: Identify the key officers (IG, DIG, SP, DCP, ACP) in charge of a zone/range/district/sub-division who are directly impacted by the CCTNS with respect to reviewing the police station performance through CCTNS, reviewing the reports generated by the system, carrying out the required analysis using CCTNS and providing the necessary guidance to the officers at the cutting edge.
    - Role-based training will be carried out for these officers at suitable location in the State Headquarters and respective Districts/Commissionerates by the System Integrator
- Group III: Identify the key officers (SHO, SI, ASI) in the Police Stations and Higher Offices who will use CCTNS for police station management, filing the necessary investigation forms, and utilize the basic and advance search features of CCTNS to facilitate their investigation process.
    - In addition to the computer awareness training, role-based training will be carried out for these officers at District Training Centers in the respective Districts/Commissionerates by the System Integrator
    - Refresher training can be carried out by the internal trainers subsequent to the System Integrator trainings

- Group IV: Identify at least 3-4 key officers/constables (Station Writers, Court Duty, Head Constables, Constables) in each of the Police Stations and Higher Offices who will use CCTNS for capturing the data/investigation forms, generating the reports and utilize the basic and advance search features of CCTNS to service the general service requests and aid in investigation process.
    - In addition to the computer awareness training, role-based training will be carried out for the identified officers at District Training Centers in the respective Districts/Commissionerates by the System Integrator
    - Refresher training, subsequent training to the remaining officers/constables in the Police Station and Higher Offices can be carried out by the internal trainers subsequent to the System Integrator trainings

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

The training will be provided to selected police personnel as per the requirements. These requirements are presented in the table below.

Training Program	Group A		Group B		Group C	
	% Covered	Actual No.	% Covered	Actual No.	% Covered	Actual No.
Awareness & sensitization of benefits of IT	100%	46	5%	123	1%	133
Basic Computer Awareness & Role based training for application users	100%	46	80%	1970	40%	5313
Trainers Training	0%	0	0.1%	3	0.25%	33
Administration & support training	0%	0	0%	0	3%	398

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

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

Develop Overall Training Plan

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

Develop District-Wise Training Schedule and Curriculum

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

Learning Management System and Training Portal

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

Develop Training Material

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

1. 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.
2. "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.
3. 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.
4. Customization of the Training Manuals, User Manuals, Operational and Maintenance Manuals provided along with the CCTNS CAS Software
5. Design and development of the Training Manuals, User Manuals, Operational and Maintenance Manuals for the modules developed at the State level.

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

SI shall ensure that the training content meets all the objectives of the training course. The material shall be developed in English, Hindi and vernacular language. SI shall also develop the training material for delivery through Computer Based Training, Instructor Led Training, Online User Material/Help Manuals and Job Aids. SI shall provide detailed training material providing step-by-step approach in soft and hard copies to all police stations and offices for reference.

Deliver Training to End Users

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

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

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

An ILT course will have the following components:

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

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

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

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

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

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

1. The first segment will be set of workshops covering effective presentation skills and coaching techniques and discussing the benefits and structure of the trainer model.
2. The second segment will be the formal CCTNS training which will consist of all modules of CCTNS relevant for their role.
3. The third segment will be a teach-back session where trained trainers will present course content and receive feedback regarding content, flow, and presentation techniques. This will also include a feedback session where trainers can provide feedback on the training materials, flow, comprehension level, and accuracy.

Training Effectiveness Evaluation

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

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

8.10 HANDHOLDING SUPPORT

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

NO. OF P.Ss / UNITS	NO. OF RESOURCES REQD.	NO. OF HIGHER OFFICES	NO. OF RESOURCES REQD.	TOTAL NO. OF RESOURCES REQD.
101	101 (1 resource * 101 locations)	152	152 (1 resource *152 locations)	253

8.11 REQUIREMENT ON ADHERENCE TO STANDARDS

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

Compliance with Industry Standards

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

Portal development	W3C specifications
Information access/transfer protocols	SOAP, HTTP/HTTPS
Interoperability	Web Services, Open standards
Photograph	JPEG (minimum resolution of 640 x 480 pixels)
Scanned documents	TIFF (Resolution of 600 X 600 dpi)
Biometric framework	BioAPI 2.0 (ISO/IEC 19784-1:200 specification
Finger print scanning	IAFIS specifications
Digital signature	RSA standards
Document encryption	PKCS specifications
Information Security	CCTNS system to be ISO 27001 certified
Operational integrity & secur management	CCTNS system to be ISO 17799 compliant
IT Infrastructure management	ITIL / EITM specifications
Service Management	ISO 20000 specifications
Project Documentation	IEEE/ISO specifications for documentation

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

All the licenses, if applicable, shall have to be procured by the selected SI for the successful implementation of this project. The system software licenses mentioned in the Bill of Materials, if applicable, shall be genuine, perpetual, full use and should provide patches, fixes, security patches and updates directly from the OEM. All the licenses and support (updates, patches, bug fixes, etc.), if applicable, should be in the name of Manipur Police.

• The SI shall provide with a full use database license. All the licenses and support (updates, patches, bug fixes, etc.), if applicable, should be in the name of Manipur Police.

• The software proposed should be from an OEM with presence in India (and easy availability of skilled resources for the product in India).

• SI shall provide a comprehensive warranty that covers all components after the issuance of the final acceptance by Manipur Police Department. The warranty should cover all materials, licenses, services, and support for both hardware and software. SI shall administer warranties with serial number and warranty period. SI shall transfer all the warranties to the Department at no additional charge at the time of termination of the project. All warranty documentation (no expiry) will be delivered to Department.

• The OEM must authorize the selected SI for products listed below.

- Operating System Name & Versions
- RDBMS Name & Versions
- Directory Server Name & Versions
- Office Productivity Suite Name & Versions
- Reporting Server Name & Versions
- Application Server Name & Versions
- Web Server Name & Versions
- Enterprise Management Server Name & Versions
- Antivirus Server Name & Versions
- Proxy and backup server name and version

8.12 ACCEPTANCE TESTING, AUDIT AND CERTIFICATION

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

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

As part of Acceptance testing, audit and certification, performed through a third party agency, State shall review all aspects of project development and implementation covering software, hardware and networking including the processes relating to the design of solution architecture, design of systems and sub-systems, coding, testing, business process description, documentation, version control, change management, security, service oriented architecture, performance in relation to defined requirements, interoperability, scalability, availability and compliance with all the technical and functional requirements of the RFP and the agreement. Here it is important to mention that there may be two agencies selected by STATE, one for audit & certification of security and control aspect of the system and the other for audit & certification of overall application 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, work-flow processing time, concurrent sessions supported by the system, Time for recovery from failure, Disaster Recovery drill etc. The performance review also includes verification of scalability provisioned in the system for catering to the requirements of application volume growth in future.

5. Availability

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

6. Manageability Review

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

7. 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.

8. 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.

9. SCOPE OF SERVICES DURING POST-IMPLEMENTATION PHASE

The SI shall be responsible for the overall management of the system including the Application, IT infrastructure and enabling infrastructure maintenance services/ facility management services at all client locations for ensuring adherence of SLAs. SI shall integrate with the existing EMS tool at the State Data Centre that monitors / manages the entire enterprise wide application, infrastructure and network related components.
SI shall provide the Operations and Maintenance Services for a period of 5 years following the deployment and "Go-Live" of the complete solution in Manipur Police.

Scope of Services during Operate and Maintain Phase

As part of the Operate and Maintain services, the SI shall provide support for the software, hardware, and other infrastructure provided as part of this RFP. SI shall also provide five (5) years of comprehensive AMC and extendable upto 3 additional years, comprising of but not limiting to the following:

1. Warranty Support
2. Annual Technical Support (ATS)

3. Handholding Services

a. Central Helpdesk from the Manipur Police designated premises – *for five years from Go-Live of complete CCTNS solution.*

b. Support for the end users at each of the locations including deployment of one competent person per two police stations and one each at Higher Offices for a period of one year to handhold the staff after the Core application and the necessary infrastructure are successfully commissioned in the police offices

c. Software maintenance and support services28 – *for five years from Go-Live of complete CCTNS solution.*

d. Application functional support services – *for five years from Go-Live of complete CCTNS solution.*

e. Other IT infrastructure related support services – *for five years from Go-Live of complete CCTNS solution.*

The services shall be rendered onsite from the Manipur Police designated premises. To provide the support for the police stations, sub-divisional offices, district headquarters, ranges, Manipur Police Headquarters and other locations across the Manipur Police where the software, hardware, and other infrastructure will be rolled out, SI is expected to provide experienced and skilled personnel at each location.

As part of the Warranty Services SI shall provide:

1. SI shall provide a comprehensive warranty, including replacement or repair of defective hardware or equipment as the case may be and on-site free service warranty for 5 years from the date of Go Live for all equipments.
2. SI shall obtain the five year product warranty and five year onsite free service warranty from OEM on all licensed software, computer hardware and peripherals, networking equipments and other equipment for providing warranty support to Manipur Police.
3. SI shall provide the comprehensive manufacturer's warranty and support in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. covered by the RFP. SI must warrant all hardware, equipment, accessories, spare parts, software etc. procured and implemented as per this RFP against any manufacturing defects during the warranty period.

4. SI shall provide the performance warranty in respect of performance of the installed hardware and software to meet the performance requirements and service levels in the RFP.
5. SI is responsible for sizing and procuring the necessary hardware and software licenses as per the performance requirements provided in the RFP. During the warranty period SI shall replace or augment or procure higher-level new equipment or additional licenses at no additional cost to the Manipur Police in case the procured hardware or software is not adequate to meet the service levels.
6. Mean Time Between Failures (MTBF): If during contract period, any equipment has a hardware failure on four or more occasions in a period of less than three months, it shall be replaced by equivalent or higher-level new equipment by the SI at no cost to Manipur Police. However, if the new equipment supplied is priced lower than the price at which the original item was supplied, the differential cost should be refunded to Manipur Police. For any delay in making available the replacement and repaired equipments for inspection, delivery of equipments or for commissioning of the systems or for acceptance tests / checks on per site basis, Manipur Police reserves the right to charge a penalty.
7. During the warranty period SI shall maintain the systems and repair / replace at the installed site, at no charge to Manipur Police, all defective components that are brought to the SI's notice.
8. The SI shall as far as possible repair/ replace the equipment at site.
9. In case any hard disk drive of any server, SAN, or client machine is replaced during warranty / AMC the unserviceable HDD will be property of Manipur Police and will not be returned to SI.
10. Warranty should not become void, if Manipur Police buys, any other supplemental hardware from a third party and installs it within these machines under intimation to the SI. However, the warranty will not apply to such supplemental hardware items installed.
11. The SI shall carry out Preventive Maintenance (PM), including cleaning of interior and exterior, of all hardware and testing for virus, if any, and should maintain proper records at each site for such PM. Failure to carry out such PM will be a breach of warranty and the warranty period will be extended by the period of delay in PM.
12. SI shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.

13. The SI shall ensure that the warranty complies with the agreed Technical Standards, Security Requirements, Operating Procedures, and Recovery Procedures.

14. SI shall have to stock and provide adequate onsite and offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met.

15. Any component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA).

16. The SI shall develop and maintain an inventory database to include the registered hardware warranties.

17. The SI may also be responsible for the comprehensive AMC of existing IT Infrastrucuture procured by Manipur Police in the year 2010 and at the CIPA Police Stations under this phase. Details of the existing hardware which may be required to covered under AMC by the selected bidder through this RFP are attached in Annexure VIII B. Currently this hardware is under AMC cover, however SI will be required to provide AMC post expiry of existing AMC cover, for which the SI is required to provide costing per component as per the commercial format.

As part of the ATS services SI shall provide:

1. SI shall maintain data regarding entitlement for application software upgrades, enhancements, refreshes, replacements and maintenance.

2. If the Operating System or additional copies of Operating System are required to be installed / reinstalled / de-installed, the same should be done as part of ATS.

3. SI should carry out any requisite adjustments / changes in the configuration for implementing different versions of Application Software.

4. Updates/Upgrades/New releases/New versions: The SI shall provide from time to time the Updates/Upgrades/New releases/New versions of the Application software, operating systems, etc. as required. The SI should provide free Updates and Patches of the software and tools to Manipur Police as and when released by OEM.

5. Software License Management. The SI shall provide software license management and control. SI shall maintain data regarding entitlement for application software upgrades, enhancements, refreshes, replacements, and maintenance.

6. SI shall have complete manufacturer's technical support for all the licensed software problems and/or questions, technical guidance, defect and non-defect related issues. SI shall

provide a single-point-of-contact for software support and provide licensed software support including but not limited to problem tracking, problem source identification, problem impact (severity) determination, bypass and recovery support, problem resolution, and management reporting.

7. The SI would be responsible for arrangements with Manufacturer for all the technical support which shall at a minimum include but not limiting to online technical support and telephone support during the Manipur Police's business hours (Business hours in Manipur Police will be from 0700 hours to 2300 hours from (Mon-Sat) with access for SI to the manufacturer's technical support staff to provide a maximum of 4 hour response turnaround time. There should not be any limits on the number of incidents reported to the manufacturer by SI as part of provisioning of support services to Manipur Police. SI shall have access to the online support and tools provided by the manufacturer as well as should have 24x7 access to a variety of technical resources including the manufacturer's knowledge base with complete collections of technical articles specifically for Manipur Police.

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

1. The service will be provided in the local language of the Manipur Police.

2. The help desk service that will serve as a single point of contact for all ICT related incidents and service requests. The service will provide a Single Point of Contact (SPOC) and also resolution of incidents. Manipur Police requires the SI to provide Help Desk services to track and route requests for service and to assist end users in answering questions and resolving problems related to the software application, network, Data Center, Disaster Recovery Center, Client site infrastructure, and operating systems at all locations. It becomes the central collection point for contact and control of the problem, change, and service management processes. This includes both incident management and service request management. SI shall provide sufficient number of lines to contact the Help Desk ensuring all the call are attended without any wait.

3. SI shall provide such type of IT training to the staff of Police that SI remains responsible for providing a second level of support for application and technical support at police stations, sub-divisional offices, district headquarters / Commissionerates (if any), range offices, Manipur Police headquarters and other locations across the Manipur Police where the

software, hardware, and other infrastructure will be rolled out. However, this does not absolve SI from providing first level of support for the aforementioned activities.

4. For all the services of Manipur Police within the scope of this RFP, SI shall provide the following integrated customer support and help.

5. Establish 16X6 Help Desk facilities for reporting issues/ problems with the software, hardware and other infrastructure.

6. SI shall maintain and support to all client side infrastructure including hardware, networking components, and other peripherals.

7. SI shall provide maintenance of Hardware, including preventive, scheduled and predictive Hardware support, as well as repair and / or replacement activity after a problem has occurred.

8. SI shall track and report observed Mean Time Between Failures (MTBF) for Hardware.

9. SI shall provide functional support on the application components to the end users.

10. SI shall also provide system administration, maintenance and management services, LAN management services, and IT security administration services.

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

1. The Software Maintenance and Support Services shall be provided for all software procured and implemented by the SI. The SI shall render both on-site and off-site maintenance and support services to Manipur Police to all the designated locations. The Maintenance and Support Services will cover, all product upgrades, modifications, and enhancements.

2. Updates/Upgrades/New releases/New versions/Patches/Bug fixes. The SI will implement from time to time the Updates/Upgrades/New releases/New versions/Patches/Bug fixes of the Application software and operating systems as required after necessary approvals from Manipur Police about the same.

3. Tuning of application, databases, third party software's and any other components provided as part of the solution to optimize the performance.

4. Amendments in the applications implemented as part of the project to meet the requirements of Manipur Police.

5. The SI shall apply regular patches/ updates/upgrades to the licensed software including the

operating system and databases as released by the OEMs.

6. Software Distribution. SI shall formulate a distribution plan prior to rollout and distribute/install the configured and tested software as per the plan.

7. Software License Management. The SI shall provide for software license management and control. SI shall maintain data regarding entitlement for Application software upgrades, enhancements, refreshes, replacements, and maintenance. SI should perform periodic audits to measure license compliance against the number of valid End User software licenses consistent with the terms and conditions of site license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions and report to Manipur Police on any exceptions to SI terms and conditions, to the extent such exceptions are discovered.

8. The SI shall undertake regular preventive maintenance of the licensed software.

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

1. The Application Functional Support Services shall be provided for all software procured and implemented by the SI. The SI shall render both on-site maintenance and support services to Manipur Police from the development center in Manipur Police.

2. Enhancements and defect fixes. SI shall incorporate changes, and provide enhancements as per the requests made by Manipur Police. SI shall perform changes, bug fixes, error resolutions and enhancements that are required for proper and complete working of the application.

3. Routine functional changes that include user and access management, creating new report formats, and configuration of reports.

9. SI shall provide user support in case of technical difficulties in use of the software, answering procedural questions, providing recovery and backup information, and any other requirement that may be incidental/ancillary to the complete usage of the application.

10. The SI shall migrate all current functionality to the new / enhanced version at no additional cost to Manipur Police and any future upgrades, modifications or enhancements of the Application software.

11. The SI shall perform user ID and group management services.

12. The SI shall maintain access controls to protect and limit access to the authorised End Users of the Manipur Police.

13. The services shall include administrative support for user registration, creating and maintaining user profiles, granting user access and authorisation, providing ongoing user password support, announcing and providing networking services for users and providing administrative support for print, file, directory and e-mail servers.

Exit Management and Transition – Capacity Building at Manipur Police

After the exit of the SI, Manipur Police shall take up the management of CAS (State). Therefore before the exit of the SI, Manipur Police must be strengthened and capacity must be developed for them to manage CAS. The SI must plan the capacity building initiative to enable Manipur Police to manage CAS, and will collaborate with them to implement the plan. The SI shall create a detailed plan for Capacity Building (CB) required at Manipur Police to manage CAS and a Transition Plan (implemented over a minimum period of three months) to affect the handover to the department; and implement the same in collaboration with Manipur Police before the completion of their engagement.

10. IMPLEMENTATION AND ROLL-OUT PLAN

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

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

assistance for the key officers (State Mission Team, District Mission Team, District Core Team) of the Districts / State during the design and implementation of CCTNS in the State.

One of the important factors that would determine the success of the CCTNS implementation in the State is the continuous availability of domain experts to the implementation team. SI shall put together a team of at least five (5) domain experts with a minimum of 10 years of experience in the State Police Department who will work on this project on a full time basis during the entire duration of the project.

List of Indicative Deliverables:

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

and Curriculum

d. Training Material

6. District-wise Roll-out / Implementation Plans

11. SERVICE LEVELS

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

ANNEXURE 1

DETAILS OF THE TECHNOLOGY STACKS FOR CAS (STATE) AND CAS (CENTER)

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

The Technical Details for CAS (State) Solution Stack 1 and Stack2, CAS (State) Offline solution, CAS (Centre) Solution are provided in subsequent tables. Bidders are requested to bid with only one (1) stack:

CAS (State) Solution - Stack 1

	Proposed Solution by Software Development Agency	Version and Year of Releases	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
Reporting Engine	Jasper Reports	3.7	Jasper	Reporting Services	

Email/Messaging	Q-Mail	1.4	Qmail Community	E-Mail Solution	
Search Engine	Search: Unstructure data: using openCMS search features Structured Data 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	openCMS	7.5.1	OpenCMS	Content Management System	

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

CAS (State) Solution - Stack 2

Proposed Solutionby	**Proposed Solution by Software Development Agency**	**Version and Year of Releases**	**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	Qmail Community	E-Mail Solution	
Search Engine	Search: Unstructure data: using openCMS search features Structured Data: SQL DB Search Engine & Custom application interface	N/a	N/a	N/a	N/a
Portal Server	IIS	6	Microsoft	Web & App Server	Microsoft
Workflow Engine	Windows Workflow Foundation	N/a	N/a	N/a	N/a
Rules Engine	Custom Built	N/a	N/a	N/a	N/a
Directory Services	Microsoft Active Directory	2008	Microsoft	LDAP	Microsoft

DMS/CMS	Windows Sharepoint Services	N/a	N/a	N/a	Microsoft
Security	Physical Security, Network Sercurity, DB Encryption (MySQL), DB Access Controls, Role Based Access Control (Custom Developed), LDAP (Sun Directory Services)	N/a	N/a	N/a	N/a
Identity Management	Microsoft Active Directory	2008	Microsoft	LDAP	Microsoft
Audit	IIS Log, Custom Built	N/a	N/a	N/a	N/a
ETL	SQL Server ETL	2008	Microsoft	ETL	Microsoft

CAS (State) Offline Solution

indiThe below list is indicative only	Proposed Solution by Software Development Agency	Version and Yr. of Releases	Original Supplier	Description(include major features/services only)	Support Provided By
Synchronization Solution	Custom Built	N/a	N/a	N/a	N/a

Application Container	Apache Tomcat	6.0	Apache Foundation	J2EE Application Container	
Database	MySQL / SQL Express	5.1/2008	SUN / Microsoft	DB Store	SUN / Microsoft

CAS (Center) Solution (only for information of Bidders)

The below list is indicative only	Proposed Solution by Software Development Agency	Version and Yr. of Releases	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				
Reporting Engine	Jasper Reports	3.7	Jasper	Reporting Services	
Search	Search:	N/a	N/a	N/a	N/a

Engine	Unstructure data: using Alfresco search features Structured Data: Sybase DB Search Engine & Custom application interface				
Portal Server	Glassfish Application Server	7.0	SUN	HTTP Server	SUN
Workflow Engine	jBPM	4.0	JBoss	Workflow engine	
Rules Engine	Custom Built	N/a	N/a	N/a	N/a
Directory Services	Sun Directory Services	7.0	SUN	LDAP	SUN
DMS/CMS	Alfresco				
Email/Messaging	N/a				
Security	Physical Security, Network Sercurity, DB Encryption	N/a	N/a	N/a	N/a

	(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	N/a	N/a	N/a	N/a
ETL + Data Quality	Sybase ETL	15.1	Sybase	ETL	Sybase

ANNEXURE 2
SERVICE LEVELS

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

1. **Definitions.**

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

(b) **"Scheduled operation time"** means the scheduled operating hours of the System for the month. All scheduled maintenance time on the system would be deducted from the total operation time for the month to give the scheduled operation time. The total operation time for the systems and applications within the Primary DC

(c) , DRC and critical client site infrastructure will be 24X7X365. The total operation time for the client site systems shall be 18 hours.

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

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

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

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

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

2. **Interpretations.**

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

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

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

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

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

(f) The SLA parameters shall be monitored on a monthly basis as per the individual SLA parameter requirements. However, if the performance of the system/services is degraded significantly at any given point in time during the contract and if the

immediate measures are not implemented and issues are not rectified to the complete satisfaction of the stateor an agency designated by them, then the statewill have the right to take appropriate disciplinary actions including termination of the contract.

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

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

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

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

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

Implementation Phase SLAs

1. Capacity Building

Service Level Description	Measurement
Capacity Building	At least 80% of the trainees within the training program should give a rating of satisfactory or above. Severity of Violation: High

	This service level will be monitored and measured on a per District basis through feedback survey to be provided to each attendee within the program. If the training quality in the program falls below the minimum service level, it will be treated as one (1) violation. The total number of violations for the payment period will be the cumulative number of violations across all the programs across all Districts in the payment period.

2. Data Migration / Digitization

Service Level Description	Measurement
Data Migration	Error rate in a batch should be less than 0.5%. Severity of Violation: Medium This service level will be measured on a monthly basis for each Police Station / Higher Office. If the data migration / digitization service level in a police station / higher office falls below the minimum service level, it will be treated as one (1) violation. The total number of violations for the payment period will be the cumulative number of violations across all the police stations / higher offices in the payment period.

3. Violations and Associated Penalties

(a) The primary intent of Penalties is to ensure that the system performs in accordance with the defined service levels. Penalties are not meant to be punitive or, conversely, a vehicle for additional fees.

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

(i) The performance will be measured for each of the defined service level metric against the minimum / target service level requirements and the violations will be calculated accordingly.

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

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

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

Post Implementation Phase SLAs

1. Client Site Infrastructure Systems

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

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

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

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

2. Handholding Support: Client Site Support

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

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

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

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

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

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

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td>Client Site Support Performance</td><td>80% of the Level 1 Incidents at each site should be resolved within 2 business hours from the time call is received / logged whichever is earlier. The maximum resolution time for any incident of this nature shall not exceed 8 business hours.
Severity of Violation: Medium
This service level will be measured on a monthly basis for each implementation site.
If the performance in a month for an implementation site falls below the minimum service level, it will be treated as one (1) instance. The total number of instances for the six-month period will be the cumulative number of instances across all the months across all sites in the six-month period.
Average number of instances per month = (Total number of instances for the six-month period) / 6
<table>
<tr><th>Average number of instances per month</th><th>Violations for calculation of penalty</th></tr>
<tr><td>>0 & <=4</td><td>1</td></tr>
<tr><td>>4 & <=8</td><td>2</td></tr>
<tr><td>>8 & <=12</td><td>3</td></tr>
<tr><td>>12</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>Client Site Support Performance</td><td>80% of the Level 2 Incidents at each site should be resolved within 6 business hours from the time a call is received / logged whichever is earlier. The maximum resolution time for any incident of this nature shall not exceed 48 hours.</td></tr>
</table>

<table>
<tr><td></td><td>
Severity of Violation: Medium
This service level will be measured on a monthly basis for each implementation site.
If the performance in a month for an implementation site falls below the minimum service level, it will be treated as one (1) instance. The total number of instances for the six-month period will be the cumulative number of instances across all the months across all sites in the six-month period.
Average number of instances per month = (Total number of instances for the six-month period) / 6
<table>
<tr><th>Average number of instances per month</th><th>Violations for calculation of penalty</th></tr>
<tr><td>>0 & <=4</td><td>1</td></tr>
<tr><td>>4 & <=8</td><td>2</td></tr>
<tr><td>>8 & <=12</td><td>3</td></tr>
<tr><td>>12</td><td>4</td></tr>
</table>
Replacement of hardware equipment shall be done within 7 days of notification by the state / UT. These equipments would have failed on four or more occasions in a period of less than three months or six times in a period of less than twelve months. (Mean Time Between Failure Condition)
Severity of Violation: High
Each instance of non-meeting this service level will be treated as one (1) violation.
</td></tr>
</table>

(f) Handholding Support: Application Support

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

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

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

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

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

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

<table>
<tr><th>Service Level Description</th><th colspan="2">Measurement</th></tr>
<tr><td rowspan="4">Application Support Performance</td><td colspan="2">95% of the Level 1 defects shall be resolved within 4 business hours from the time of reporting full details.
Severity of Violation: High
This service level will be monitored on a monthly basis.</td></tr>
<tr><td>Performance over the six month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>< 95% & >= 90%</td><td>1</td></tr>
<tr><td>< 90% & >= 85%</td><td>2</td></tr>
</table>

<table>
<tr><td></td><td><table>
<tr><td>< 85%</td><td>3</td></tr>
<tr><td colspan="2">In addition to the above, if the service level in any month in the six-month period falls below 85%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td colspan="2">95% of the Level 2 defects shall be resolved within 72 hours from the time of reporting full details. Severity of Violation: High
This service level will be monitored on a monthly basis.</td></tr>
<tr><td>Performance over the six month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>< 95% & >= 90%</td><td>1</td></tr>
<tr><td>< 90% & >= 85%</td><td>2</td></tr>
<tr><td>< 85%</td><td>3</td></tr>
<tr><td colspan="2">In addition to the above, if the service level in any month in the six-month period falls below 85%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
</table></td></tr>
<tr><td>Application Support Performance</td><td><table>
<tr><td colspan="2">100% of the Level 3 defects shall be resolved within 120 hours from the time of reporting full details.
Severity of Violation: High
This service level will be monitored on a monthly basis.</td></tr>
<tr><td>Performance over the six month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>< 100% & >= 90%</td><td>1</td></tr>
</table></td></tr>
</table>

	< 90% & >= 80%	2
	< 80%	3
	In addition to the above, if the service level in any month in the six-month period falls below 80%, one (1) additional violation will be added for each such month to the overall violations for this service level.	
	Up to date of the documentation of the design, modifications, enhancements, and defect-fixes in the half-yearly period. Severity of Violation: Medium This service level will be measured on a half-yearly basis. Each instance of non-meeting this service level will be treated as one (1) violation.	

(g) Network Uptime:

Severity of Violation: High

This service level will be monitored on a monthly basis.

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

Service Level Description	Measurement
Network Uptime	Availability of the network and all related components at all the implementation sites shall be at least 99% Severity of Violation: High This service level will be measured on a monthly basis for each implementation site. If the network availability in a month falls below the minimum service level, it will be treated as one (1) violation.

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

(h) Handholding Support: Helpdesk Support

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

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

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

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

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

<table>
<tr><th>Service Level Description</th><th colspan="2">Measurement</th></tr>
<tr><td rowspan="4">Helpdesk Performance</td><td colspan="2">98% of the calls shall be answered within 45 seconds</td></tr>
<tr><td colspan="2">Severity of Violation: High
This service level will be monitored on a monthly basis</td></tr>
<tr><td>Performance over the six-month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>< 98% & >= 90%</td><td>1</td></tr>
<tr><td></td><td>< 90% & >= 80%</td><td>2</td></tr>
</table>

	< 80%	3
	In addition to the above, if the service level in any month in the six-month period falls below 80%, one (1) additional violation will be added for each such month to the overall violations for this service level.	
	98% of the incidents within helpdesk resolution capacity shall be resolved in a cycle time of 24 hours Severity of Violation: High This service level will be monitored on a monthly basis	
	Performance over the six-month period	**Violations for calculation of penalty**
	< 98% & >= 90%	1
	< 90% & >= 80%	2
	< 80%	3
	In addition to the above, if the service level in any month in the six-month period falls below 80%, one (1) additional violation will be added for each such month to the overall violations for this service level	
Helpdesk Performance	98% of the non SI supported incidents shall be routed to the appropriate service provider within 30 minutes. Severity of Violation: Medium This service level will be monitored on a monthly basis.	
	Performance over the six-month period	**Violations for calculation of penalty**
	< 98% & >= 90%	1
	< 90% & >= 80%	2

	< 80%	3
	In addition to the above, if the service level in any month in the six-month period falls below 80%, one (1) additional violation will be added for each such month to the overall violations for this service level	
Helpdesk Performance	80% of the Level 1 calls shall be resolved within 2 hours from call received / logged whichever is earlier. The maximum resolution time for any incident of this nature shall not exceed 8 business hours. Severity of Violation: High This service level will be monitored on a monthly basis	
	Performance over the six month period	**Violations for calculation of penalty**
	< 80% & >= 70%	1
	< 70% & >= 60%	2
	< 60%	3
	In addition to the above, if the service level in any month in the six-month period falls below 60%, one (1) additional violation will be added for each such month to the overall violations for this service level.	

<table>
<tr><td>Helpdesk Performance</td><td>
80% of the Level 2 calls shall be resolved within 6 hours from call received / logged whichever is earlier. The maximum resolution time for any incident of this nature shall not exceed 48 hours.
Severity of Violation: High
This service level will be monitored on a monthly basis.
<table>
<tr><th>Performance over the six month period</th><th>Violations for calculation of penalty</th></tr>
<tr><td>< 80% & >= 70%</td><td>1</td></tr>
<tr><td>< 70% & >= 60%</td><td>2</td></tr>
<tr><td>< 60%</td><td>3</td></tr>
</table>
In addition to the above, if the service level in any month in the six-month period falls below 60%, one (1) additional violation will be added for each such month to the overall violations for this service level.
80% of the Level 3 calls shall be reported on status and action to be communicated within 24 hours from call received / logged whichever is earlier. The maximum resolution time for any incident of this nature shall not exceed 72 hours.
Severity of Violation: High
This service level will be monitored on a monthly basis
<table>
<tr><th>Performance over the six month period</th><th>Violations for calculation of penalty</th></tr>
<tr><td>< 80% & >= 70%</td><td>1</td></tr>
<tr><td>< 70% & >= 60%</td><td>2</td></tr>
</table>
</td></tr>
</table>

	< 60%	3
	In addition to the above, if the service level in any month in the six-month period falls below 60%, one (1) additional violation will be added for each such month to the overall violations for this service level.	
Datacenter Support Performance	Replacement of hardware equipment shall be done within 15 days of notification by the state / UT. These equipments would have failed on four or more occasions in a period of less than three months or six times in a period of less than twelve months. (Mean Time Between Failure Condition) Severity of Violation: High Each instance of non-meeting this service level will be treated as one (1) violation.	
	Up to date of the documentation of the design, modifications, enhancements, and fixes. Severity of Violation: Medium	
	This service level will be measured on a half-yearly basis. Each instance of non-meeting this service level will be treated as one (1) violation.	

(c) **Reporting**

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

<table>
<tr><th>Service Level Description</th><th colspan="2">Measurement</th></tr>
<tr><td rowspan="4">Availability and Performance Report</td><td colspan="2">Provide monthly SLA compliance reports, monitoring and maintenance related MIS reports by the 5th of the following month.
Severity of Violation: Medium
This service level will be monitored on a monthly basis. If the monthly SLA compliance report related to the service level metrics is not provided in the given timeframe, it will be treated as one (1) instance.
The total number of instances for the six-month period will be the cumulative number of instances across all the months in the six-month period</td></tr>
<tr><td>Total number of instances over the six month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>>0 & <=3</td><td>1</td></tr>
<tr><td>> 3</td><td>2</td></tr>
</table>

(d) **Credits for Successful Application Uptake**

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

Service Level Description	Measurement
CCTNS Uptake	The following metrics will be measured at the end of each reporting period for each District that has been declared as "Go Live": 1. Number of key transactions carried through internet (ex: Transactional such as submitting an application for a no-

<table>
<tr><td></td><td>objection certificate and Informational such a requesting the status of a case)
2. Number of active users profiles in CCTNS
3. Number of read-write transactions on CCTNS system
4. Number of Searches carried out on data in CCTNS
5. Total number of FIRs prepared through CCTNS
6. Total number of Crime Details Forms prepared through CCTNS
7. Total number of Key Investigation Forms prepared through CCTNS
8. Total number of Arrest Cards prepared through CCTNS
9. Total number of ChargeSheets prepared through CCTNS
10. Quality (recency and accuracy) of information available in CCTNS
11. Number of cases reported to be solved because of the availability of CCTNS
12. Number of ad-hoc requests successfully responded to using CCTNS
13. Turnaround Time for submitting the monthly and annual crime/criminal information to NCRB from Manipur

A credit will be gained for each of the above parameters if the uptake for that parameter shows significant improvement.</td></tr>
<tr><td></td><td>The following table applies for each of the above parameters:
<table><tr><th>% increase over the measurement in the last reporting period</th><th>Credits</th></tr><tr><td>>5 & <=10%</td><td>2</td></tr><tr><td>>10 & <=15%</td><td>3</td></tr><tr><td>> 15%</td><td>4</td></tr></table></td></tr>
</table>

(e) **Violations and Associated Penalties**

(a) The primary intent of Penalties is to ensure that the system performs in accordance with the defined service levels. Penalties are not meant to be punitive or, conversely, a vehicle for additional fees.

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

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

ii. The performance will be measured for each of the defined service level metric against the minimum / target service level requirements and the violations will be calculated accordingly.

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

i. If the total number of credits gained by the SI is lower than the total number of high severity violations in the reporting period, the total number of credits will be subtracted from the total number of High Severity Violations in the reporting period for the calculation of Penalties.

ii. If the total number of credits gained by the SI is higher than the total number of high severity violations in the reporting period, the resultant total number of high severity violations in the reporting period for calculation of penalties will be considered as zero (0).

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

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

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

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

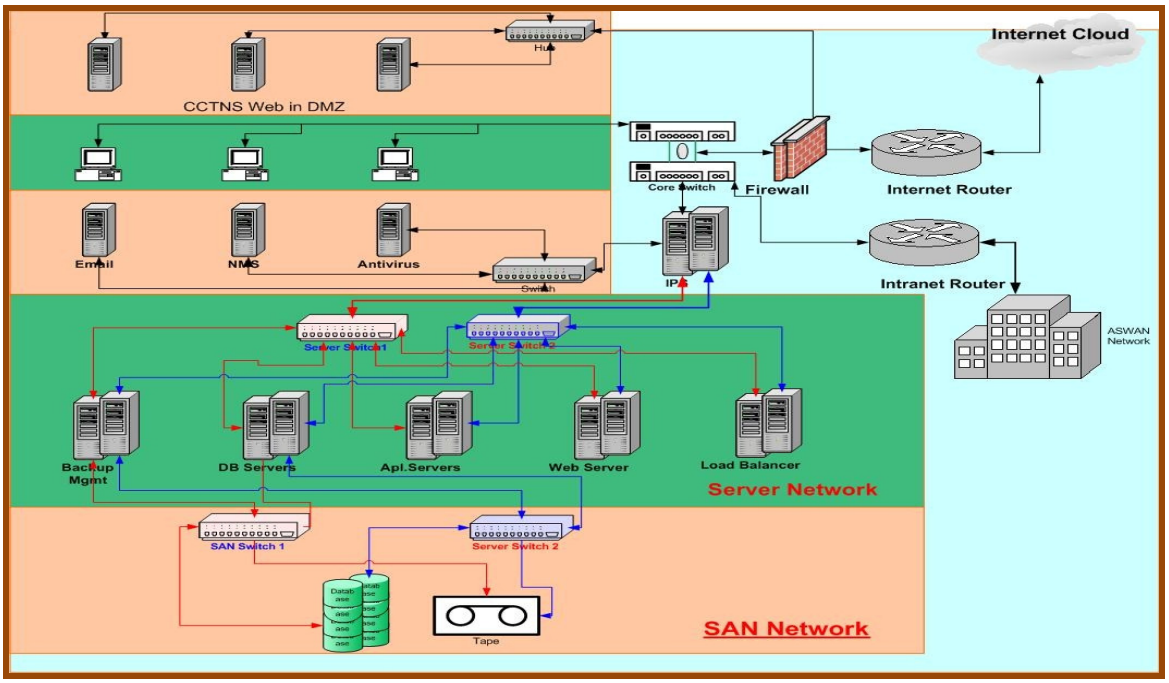
vii. Penalties applicable for not meeting **a medium (M) critical** performance target in two consecutive half yearly periods on same criteria shall result in additional deduction of 3% of the respective half yearly payment to the SI. Penalty shall be applicable separately for each such medium critical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

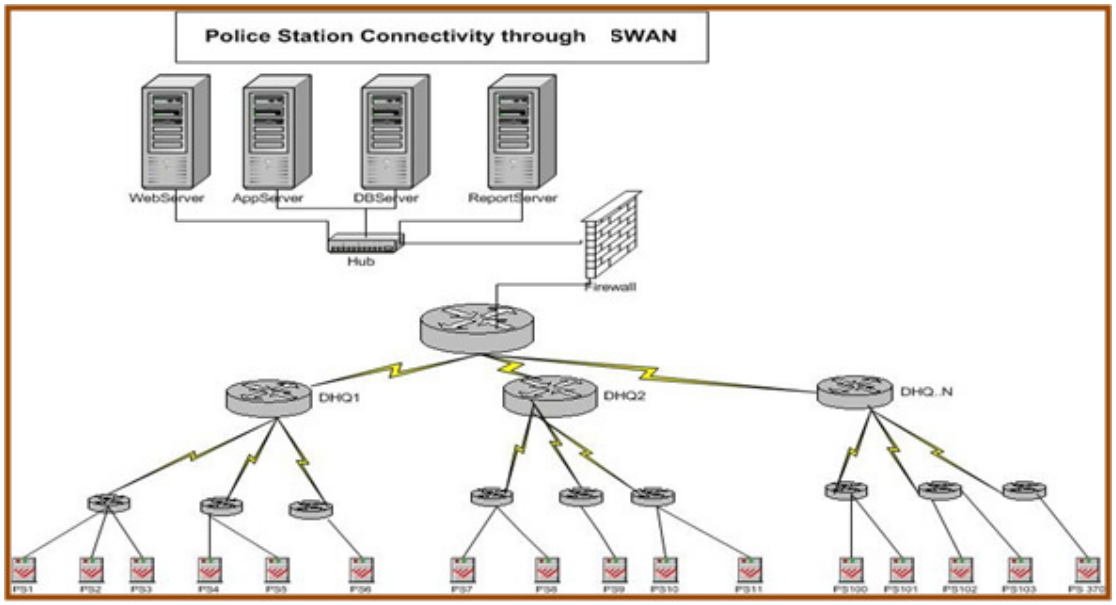
viii. Penalties applicable for not meeting **a low (L) critical** performance target in two consecutive half yearly periods on same criteria shall result in additional deduction of 2% of the respective half yearly payment to the SI. Penalty shall be applicable separately for each such medium critical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

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

ANNEXURE 3

Guidelines on Network Architecture and details provided by BSNL with respect to Connectivity





The overall connectivity can be planned in two way for CCTNS :

1. Complete wireless
2. MPLS VPN (both wire and wireless)

Wireless

It is planned to have a centralized architecture for implementing the CCTNS in Manipur Police. In order to achieve this, it is proposed to connect all the office of Manipur Police to the Data Centre at Imphal using the Manipur State Wide Network (MSWAN). It may be mentioned that, MSWAN which is planned to have 160 nos. of POPs across the state of Manipur when fully operational. The police stations and other offices will be connected to the nearest POP using wireless, which is considered to be most reliable. Wireless Last Mile data Connectivity is to be implemented from SWAN PoPs in the state. A 4Mbps Back haul equipments for connecting all the remotes sites and 300Mbps Back haul for connectivity between MSWAN Network Operating Centre, Imphal and DGP office, Imphal may be considered. The solutions may suit the weather condition of Manipur by incorporating through line surge suppressor on data and power cables. All the towers are equipped with lightning protection and earth pits. The net work can use bandwidth , which will be free as such there will not be any recurring cost.

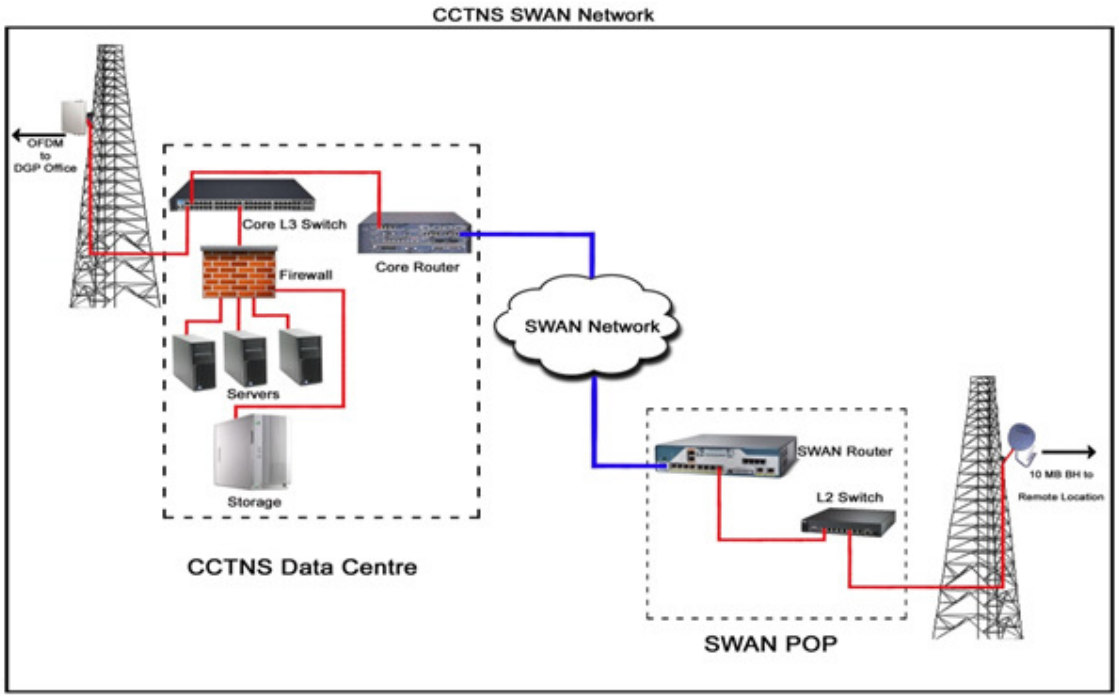
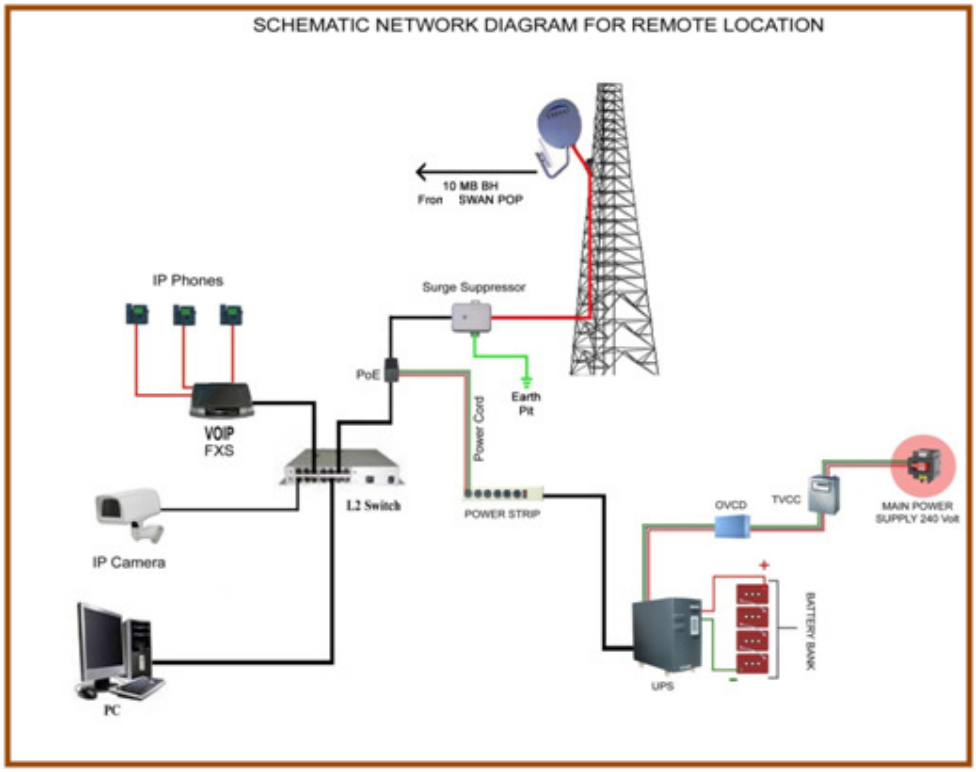


Diagram showing for connectivity at Remote Police Location

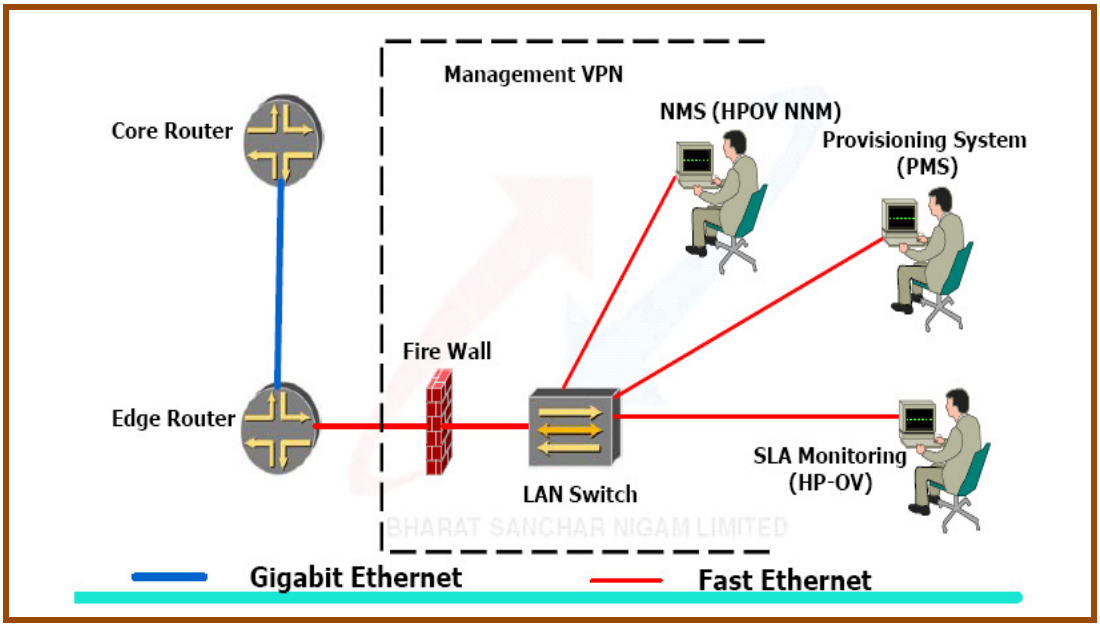


To avoid recurring cost of license free, it is preferred to configure the network with equipment operating in license free band. i.e. 2.4 GHz & 5.7 GHz with I-DES functions. I-DES will help to work in frequency congestion zone with help of adoptive modulation to the different spot frequency of same frequency band. Selection of proven rugged and reliable equipment will eventually reduced the cost of ownership, by way of reduced maintenance and high level of availability (99.9%).

MPLS VPN Network (wire and wireless)

MPLS VPN is a technology that allows a Service Provider to have complete control over parameters that are critical to offering customers service guarantees with regard to bandwidth throughputs, latencies and availability. The technology enables secure Virtual Private Networks (VPN) to be built and allows scalability that will make it possible for BSNL to offer assured growth to its customers without having to make significant investments. BSNL would now be geared to provide Bandwidth on demand, Video Conferencing, Voice Over IP (VoIP) and a host of other value added services as per demand. This Network can be easily implemented and built for better traffic management . Any Differentiated Services possible and further network considered as reliable due to built in redundancy

NOC Lay out Diagram of MPLS VPN Network



ANNEXURE 4

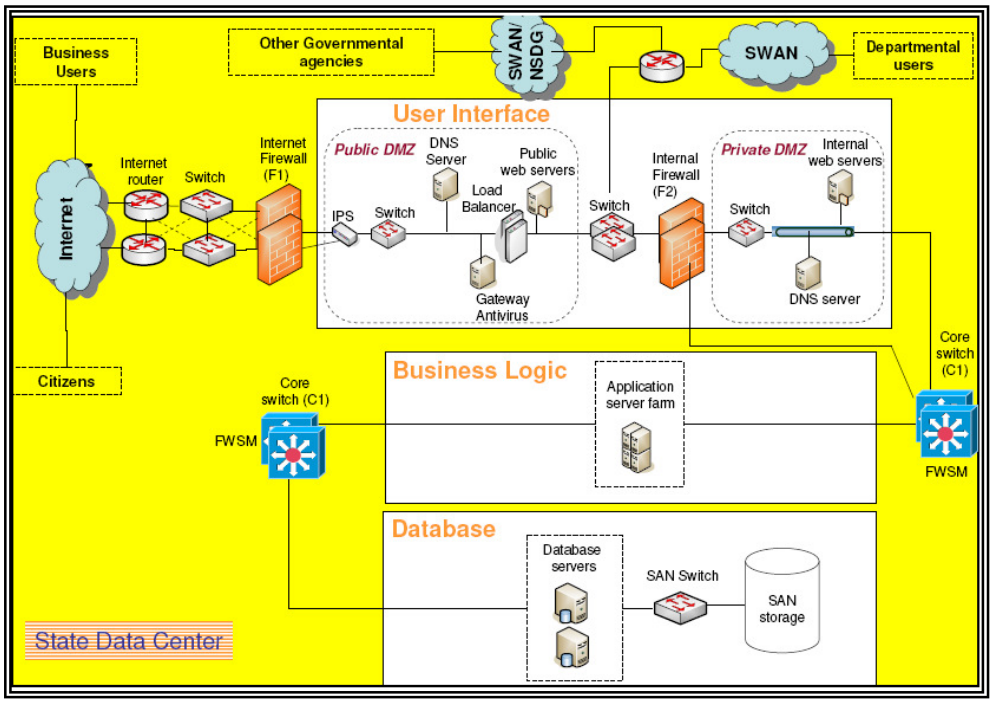
Suggested Technical Architecture and Standards

CCTNS shall be deployed on a centralized architecture wherein various offices of Police Department connect to the system through State Data Centre.

Deployment Architecture

The deployment architecture would be centralized (3) three-tier deployment architecture for the CCTNS application. Three-tier deployment architecture would allow any of the three tiers to be up-graded or replaced independently as requirements change. Any change in the business rules, would need little changes to be made in the business logic layer, and if any, to the user interface or the database tier. Illustrative three-tier deployment architecture has been shown as below.

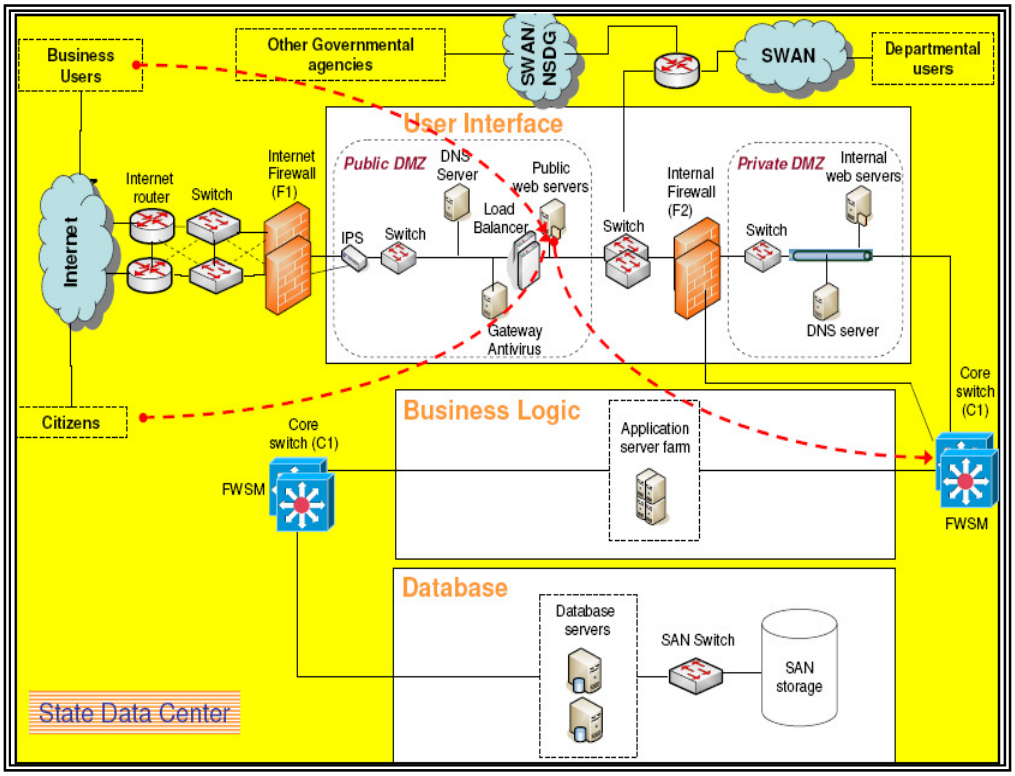
Centralized Diagram of the Deployment Architecture



Presentation Layer

The user interface would receive requests from users and would output results back by communicating with other tiers. The State has to define the various infrastructure components to be hosted in a Private and Public Demilitarized Zone (DMZ). E.g. Firewalls, intrusion prevention systems (IPS), Load balancers, gateway level anti-virus system etc would be deployed in the Public Demilitarized Zone. State has to explain the access mechanisms for user categories defined i.e. 'External users and Internal users' to the various zones. For example, External users (citizens/business users) would be able to access non-restricted areas of the application over internet. The public web server and the internal firewall a part of the public DMZ would be configured to render only those application pages that can be accessed publicly.

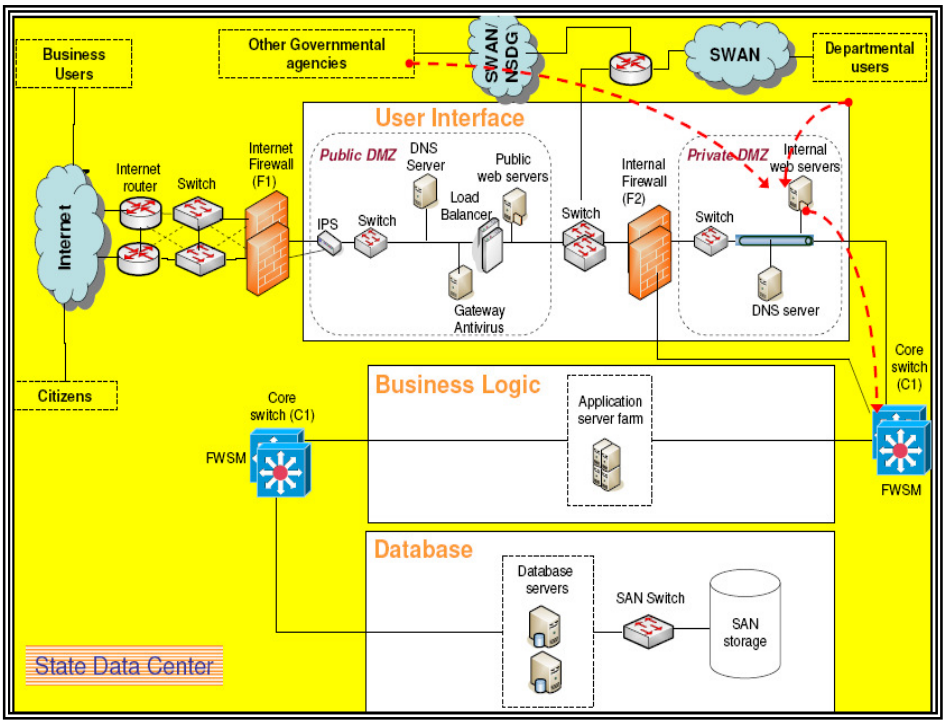
The following figure depicts the access path in case of external users:



Deployment Internal User

a. Internal users (Internal departmental) would be connected through SWAN and would access the application over intranet.

b. Other government agency communicating between the various CCNTNS application would access the applications via web-services (over NSDG/SWAN). Web Services are de facto standard for communication across different hardware platforms, operating systems and business processes. They are modeled according to publicly accepted open standards, so that different implementations running on different operating systems can interoperate. Common markup languages for Web Services communication used are XML messages, SOAP protocol (which is also based on XML) as common message format for exchanging information and WSDL (based on XML) as common format for Web Service description. Web Services are published via UDDI (based on XML).



ANNEXURE 5

Governance Structure

The table below provides the committees /teams that form part of the governance structure and their roles and responsibilities as defined in the CCTNS implementation guidelines provided by MHA

Committee/Team	Roles & Responsibilities
State Apex Committee	• Reviewing progress of the Project, • Overseeing utilization of funds, • Policy Directions and Guidance for successful execution of the Project, • Ensuring continuance of Mission Leader for sufficient duration, and • Creating a supporting environment for the success of the project
State Empowered Committee	• Disbursement of funds to Districts and other units/agencies • Approval of BPR proposals • Sanction for various project components, as may be specified, including the Hardware/Software procurement as per the specifications from NIC • Approval of various Project Components and 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
State Mission Team	• Operational responsibility for the Project • Formulating Project Proposals • Getting sanction of GOI for various projects • Hardware rollout and operationalization • 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
District Mission Team	• 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

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

Members		Composition
Member 1	Chairperson	Chief Secretary
Member 2	Co-Chair	Principal Home Secretary
Member 3		Secretary Finance
Member 4		IT Secretary, Govt. of Manipur
Member 5		Head of SCRB
Member 6		Representative of NIC
Member 7		Representative of GOI, MHA
Member 8	Convener	Nodal Officer (CCTNS project), i.e., SP(CR)
Member 9		GM(Telecom) BSNL

The composition of the **State Empowered Committee** is as follows:

Members		Composition
Member 1	Chairperson	DGP
Member 2	Co-Chair	IGP
Member 3		DIGP (Crime) as supervising officer of SP (Cr)
Member 4		Representative of NCRB
Member 5		Representative of Home Department i.e. Joint Secy. Home Govt. of Manipur
Member 6		Representative of Finance Department i.e. Joint Secy. Finance, Govt. of Manipur
Member 7		Director, IT Govt. of Manipur
Member 8		Head of NIC, Manipur
Member 9	Convener	Nodal Officer, i.e. SP(Crime)

The composition of **State Mission Team** is as follows:

Mission Leader	DIGP (Crime)
Member	SP (Crime)
Member	State Informatics Officer, NIC

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

Chairperson	SP District
Convener	Addl. SP/DY.SP of District
Member	DIO of NIC, District Centre
Member	An officer from District Police having knowledge about computers

Other Agencies

State Designated Agency

"State Designated Agency", (agency/society/public sector unit) at the state level that would serve as a channel for transfer of funds from GOI to states and from state governments to the vendors implementing CCTNS. Identification of such an agency/society and routing funds through it would ensure the following:

- Timely payments for time-critical events
- Strict control on utilization of funds for intended purpose
- Sustainability even beyond plan period
- Enable States in timely hiring of experts and internal capacity building

The State Designated Agency for Manipur CCTNS is as follows :

"Manipur Police Housing Corporation Ltd., Imphal, Manipur"

ANNEXURE 6

Indicative Technical Specifications

1. Desktops

DETAILS
Processor: Intel Core 2 Duo processor (2.93 GHz or higher) and 1066 MHz FSB
Chipset : Intel 4 Series
Cache: 3 MB L2 Cache
Memory Type: 2 GB DDR-2 @ 1066 MHZ or higher with 4 GB expandability
Internal Hard Disk : 320 GB Serial ATA 7200 RPM or higher
Optical Drive: 8X or better DVD ROM Drive
Display size: 47 cm (18.5 inch) measured diagonally TFT Digital Color Monitor
Graphics Controller: Integrated Intel Graphics Media Accelerator
Bus Architecture : 2 PCI, 1 PCI Express X1 and 1 PCI Express X16
Cabinet : Minitower
External I/O ports : 6 USB Ports (with atleast 2 in front), 1 standard serial port, audio ports for headphone and microphone in front
Networking Facility : 10/100/1000 on board integrated Network Port
Power Management : Screen blanking, Hard Disk & System Idle Mode in power on, Set up Password, Power Supply SMPS Surge protected
Keyboard: USB Keyboard with 104 or higher keys
Pointing device: USB Optical Mouse, 2 button scroll
Bays : 4 nos. (2 nos. 5.25 inches for Optical Media Drives and 2 nos. 3.5 inches for Hard Disk Drives)
Software : Preloaded MS Windows 7 Professional, MS Office 2007 Professional Plus or latest ver., Antivirus (3 yrs)

Warranty: 3 Years Part, 3 Years Labour, 3 Years On-Site
OEM Certifications : ISO 9001-14001, ISO 9001-2008, Greenpeace International

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 Bill of Quantity. All software licenses (if softwares not preloaded) should be in the name of DGP, Manipur Police, Imphal. All System Software licenses if applicable, shall be genuine, perpetual, full use and should provide patches, bug fixes, security patches, and updates directly from the respective OEM for the contract period. The software product used should have well defined product roadmap by the respective OEM. 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 Manipur Police any developer / manufacturer warranties will be transferred to Manipur Police at no additional charge. All warranty documentation (whether expired or not) will be delivered to Manipur Police at the issuance of final acceptance certificate.

2. HDD 160 GB :

CRITERIA	DETAILS
	Internal – Serial ATA
Speed	5400 RPM
Hard Disk Size	

3. Duplex Laser Printer (Network)

CRITERIA	DETAILS
Speed	28 PPM (A4) or higher
Processor	400 MHz or higher
Resolution	Min. 1200 * 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 (10/100 Mbps)
Duplex	Yes
Paper Support	A4
Compatibility	Windows 7/Windows XP

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

CRITERIA	DETAILS
Functions	
All-in-one functions	Print, Copy, Scan
Multitasking Capability	Yes
Printing Specifications	
Print Speed	18 PPM or higher
Monthly Duty Cycle	Upto 8000 pages

Print Technology	Upto 1200 * 1200 dpi
Scanner Specifications	
Scanner Type	Flatbed, ADF
Scan Resolution	Upto 1200 dpi
Bit Depth	24 bit, 64 bit
Scan Size Maximum	A4, A3
Scan Speed (default)	15 ppm or higher
Copier Specifications	
Copy Resolution, Black	Upto 600*600 dpi
Copy Resolution, Color	Upto 1200*1200 dpi
Maximum no. of copies	99
Compatibility	Windows 7/Windows XP

5. Online UPS System

CRITERIA	DETAILS
	True Online, Double Conversion
Capacity	2 KVA
Input Volt	120 – 270 V (on full load)

Input Power Factor	> 0.95
Output Volt	230 V +/- 1%
Output Frequency	50 Hz +/- 1%
Wave Form	Sine Wave
Distortion	THD < 3%
Battery backup time on full rated load	2 hours
LED / LCD Bar Graph	Load level & Battery level
Rack	Suitable metallic rack for housing of batteries
SNMP Support	Yes

6. Portable Generator Set

CRITERIA	DETAILS
Rated Power	2 KVA
Rated Current	AC 3.0 A / AC 7.1 A
Ignition System	Transistor Controlled Ignition (TCI)
Fuel Tank Capacity (diesel)	2.7 L minimum
Fuel Tank Capacity (petrol)	0.25 L minimum
Continuous running hours	6 hours
Frequency (Hz)	50 Hz
Rated Output (VA)	350 VA
Maximum Output	450 VA

(VA)	
Silent Type	Yes

7. Finger Print Reader

CRITERIA	DETAILS
Sensor	Optoelectronic
Prism Architecture	Dual Prism
Size of Window	18 mm * 22 mm minimum
Glass Thickness	25 mm
Resolution	512 PPI upgradable
Scanning Time	0.01 sec
Distortion Rate	0.1%
Computer Interface	USB 2.0
Operating Temperature	0 – 55 Degree C
Operating System Support	Windows 7 / XP

8. Electronic Pen

CRITERIA	DETAILS
Data Communication	USB 1.1 standard
Built-in battery	Rechargeable battery
Continuous Writing Time	2 hours minimum
Charging Time	2 hours approx.

Operating System Support	Windows 7 / XP

9. Digital Camera

CRITERIA	DETAILS
Pixels	12 Megapixels minimum
LCD Monitor	
Type	TFT
Display Size	2.7 inches minimum
Recording Format	JPEG
Zoom	4X or higher
Recording Media	SD Memory Card, SDHC Memory Card, SDXC Memory Card, Multimedia Card
Self Timer	Yes
Shooting Modes	Auto, Portrait, Landscape, Night Snapshot, Indoor, Face self-timer, Low Light, Beach, Underwater, Foliage, Snow, Fireworks, Movie, Documents
White Balance	Auto/Daylight/Cloudy/Fluorescent/Incandescent/Flash
Flash Function	Auto/Red Eye Reduction/Off/Face Detection/Noise reduction
USB Connectivity	Yes
Operating System Support	Windows 7/XP

10. Port Network Switch 10/100 MBPS

CRITERIA	DETAILS
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 – 10/100 BaseT
Switching Method	Store and Forward
Switch Fabric	4.8 Gbps
Physical Specifications	Metal housing with Side air vents with proper Air Cooling design
Power Requirements	Universal AC input: 100 to 240 VAC, 50 to 60 Hz