E-GOVERNANCE MISSION MODE PROJECT (MMP)

CRIME & CRIMINAL TRACKING NETWORK AND SYSTEMS
(CCTNS)

REQUEST FOR PROPOSAL FOR SELECTION OF SYSTEM INTEGRATOR FOR IMPLEMENTING, COMMISSIONING AND MAINTAINING CCTNS IN MEGHALAYA POLICE

VOLUME-I: FUNCTIONAL AND TECHNICAL SPECIFICATIONS

RELEASED BY:

GOVERNMENT OF MEGHALAYA

Contents

LIST OF ABBREVIATIONS

ADGP	Additional Director General of Police
AFIS	Automated Fingerprint Identification System
AIG	Assistant Inspector General of Police
AT	Acceptance Testing
BOM	Bill of Material
BPR	Business Process Reengineering
BSNL	Bharat Sanchar Nigam Limited
CAD	Computer Aided Dispatch
CAS	Core Application Software
CBI	Central Bureau of Investigation
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
CRP	Closed Room Pilot
DCRB	District Crime Record Bureau
DG	Director General
DG Set	Diesel Generator Set
DGP	Director General of Police
DIG	Deputy Inspector General of Police
DIT	Department of Information Technology
DRC	Disaster Recovery Centre
DSP	Deputy Superintendent of Police
EMD	Earnest Money Deposit
EMS	Enterprise Management System
FIR	First Information Report
FRS	Functional Requirement Specifications
GIS	Geographical Information System
GO	Gazetted Officer
GoI/GOI	Government of India
GoM/GOM	Government of Meghalaya
GPS	Global Positioning System
HLD	High Level Design
HQ	Headquarters
ICT	Information & Communication Technology
IGP	Inspector General of Police
IIF	Integrated Investigation Forms
IO	Investigation Officer
IPC	Indian Penal Code
IT	Information Technology
LAN	Local Area Network

LLD	Low Level Design
MHA	Ministry of Home Affairs
MIS	Management Information System
MMP	Mission Mode Project
MPLS	Multiprotocol Label Switching
NCR	Non-Cognizable Report
NCRB	National Crime Record Bureau
NeGP	National eGovernance Plan
NGO	Non-Gazetted Officer
NIC	National Informatics Centre
NOC	No Objection Certificate
PCR	Police Control Room
PHQ	Police Headquarters
RFP	Request for Proposal
RTI	Right To Information
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
SyRS	System Requirement Specifications
UT	Union Territory
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 Meghalaya 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 Meghalaya 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 Meghalaya 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
    - Site Preparation including civil works, creation of LAN, electrical works, etc. during that phase after verification and approval by Meghalaya Police or its constituted committees or representatives
    - Successful Data digitization / migration after verification and approval by Meghalaya Police or its constituted committees or representatives
    - Training and Certification of all the trainees, trained on the CCTNS application modules of that Phase
    - 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
    - Procurement, deployment and commissioning of the networking equipments and provisioning of desired connectivity required to support the functioning of modules of that Phase
    - Achievement of the Service Levels as expected during that Phase
    - Acceptance / Sign off from Meghalaya Police or its constituted committees or representatives

1 REQUEST FOR PROPOSAL DATASHEET

S. No	Information	Details
1.	RFP reference No and Date	**Letter No. S-298/RFP-SI/CCTNS/2011/104 Dated 14th April, 2011**
2	Non Refundable Tender Cost	**Rs. 10,000/-**
3	Sale of RFP Document	**15th April, 2011**
4	Earnest Money Deposit (EMD/ Bid Security)	**Rs. 25,00,000/-**
5.	Last date and Time for submission of written queries[1] for clarifications	**25th April, 2011; Till 4 PM**
	Date, Time and Venue of pre-proposal conference	**29th April, 2011; 12 PM; at Meghalaya Police Headquarters Conference Hall, Shillong.**
6.	Release of response to clarifications on	**4th May, 2011**
7.	Last date, Time (deadline) and Venue for receipt of proposals in response to RFP notice	**3 PM on 12th May, 2011 at Address mentioned below**
8.	Date, Time and Venue of opening of Technical proposals received in response to the RFP notice	**3 PM on 12th May, 2011 at Police Headquarters conference Hall**
9.	Place, Time and Date of Technical Presentations by the bidders	**To be decided and informed.**
10.	Place, Time and Date of opening of Financial proposals received in response to the RFP notice	**To be decided and informed.**
11.	Contact Person for queries	**Shri D.N.JYRWA, SP (SCRB)** **Office Address: Police Headquarters, Meghalaya, Shillong-793001**
12.	Addressee and Address at which proposal in response to RFP notice is to be submitted:	**Shri A.K.Mathur, ADGP(CID), Nodal Officer(CCTNS)** **Office Address: Police Headquarters, Meghalaya, Shillong-793001** **email:** meghcctns@yahoo.com

Table 1: RFP Datasheet

[1] Queries submitted in written to State Police would only be accepted for further consideration

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

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.

2.2.3 Crime & Criminal Tracking Network and System (CCTNS)

The Crime & Criminal Tracking Network and 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[2] 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.

With the introduction of CCTNS in Meghalaya, Meghalaya Police aims to reap rich rewards of using ICT for tracking of Crime & Criminals in the state, as well as bring in a seamless convergence of the police establishment in the state with elsewhere in the country, and to become extremely efficient and take a leading role in providing crime and criminal tracking services to the citizens of the country. The entire police establishment in Meghalaya is planned to be made comparable to the best policing systems in the country and service delivery to the stakeholders is also planned to improve by leaps and bounds.

2.3 CCTNS Implementation Framework

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

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

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

2.4 Goals of this Request for Proposal (RFP)

The primary goal of this RFP is to help State of Meghalaya in selecting System Integrator (SI) through a competitive bidding process for implementing CCTNS project in the State. 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 this RFP document are further elaborated below:

- To seek proposals from potential bidders for providing the "bundle of services" in implementing and managing the CCTNS solution in Meghalaya.
- To understand from the bidders how they propose to meet the technical and operational requirements of CCTNS.

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

- 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.

The state of Meghalaya (through State Apex Committee or State Empowered Committee) shall be the final authority with respect to qualifying a bidder through this RFP. Their decision with regard to the choice of the SI who qualifies through this RFP shall be final and the 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 adhering to State Government rules/ policy/ regulations.

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 of Meghalaya Police through this initiative is as follows:

"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:

i. ***Empowerment of Police Officers at all level***
   Police officer having the right type of information at the right time with the right tools to perform out his duty is what is envisioned through this project. It is imperative that the project should implement the aforementioned concept and shall provide Officers with a greater control, with the tools, technologies and information to facilitate prevention of crime, faster & more accurate investigation of crime and detection of criminals.

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

iii. ***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.

iv. 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.

v. 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.

vi. Eliminating Drudgery from Police System

Institutionalization of a platform to share information seamlessly with other states and other departments would rely on the central repository of information regarding crime and criminals. This central repository would be a step-stone towards efficient policing by reducing drudgery from the system and allowing police to spend more time in activities related to crime prevention and crime investigation.

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 (People of Meghalaya , Other citizens of India & Foreign nationals)
- MHA/NCRB/Others
- State Police department, CID, CBI, etc.
- Employees of Meghalaya Police
- External Departments of the State such as Jails, Courts, Passport Office, Transport Department and Hospitals etc.
- Non-Government/Private sector organizations

4 PROJECT OVERVIEW

Introduction to the Department of Police, Meghalaya

Meghalaya Police was formed on January 21, 1972. Since then the state police has grown from strength-to-strength. The Current Police Force Strength in the State of Meghalaya is 11333.

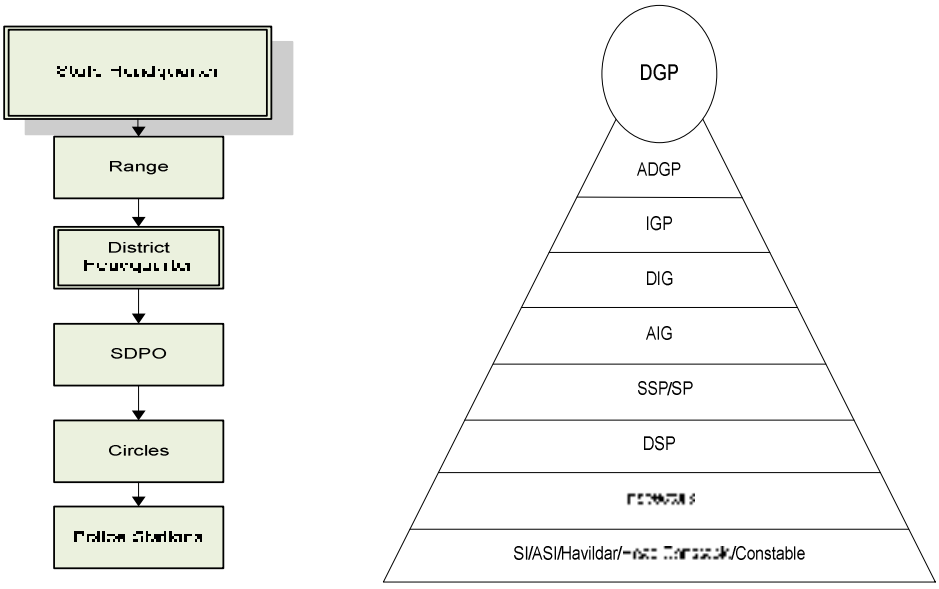
Police stations are the basic functional units responsible for the execution & maintenance of the law & order situation in the area of jurisdiction. These police stations are monitored at various levels of higher offices for proper administration throughout the state. At present, there are 39 operational police stations across the seven districts of Meghalaya. A circle inspector supervises 2 to 3 police stations from the Circle office. There are, in total, 19 circles in the state.

The Circle offices and the Police stations are in turn under the supervision of the Sub divisional office (SDPO), District headquarters and the Ranges. There are 8 SDPOs, 7 District Headquarters and 2 Ranges in the state.

At the highest level, all the police units/wings are administered / monitored from the State Police Headquarters.

State Police Headquarters

The central administrative unit State Police Headquarter is located in Shillong which is headed by the DGP. It monitors and supervises all the police units/offices scattered throughout the state.



All the administrative and higher level functions are executed/performed at the State Police headquarters. It is headed by the Director General of Police who is assisted by officers of subsequent ranks as depicted in the figure above.

The Headquarters functions through its various wings/units such as

- Range Office
- Infiltration
- Special Branch
- Crime Branch

- CID
- SCRB

Hierarchy

Gazetted Officers

a. - Director General of Police (DGP) is overall head of the Department.

b. - DGP is assisted by Additional Director General of Police (ADGP) (L&O/SB/CID etc) who is further assisted by multiple IGP/ DIG.

c. Inspector General of Police-Range (IGP) is the head of the range headquarters and is overall responsible for the areas falling within the jurisdiction of the range.

d. - IGP/Range is assisted by Superintendents of Police (SPs), who are in-charge of a districts falling within the range.

e. - Deputy Superintendent of Police (DSP) is responsible for sub-divisional area falling within a district and reports to SP.

Non Gazetted Officers

a. - Police Station is headed by Station House Officer (SHO), who is of the rank of Inspector (though in some case SHO is of the rank of SI/ ASI based on the jurisdiction of the Police Station). He reports to DSP.

b. - SHO is assisted Sub-Inspector (SI), Assistant Sub-Inspector (ASI), Head Constable and Constable in day to day police functioning including case registration, investigation, law and order maintenance etc.

The ranges covering various sub-division offices and PS coming under it are shown below:

S. No	Range	District	Subdivision	Circles	Police Station
1	Eastern Range	East Khasi Hills	Sohra	Sohra	Shillong Sadar
2				Mawsynram	Laitumkhrah
3					Lumdiengiri
4					Laban
5					Mawlai
6					Rynjah
7					Madanrting
8					Mawsynram
9					Pynursla
10					Sohra
11					Mawryngkneng
12					Shella
13					CID PS
14		West Khasi Hills	Nogstoin	Nogstoin	Nongstoin
15			Mawkyrwat	Mawkyrwat	Mawkyrwat
16			Mairang	Mairang	Mairang
17					Ranikot
18		Jaintia Hills	Khliehriat	Khliehriat	Jowai
19			Amlarem	Jowai	Dawki
20				Amlarem	Khliehriat
21					Amlarem
22					Saipung
23		Ri-Bhoi Hills		Khanapara	Nongpoh
24				Nongpoh	Umiam
25				Umiam	Khanapara
26	Western Range	East Garo Hills	Resulbelpara	Resulbelpara	Williamnagar
27				Williamnagar	Rongjeng
28					Mendipathar
29					Songsak

30		**West Garo Hills**	Dadengiri	Tura	Tura
31				Dalu	Phulbari
32				Mahendraganj	Mahendraganj
33				Phulbari	Dalu
34					Ampati
35					Tikrikilla
36					Dadengiri
37		**South Garo Hills**		Baghmara	Baghmara
38				Nongalbibra	Chokpot
39					Rongara

4.1 Organization Structure

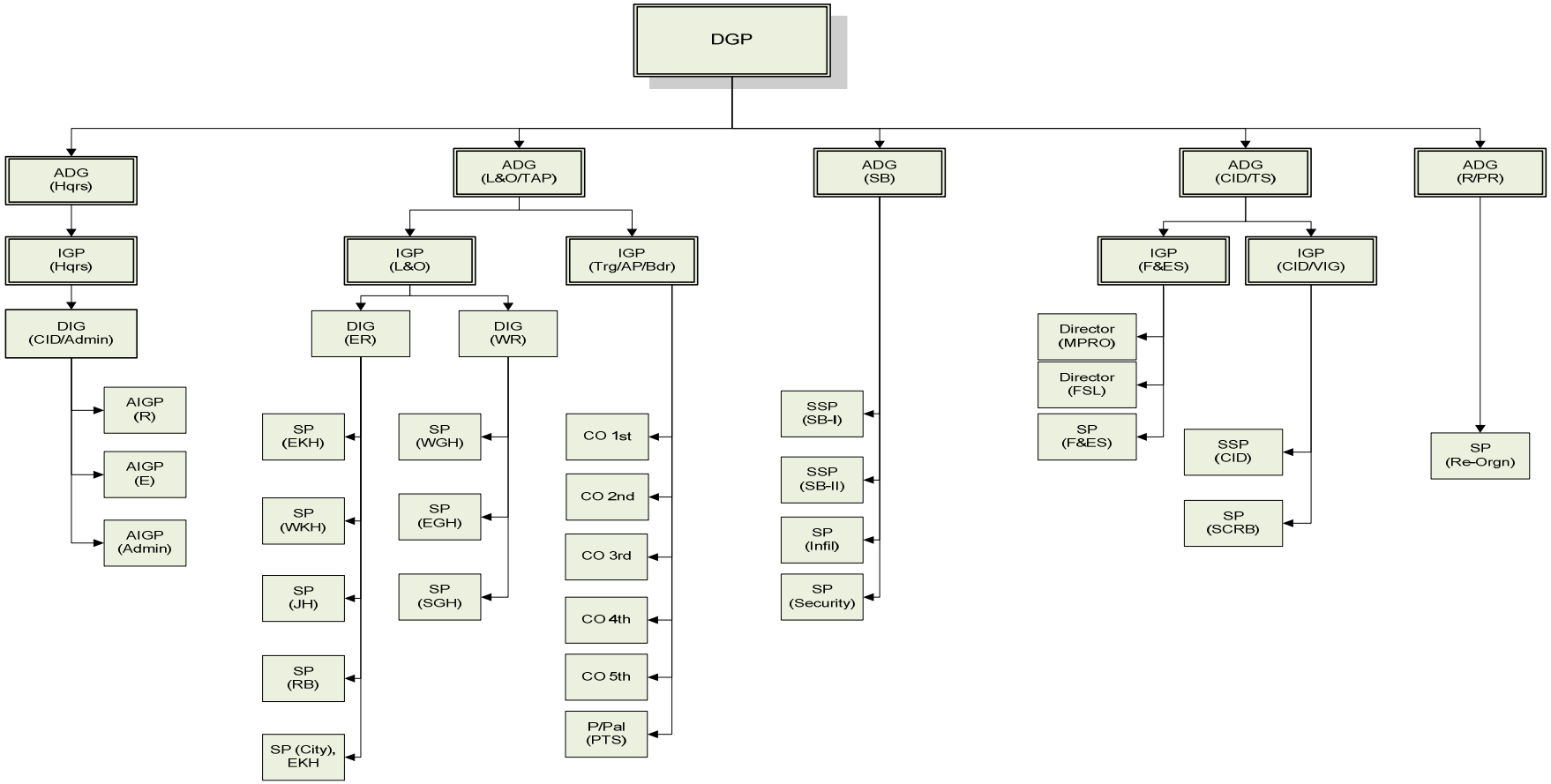


Exhibit 1: Organizational Structure of Meghalaya Police

4.2 Functions of the department of Police

Main functions of the department can be described as:

i. - Registration of Cases: Registration of a complaint lodged by the victim in case of a criminal offence in the concerned Police Station.
ii. - Investigation of Crimes: The cases registered in the Police Stations are investigated and appropriate action taken against the accused. After due investigation the case is charged in the Court of Law.
iii. - Law & Order: Enforcement of Law & Order to maintain peaceful atmosphere by monitoring various anti social elements.
iv. - Prevention of Crime: Prevention of crime by conducting day and night patrolling, monitoring and keeping a tab on criminals and their activities and taking appropriate action as and when required.
v. - Licenses: Verification for issuing number of Licenses for Hotels and Arms License.
vi. - Intelligence & Counter Intelligence: Various types of intelligence is gathered and is passed on to concerned wings for taking action in Security related, socio-economic related matters. Liaison with Govt. of India and other organizations to tackle terrorism and other related issues.
vii. - Maintenance of Criminal Records: Helping in obtaining information about the antecedents or background of any suspected person. This is also effectively used as validating information in cases of conviction of criminals.
viii. - Disaster Recovery: Respond quickly to natural and man-made disaster.
ix. - Others Functional Processes: The police department performs various other key functions such as-
    a. Verification Services for Passport Applicants -
    b. Crime against women / SC/ST -
    c. VIP / Special Security and protection -
    d. Traffic Management -
    e. Special Cells to counter terrorist activities, etc -
x. - Procurement: Procurement of items such as Vehicles, Communication equipment, Dress Material for police uniforms, leather equipment, and other office supplies such as stationery and consumables etc.
xi. - Human Resources Management: Recruitment, Training, Rewards, Punishments Performance Appraisal, etc.

Services offered by Department of Police

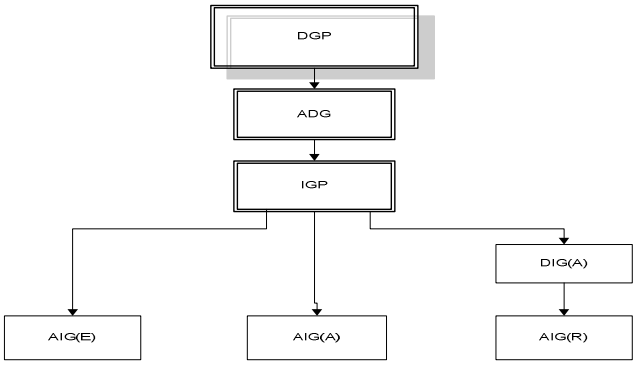
The key services offered by the department are:

i. - Registration of a Complaint under the Criminal Procedure Code
ii. - Issue of an FIR (First Information Report) under the Criminal Procedure Code
iii. - Status of a complaint under Criminal Procedure Code
iv. - Status of investigation of FIR under Criminal Procedure Code
v. - Status of stolen motor vehicles.
vi. - Status of stolen arms.
vii. - Status of recovered stolen property.
viii. - Status of a trial under Criminal Procedure Code.
ix. - Status of passport verification.
x. - Status of Nationality verification
xi. - Registration of permissions for processions etc. under Police Act
xii. - Status of permissions for processions etc under Police Act
xiii. - Proclaimed offenders / absconders under Criminal Procedure Act
xiv. - Status of verification of arms license under Arms Act
xv. - Information on missing persons / dead bodies under Criminal Procedure Act

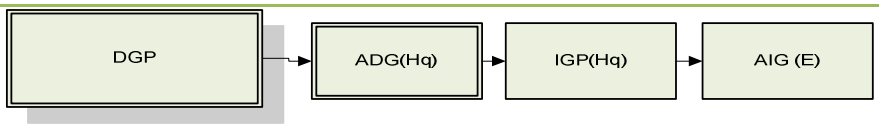
xvi. Verification of domestic servants, tenants, job seekers etc.
xvii. Response to PCR to the scene of crime / place of assistance
xviii. Security of individuals / institutions
xix. Resource management i.e. transport, finance, arms etc.

The Meghalaya Police operates through its following wings

- Police Headquarter
  - Establishment
  - Reorganization
  - Administration
- Law & Order
- Traffic Branch
- Armed Police / Battalions
- Special Branch
- Infiltration
- Forensic Science Laboratory
- CID/ACB
- Crime Branch
- SCRB
- MPRO
- Computer Wing

1. POLICE HEADQUARTERS	
Staff structure	
	
Functions:	The police headquarters are divided into three wings to manage its operations effectively. 1. Establishment 2. Reorganization 3. Administration

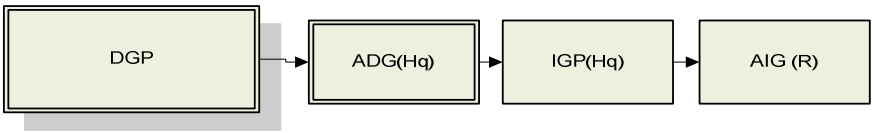
ESTABLISHMENT
Departmental structure



Functions:	1. Construction for new Set-ups e.g. Forensic Lab set up, construction of dog canals for Special branch etc. 2. Works related to engineering like repairing and renovation of existing establishments.

REORGANIZATION

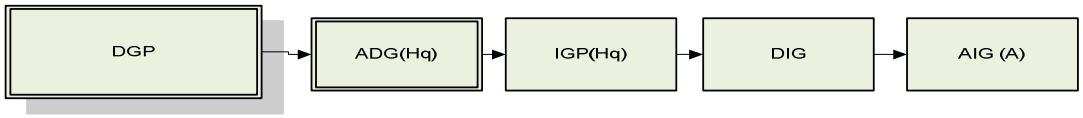
Departmental structure



Functions:	1. Issuance of pension to eligible police personnel. 2. Issuance of official departmental Orders like Transfer, leaves etc 3. Interdepartmental and Intra departmental communication 4. Record maintenance regarding sanctioned and existing strengths of the Meghalaya Police. 5. Police welfare measures. 6. Coordination with other branches of police.

ADMINISTRATION

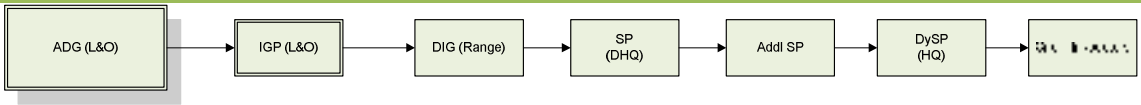
Departmental structure



Functions:	1. Preparation of police budget and allocations of funds to different branch. 2. Maintenance of ACR. 3. Issuance and renewal of arm licenses. 4. Court Proceedings of the Police Personnel e.g. if any officer or police department is involved in court prosecution. 5. Requisition of arms, ammunition and cars for different branches. Deployment of personnel for Immediate Law and Order situation.

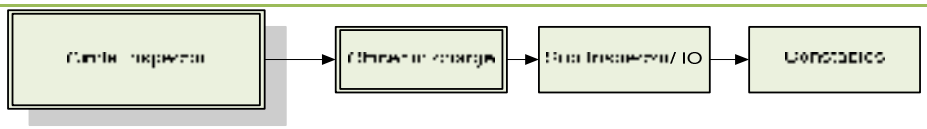
2. Law & Order

Staff Structure



Functions	Its function is monitoring, screening, supervising and administrating the law & order

	situation in the state. DIG of the range have to report for the law & order situation under their Jurisdiction. SPs of the districts have to report to DIG of the range. All the field policing are done by the district executive forces which are monitored by the DIG of that Range. The Meghalaya state is politically divided into 7 districts. Four of those Districts come under the Eastern Range and the rests in the western range.

District Executive Forces	
Staff Structure	
	
Functions	1. Maintaining Law and Order in the districts. 2. Writing Citizen's complains and grievances and taking necessary action. 3. Investigation of criminal cases at the district level. 4. FIR registration. 5. Provide security to VIPs 6. Reporting of Cognizable/ Non-Cognizable offence. 7. Bringing the accused in front of courts. 8. Verifications for Passports, Vehicle registration, etc

Indicative details of records maintained at PS		
Name of the Register	**Description of Record**	**Reason for Management**
1. Process Register	This Register keeps record of the all the Slips, Summons, Warrants, Proclamation and Attachments issued by court. 1. Summon - A written order issued to a person to appear before the court issuing it. 2. Warrant- A written order issued to arrest the accused. 3. Proclamation- An order requiring the appearance of a person accused. 4. Attachment- An order to compel the appearance of a person accused.	Maintains records of communication with court
2. Malkhana Register	This register keeps record of all the articles/property that is seized by the police. e.g. 1. Stolen property 2. Interstate property 3. Unclaimed Property 4. Suspicious Property 5. Exhibits & other Property.	Keeps track of all the property that has been seized
3. Non-FIR register	This register keeps record of all the NON-FIR cases that has been registered in the Police station.	Record of Non-FIR cases
4. Receipt and Dispatch Register	This register keeps a record of all the correspondents that has been received and	This is the correspondence register

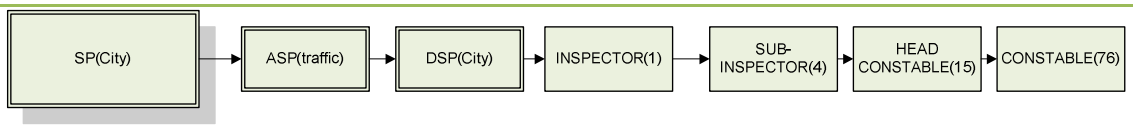
	dispatched. 1. Court related 2. Higher Officers 3. W.T. Message & Papers from NON-Gazetted Officers of Police. 4. Other Civil Officers 5. Domicile, Passport and Service verification. 6. Gun Verification.	
5. UDMR Register	This register contains information of all Undetected articles that have been found by the police.	Maintains the records of undetected articles
6. Missing Person Register	When a person is reported missing, his details like age, sex, Place of Missing etc are registered in Missing Person Register.	It helps the PS to serve the general public efficiently.
7. Arrested Person Register	It maintains the records of all the accused persons that have been arrested. The record includes the physical appearance of the persons in detail.	Keeps records of all the persons arrested.
8. Telephone Information received for Law & Order	It maintains all the records that have been received via telephone.	Messages recorded for future reference.
9. VCNB Register	This register is used to store information like 1. The area, population, Tourist Centre, Commercial centre, Nearest hospital, Name of hotels, Transportation, etc 2. Crimes and Criminal details in the village. 3. Magistrate Orders and the result of the case.	This record is maintained to keep village/beat information for better management of Crime.
10. Patrolling register	This Register contains all the details of Patrolling conducted by the police.	Patrolling details
11. Arms Issue Register	It contains the type of Arms/Ammunition which are issued to a police personnel.	Keeps track of arms issued.

Indicative Monthly Reports	
Name of the Monthly Report	**Detail**
1. Explosive Case	Details of all the explosions that have occurred in the month.
2. Vice Raid	Details of the raids conducted in the region.
3. Loss/Theft/Recovery &Arms & Ammunition.	Details of the loss/theft/recovery of the arms & ammunition.
4. Escape from Lawful Custody	Details of the escape of a prisoner from lawful custody.
5. Leave	Contains details like name & rank of personnel and no. of days of leave.
6. Sick	Contains details like name & rank of personnel and no. of days of sick leave.
7. Crime Against Women	Details of the crime, Name of victim and the name of the accused.
8. Kidnapping of children	Details of the Kidnapped children, Kidnapping Location etc
9. Missing Children	Details of the missing children along with the date of missing and date of reporting.
10. Cases Registered	Cases which are registered(Case No. with section of law & Name

	of the IO)
11. Cases Disposed off	Contains details of the Cases which are disposed off (Case No. With Section of Law and the Name of Concerned IO)
12. Seizure of Counterfeit Currency Notes	Contains details like Date& Place of seizure, Source of seized currency, Name of arrested accused, denomination of currencies seized etc.
13. NDPS Case	Narcotics, Drugs & psycho tropic substances Case. Contains details like Drugs seized, place of seizure, Name of IO etc.
14. UD case registered	Details of the Unnatural deaths which has been reported.
15. Talash data	Physical and personal details of all the criminals who are taken into custody.

3. Traffic Branch

Staff Structure



The structure is presented for Shillong Traffic branch.

Functions	1. Controlling the state traffic. 2. Charging fine to the Traffic law violator. 3. Maintaining records of vehicles involved in traffic violation. 4. Maintaining records of Fines collected. 5. Discharging duties of law enforcement as mandated by MV Act and rules framed there under.

Records Management

Name of the Register	Description of Record	Reason for Management
1. General Diary	Record of all the traffic related issues in the diary	Every traffic related issues is entered here. So any traffic related information can be retrieved.
2. Duty Register	Maintains the record of the distribution of duties	Helps in the proper allocation of duties
3. Compounding register	Records of all the compounding done.	Records of all the compounding helps in calculating the fine received during a particular duration.
4. Collision Register	Records of all the road collisions.	Helps in analyzing the traffic situations during a particular time period.

4. Armed Police / Battalions

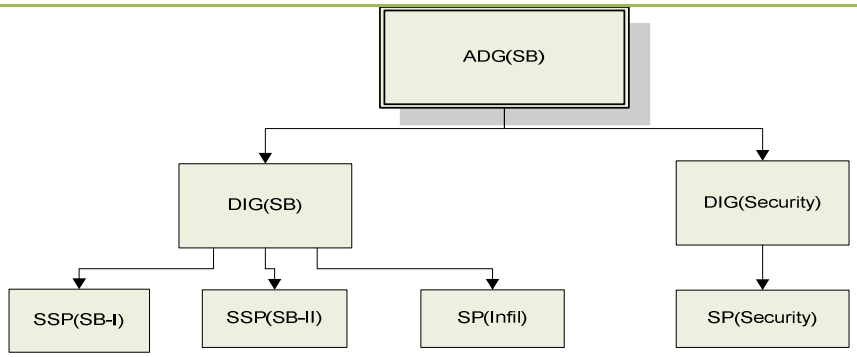
Divisions:	1. 1st MLP Bn 2. 2nd MLP Bn 3. 3rd MLP Bn 4. 4th MLP Bn 5. 5th MLP Bn
Functions	Main role of a battalion is to assist the district SPs by providing man power for providing securities to VIPs or helping out during disasters, law and order situations, insurgencies etc. Battalions have to keep the track of how many personnels have been deployed for what.

About Different Battalions:	
1st MLP Bn	The 1st MLP Bn. was formerly located at Bishnupur, Shillong and later on shifted to its present location at Mawiong, on 7th April 1981. With the shifting of the Bn. to the present location, various facilities have been provided to the Bn. personnel, namely:- (i) Construction of 20 bedded Hospital with 2 Doctors, 2 Nurses, 1-Dhai and 24 Nursing Halviders. (ii) The Hospital besides treating the force personnel and their family members is also catering to the health needs of local residents in times of emergency. (iii) A Private L.P. M.E. School for the benefit of the children of Bn. personnel was established in 1974 at Bishnupur and later on shifted to the present location in 1985. Class VII to X were introduced in the year 1998. Presently, there are 275 Students in L.P. Section and 65 in M.E. Section with 6 teachers' salary being paid by the Education Department and salary of another 6 teachers being paid from the Private Fund of the Unit. (iv) Welfare Canteen:- The Welfare canteen was established on 14.11.1988 with a view to providing grocery and other essential commodities to the Bn. personnel and their family members on credit basis. (v) An S. K. Oil Storage and Depot were also established in 1989 under the license from D.C Supply, Shillong for supplying K. Oil not only to Bn. personnel but also to the other Police personnel of E.K. Hills and ministerial staff of the D.G.P. Office, Shillong. (vi) Through the Indian Oil Corporation, an L.P.G. Agency was opened in the same year for the benefit of the Bn. personnel and their family members. (vii) Sincere efforts are being made by Police Headquarters to provide family quarters to Bn. personnel under Police Housing scheme. Till date, MGCC has constructed 7 (seven) Nos of G.Os' Quarters, 30 (thirty) units of U.S. Quarters and 188 units of L.S. quarters. (viii) This unit has also been functioning as a Training Centre all along and 29 Batches of Recruits have passed out from this Training Centre till date. The present batch comprising a total of 196 Recruits from various units will also be passing out shortly. Various promotion / Cadre Courses from Constable to ABI are also conducted in this Training Centre. Besides the Re-Orientation Course from ASI to Inspectors, Special Courses on WT / PSO / CIC and Tear Smoke Courses, etc. are also conducted. However, this Training Centre is yet to be recognized. (ix) Besides providing work force for construction and renovation of buildings, etc. from out of unit fund, the men are also pressed into service for rescue operations in times of natural calamities. Recently, the officers and men of this unit were pressed into service during the floods at Polo ground and its adjacent areas, for relief operation. (x) The Central Workshop at Bishnupur is also manned by the staff of 1st MLP Bn. with one Asstt. Comdt. who is directly supervising the repair and maintenance work of Police and Govt. Vehicles and at the same time imparting Training in driving and repairing works of vehicles to the Police drivers and mechanics. (xi) This unit has a Firing Range which is used both for small arms and other weapons. The other units besides the CRPF and Home Guards are also using this

	Firing Range for range firing practice.
2nd MLP Bn	One of the main tasks of the 2nd MLP Battalion is to impart training to the newly recruited constables. Temporary Katcha barracks have been constructed on self help basis to accommodate the trainees. Till date, 1154 recruit constables from all over the State have successfully passed out from the Training Centre. In addition to the basic training, the Battalion also conducts courses for Gazetted Officers, UBSIs, ASI Instructors, Senior Cadre Courses, Junior Cadre Courses, Advanced Riot Drill courses and Refresher Courses. In addition to their normal duties, the services of the Bn. personnel have been utilized for helping people in times of natural calamities and other dire needs. During 1983 and 1985 when heavy monsoons affected the entire Garo Hills snapping road communication by sweeping away the bridge over river Ganol, the Battalion personnel came to the rescue of the affected people. They did a commendable job to clear heaps of earth from the road and helped transport the stranded passengers. The Bn. personnel also donated blood to the needy and sick people.
3rd MLP Bn	At present, the main function of this Battalion is to provide security and assist the District executive force in the border districts of West Khasi Hills and South Garo Hills. Besides, a company of S.O.T. with Head Quarters at Mawiong, Shillong is also a part of this Battalion.
4th MLP Bn	The 2nd IRBN which is also the 4th MLP Bn formally became functional on 28.02.2002 with the assumption of charge of the office by Shri J. Rymmai, MPS as Commandant. The office of the 4th MLP Bn is currently functioning from the Police Headquarters as land for this battalion is yet to be acquired. The Commandant is assisted by 1(one) 2nd - in – Command, 1(one) Asstt. Commandant, 1 Insp, 1 ASI and 2 Constables.
5th MLP Bn	This is 3rd IRBN situated at Shillong.

5. SPECIAL BRANCH

Departmental structure



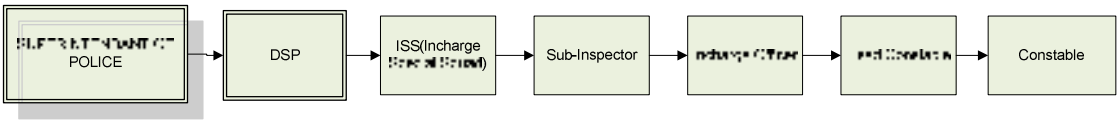
Functions

-	SB-I is concerned with two types of Intelligence collection 1. Political Intelligence- Collecting Information on the current activities of the major political parties. To assess if there is any planning going on to topple the government or to disturb Law & Order. The complete profile of the political parties are recorded and updated. 2. Border Intelligence- Intelligence collection on the activities near the border area.
SPECIAL BRANCH - II	1. Students and Youth Organization, Employees/Trade Unions, Labour and Services - To collect intelligence of the active organizations, their activities, their details like where are their locations, who is the leader and who is associated with it, etc. Special Branch has to prepare a Dossier for that so that Information can be extracted whenever required. 2. Inspection Notes- Maintains this register where the balance sheet of the criminals' activity is prepared. Record of the Number of criminals charge sheeted, acquitted etc are maintained. 3. Extremist Organization- Concerned with the Intelligence of the Extremist activities 4. Interrogation Report 5. Disaster Management- If there is any occurrence of a disaster, Special Branch prepares the plan like what needs to be done n how to respond to the crisis. SSP instructs the Fire Service Department to fight out the Disaster which is coordinated by District SP and District Magistrate. 6. Coordination with other agencies- There are monthly meetings with Subsidiary Multi Intelligence Agency. SB liaisons with branches like BSF, CRPF, AIR-Force, Assam Rifles for Intelligence sharing. 7. Gazettes Maintenance- Monitoring the use and status of the gazettes given to different police departments. 8. Surrendered Militants- Activities of Militants who have surrendered are monitored and screened. They are kept in sponsored Rehabilitation camp for 3 months after which they are released. 9. Service Verification- The service verification is to be done by SB 10. Indexing- Indexing of the criminals and their activities is done which are used for any verification purpose. 11. SOP(Special Operating Procedures)
SECURITY	1. Concerned mainly with providing security to visiting VIPs, and Maintaining Bomb

	disposal cell. 2. If there is any life threat to any civilian, he can contact the police department to provide him the security. If Security branch receives any kind of request, it guides the district police to assess the threat situation and provide the security. 3. Bomb Disposal is again very important function of the security branch. If there is any suspicion or detection of Bombs, the special branch is alerted to send the bomb disposal squad at the bomb site. In the mean time, the traffic control is contacted to clear out the traffic around the site. The bomb is to be diffused by the squad.

6. Infiltration

Departmental Structure and Strength



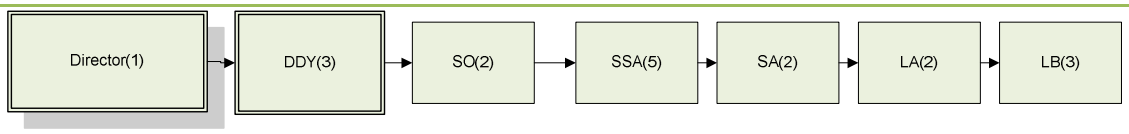
Functions	The main objective of the State Infiltration Branch is to prevent and check the influx and illegal entry of foreign nationals detecting, prosecuting and deporting them after concrete evidence is established against them. Some of the important duties assigned to the personnel working under the PIF Scheme are : a. Undertake enumeration of all the Inhabitants residing In border villages. b. The national Register of Citizens (NRC) of 1951 census be used as reference for determining citizenship. c. Collect intelligence from all possible quarters namely, secret sources, VDP, dependable Headmen and other village officials about infiltrators. d. Check all pedestrians and vehicles for presence of foreigners entering the area without valid documents, to detect and push them back to the International borders if such foreigners are detected within 10 kms of the International borders. Those detected beyond 10 kms of the International border are to be prosecuted under the Foreigners' Act, 1946 through Police Stations. e. Verify arrival of any new-comer by constant patrolling. The primary objective of the I/C of a Watch Post/Patrol Post/Infil Check Post is to ensure that the arrival, stay and movement of any foreigner does not go unnoticed. f. Maintain records of detections, push back and prosecution of foreigners. Also, to maintain a record of finger prints and photographs of all foreigners detected. g. Check the papers, passports, visas, of all foreigners attempting to enter the country illegally, to maintain a record of such traffic and to keep a look out for certain foreigners who have been black-listed (PCP only). h. Prepare and send necessary returns to Ministry of Home Affairs, New Delhi, with copies to the State Govt. and Infil Hqrs (PCP only) i. Detect foreigners whose papers and/or passports are not in order. They are to be prosecuted under Passport Rules, 1950 through Police Stations. (PCP only). j. Conduct raids to arrest foreigners entering and staying illegally in the district and to prosecute them under the Foreigners Act, 1946. (District Hqrs. Special Squad only).

	k. Maintain a record of finger prints and photographs of all foreigners detected by the Infiltration units within the district and to computerize them easy retrieval. District Finger Print and Photo Units.

Records Management		
Name of the Register	**Description of Record**	**Reason for Management**
Detection Register	Contains the details of the person whose identification is to be validated.	Helps in recording the details of all the foreigners who have been found entering illegally.
Enumeration Register	Contains the Population data of the villages which is counted at regular intervals to check the entry of foreigners.	Helps in checking the illegal entry of any foreigner.
Labour Register	Contains the registration details of the Laborers. If during inspection Bangladeshi Laborers are found, they are sent for prosecution.	Helps in checking the illegal entry of those who enters as laborers.

7. Forensic Science Laboratory

Departmental Structure and Strength

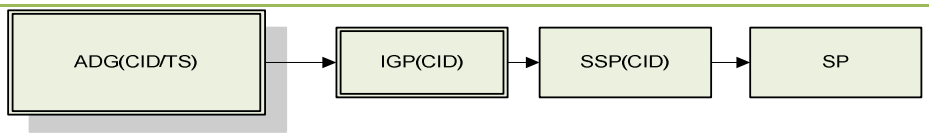


Functions

1. This Laboratory is functioning with only 4 (four) Technical Divisions viz.
   - Physical Division for Examination of Firearm ammunition, Exhibits from accident cases, Explosive substances, Metal & Metallic fragments etc.
   - Chemical Division for Examination of Drugs & Narcotics substances, Chemicals, Fire debris, poisons, viscera for determination of causes of death.
   - Biology Division for Examining exhibits like Dead bodies and Skeletal remains, Plant, Poisons, Blood, Semen and other body fluids for murder and rape cases etc.
   - Questioned Documents Division for Examination of forgeries, Currency notes and others Document cases. The Laboratory is headed by a Director and is functioning under the overall control of the Director General of Police.
2. The staffs of the Laboratory have to depose evidence in the Court of law and help the Investigating Officers in the Crime Scene as and when called for.
3. Seven District Mobile Units to the 7 (Seven) District of Meghalaya is recommended by XIth Finance Commission which should go to the Crime Scene with simple Equipment, Test Materials and Photographic aids to record the crime scene and to collect all the clue materials available not only in the Place of Occurrence but also from the possession of the victim and the suspect.

8. CID/ACB

Staff Structure



Functions

- Investigation of complicated cases or organized crime extending over two or more districts.
- Institution of confidential enquiries into matters of general interest under the direction of the Director General and Inspector General of police or the State Government.
- Co-operating with the Criminal Investigation Department of other States and exchanging with them information on inter-State Crime and Criminals.
- Collection of Statistics relating to Crime and Criminals and submission thereof to the Director General and Inspector General of Police, the State Government and other authorities as and when required.
- Giving expert legal advice or guidance n matters referred to it by Superintendents of Police in charge of districts.
- Publication of the Criminal Intelligence Gazette every month containing information on matters of general interest affecting the prevention and detection of crime.
- Maintaining Narcotic Cell.
- Maintaining Photographic Cell.
- Maintaining, Law and Research Cell.
- Maintaining Dog Squad.
- Maintaining Juvenile Guidance Bureau.
- Keeping Liaison with the Forensic Science Laboratory and other Organization and Departments of the State and the Central Governments, reference to which may be required to be made for purposes of investigation or with organizations dealing with Juvenile Crime, Probation, after care, etc.
- Carrying out such other functions as may be assigned to it by Director General and Inspector General of Police or the State Government.

9. CRIME BRANCH

Functions

The main functions of crime branch are

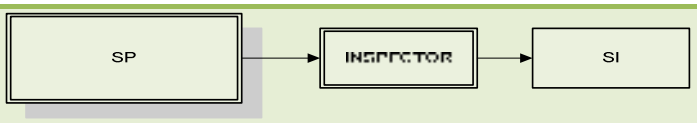
- Compilation and analysis of Crime Reports
- Monitoring of Special Cases

- Crime Branch collects crime reports from all the police stations, collates them and prepares the crime report.
- Crime Branch maintains a register called Crime Register. The detail of all the crimes that has been registered in the state is recorded here.
- Before closing any case, the PROGRESS REPORT which is prepared by the IO is forwarded to the immediate senior i.e. OC. OC has to submit that report to the SP. If SP is satisfied, then the case can be closed.
- Cases which are treated as SPECIAL are handled by CID. Crime Branch maintains a separate register called SPECIAL REIGSTER for Special cases. The case diaries of the special cases are maintained by CID. Triplicate copy of that file is received and recorded in the Crime Branch Special reports.

Following are the reports that are prepared by Crime Branch

1. Pending Cases
2. Disposed Off Cases
3. Monthly return of cases treated as S.R.
4. Monthly return of S.R Cases Disposed off.
5. Number of cases Registered and Disposed off

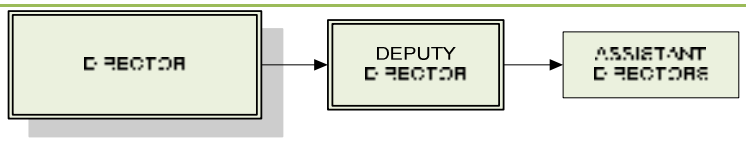
6. - Monthly return of LOSS/THEFT/SEIZURE of ARMS/AMMNS
7. - Monthly return of seized by police counterfeit Currency Notes.
8. - Monthly Return of Kidnapping children for Begging/Ranson/Prostitution
9. - Monthly return of Explosive Act.
10. Monthly return of Extortion Cases
11. Return for U.A. (P) ACT
12. Monthly return of Vice Raids
13. Monthly Return of Finger Prints of Arrested Person
14. Monthly return of LOSS/Theft/Recovery of Motor Vehicless
15. Monthly return of Crime Against Women
16. Monthly return of Seizure of N.D.P.S
17. Quarterly Return of ESCAPE from Lawful Custody
18. Monthly return of arrest/ detention of foreigners
19. Monthly return of cheating
20. Monthly return of Missing Person
21. Comparative statement of crime for the fortnight ending
22. U.D. Cases

10. SCRB	
Staff Structure	
Functions	1. - SCRB is the record centre of all the criminal activities that have happened in the State. There are crime records bureau situated at district level which sends their report to the SCRB headquarters. It is mandatory for police stations in the district to prepare and send timely reports to the DCRB about the crime scene in their district, and also regarding various other activities. The crime reports are to be sent in statistical as well as in detailed form. E.g. the police stations have to send one copy of FIR of all the cases that have been registered in the police station. Detailing like Progress of the case, its proceedings and the outcomes, everything is recorded. It is the job of DCRB to collate the crime reports from different police stations sent it to SCRB. Each DCRB is provided with a CCIS application platform where it has to input these details and send the compiled data in a CD or through other means to SCRB. Apart from CCIS, there are some DOS based platforms which are employed to form statistical reports such as a. - Monthly Crime statistics – All crimes under different heads starting from IPC crimes, Local and Special Laws, crime against women, crime against children, etc. b. - Crime in India- This is a 53 page yearly statistics which is being compiled at SCRB it contains information on cognizable crimes, arrested persons, juvenile cases, police housing, police strength, pay, budget etc c. - Accidental Deaths and Suicides in India- This is another yearly report which contains information of unnatural deaths by various causes. d. - Other reports. 2. - Maintenance of Meghalaya Police website www.megpolice.gov.in 3. - Motor Vehicle Verification system- This is a public utility system where people can come and verify the status of vehicle they intend to buy. It also provides service to the public who intend to make enquiry about their lost/ stolen vehicles to ascertain whether it has been found or recovered anywhere in India. 4. - Talash system- The NCRB has been maintaining a National level database of

	Arrested, Wanted, Missing, Kidnapped, Deserters, Escapees, Unidentified persons and Unidentified Dead Bodies under the Talash System. If someone is missing or kidnapped, DCRB/SCRB updates the information in the database which is accessible in the whole of India.

11. Meghalaya Police Radio Organization (MPRO)

Departmental Structure

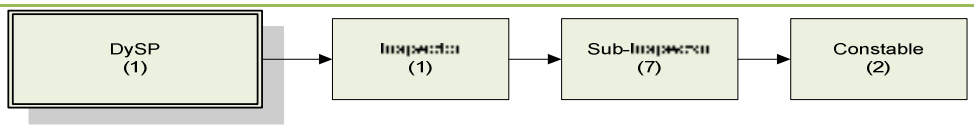


Total Strength: 647

Functions	• The MPRO manned by Operators, G D Constables and other supporting staff plays a vital role in the transmission of important messages for the Meghalaya Police. • It assists in passing important information and messages from one Police department to other. In other words we can say that it acts as a media which is accessible to all the police departments. • Information's are passed in both vocal and written form. Only text messages are logged and registered. • The Secret Messages are sent in encrypted form using ciphers. • At the MPRO headquarter, IN-OUT registers are maintained to record all the messages that are being transmitted and received. • It is also involved in the maintenance of communication equipments of the police department. • Two reports have to be submitted daily to the MPRO headquarter called sit-rep or the situation report. This report contains the situation analysis of the region from where it is being reported. The originator generates a report, signs it and keeps a copy with itself. The signed copy is send to the MPRO Headquarter. • If the message is confidential, then the encrypted form of that message is transmitted which has to be deciphered at the receiving MPRO station.

12. Computer wing

Staff Structure



Functions	1. Maintains several databases like a. ACR tracking b. PIS tracking(Personal Information System) c. VIS(Vehicle Information System) d. Budget Management. e. Others as assigned 2. Impart computer training to DGPs office employees.

4.3 Existing Legacy Systems

The detailed information pertaining to the existing systems has been provided as Annexure IX to this RFP.

4.4 Infrastructure in Meghalaya State Data Centre

Meghalaya State Data Centre is in the advanced state of implementation and is expected to be up by March, 2011. The list of hardware to be leveraged has been indicated in the section 5.4.7 the RFP and bidder to do detail assessment before submitting their proposal.

4.5 Existing WAN Infrastructure

The information pertaining to the existing WAN infrastructure and the SWAN utilization for providing connectivity to police locations has been provided as Annexure VII to this RFP.

4.6 Existing Client Site Infrastructure

The detailed information pertaining to the existing client site infrastructure procured for CIPA has been provided as Annexure VIII to this RFP.

4.7 Existing Capacity Building Infrastructure

Meghalaya Police has various training centers across the state and the SI can use these centers for CCTNS trainings. The detailed information pertaining to the existing capacity building infrastructure has been provided in Annexure VIII to this RFP

4.8 Core Application Software

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

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

This section provides the details of the CAS (State) and CAS (Center) that will be developed by the Software Development Agency at the Center. The details provided in subsequent sections (4.10 and 4.11) 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).

The functional requirements and the technical architecture of the CAS (State) and CAS (Center) is provided in detail in the RFP issued by NCRB for the selection of the SDA. The CCTNS application software can be conceptualized as comprising different services that fall under two broad categories, CAS (Center) and CAS (State).

4.9 CAS (Center)

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

Overview of Services for CAS (Center)
State-SCRB-NCRB Data Transfer and Management
The service shall enable the NCRB to receive, transform, and collate the crime, criminal, and related data from States/UTs, to organize it suitably to serve NCRB requirements.
Crime and Criminal Reports
The service shall enable authorized personnel to generate the reports and perform analysis on the central crime, criminals, and related data repository of the nation.
Crime and Criminal Records and Query Management
The service shall enable the authorized personnel to view various registers and perform basic and advanced queries on the central crime, criminals, and related data repository of the nation.
Talaash Service
The service will enable the user to search for missing persons across a central/ national database.
Person of Interest
The service will enable the user to search for persons of interest such as persons wanted on outstanding warrants, accused, charged, habitual offenders, convicts across the national database.
Registered Vehicle and Vehicle of Interest Service
The service will enable the user to search for registered vehicles and vehicles of interest such as, missing / stolen vehicles, abandoned / unclaimed vehicles, and vehicles involved in traffic incidents across the national database.
Publication Service
This functionality will help the NCRB to publish the periodic crime reviews to the NCRB portal.
NCRB Citizen Interface
The service shall enable the citizens to access/ search the NCRB National Database on the data (ex, Stolen Vehicles / Property, Missing Persons, etc.) that is approved to be made accessible to public.
NCRB Interface for RTI
Due to the sensitivity of the information that pertains to national security and harmony, this service shall enable a limited and restricted access to the authorized external stakeholders to search the NCRB National Database, upon submission of any RTI requests.

4.10 CAS (State)

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

Police would determine the requirements for configuration, customization and enhancements / extensions. The following are the main function blocks that would comprise CAS (State):

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

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

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

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

- It will lay special emphasis on the functions at police stations with focus on usability and ease of use of the application
- It will be designed to provide clear and tangible value to key roles at the Police Station: specifically the SHO (Station House Officer), the IO (Investigation Officer) and the Station Writer.
- It will be event and role-driven. Access controls will be developed and role based access will be provided in the application.
- It will be content/forms-based, with customized forms based on requirements
- It will be a flexible application, event and role-driven system where actions on a case can be taken as required without rigid sequence / workflows
- It will eliminate the need for duplicate and redundant entry of data, and the need for repetitive, manual report preparation – this freeing valuable time and resources for the performance of core police functions
- It will be intelligent and help police perform their roles by providing alerts, highlighting key action areas, etc.
- Ability to view and exchange information amongst Police Stations, between Police Stations and other Police formations and with external entities including citizens
- Reporting and data requirements of higher offices must be met at the State Data Centre/SCRB level and not percolate to the police station level
- 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)
Citizens Portal Service
This service shall enable Citizens to request services from Police through online petitions and track status of registered petitions and requests online. Citizens requests/services include passport verification services, general service petitions such as No Objection Certificate (NOC) for job, NOC for vehicle theft, NOC for lost cell phone/passport, Licenses for arms, processions etc.
Petition Management Service
The service shall enable the police personnel to register and process the different kinds of general service petitions and complaints.
Unclaimed/Abandon Property Register Service
The service shall enable the police personnel to record and maintain unclaimed/abandoned

property registers and match unclaimed/ abandoned property with property in lost/stolen registers.
Complaint and FIR Management Service
The service shall enable the police personnel to register and process the complaints (FIR for cognizable complaints, Non-Cognizable Report for non-cognizable, Complaint Report for genera complaints, etc.) reported by the public.
PCR Call Interface and Management Service
The service shall enable the police personnel to register and process the complaints as received through the Police Control Room through the Dial 100 emergency contact number.
Investigation Management Service
The service shall enable the police personnel to process the complaints through capturing the details collected during the investigation process that are required for the investigation officer to prepare a final report.
Court and Jail Interface and Prosecution Management Service
The service shall enable the police personnel to interface with the courts and jails during the investigation process (for producing evidence, producing arrested, remand etc) and during the trial process.
Crime and Criminal Records and Query Management Service
The service shall enable the police personnel to view various registers and perform basic and advanced queries on the crime and criminal information.
Police Email and Messaging Service
The service shall enable the police personnel to send / receive, official as well as personal correspondence.
Periodic Crime, and Law & Order Reports and Review Dashboard Service
The service shall enable the police personnel to view relevant reports and dashboards and to conduct periodic crime, and law & order reviews of the police station(s) under the officer's jurisdiction.
Notification of Alerts, Important Events, Reminders and Activity Calendar or Tasks Service
The service shall capture / generate the required alerts, important events, reminders, activity calendar and tasks.
State-SCRB-NCRB Data Transfer and Management Service
The service shall enable the States/UTs to collate, transform and transfer the crime, criminal, and other related data from state to NCRB.
State CAS Administration and Configuration Management Service
The service shall enable the individual State/UT to configure/ customize the application to suit to their unique requirements.
User Help and Assistance Service
The service shall enable the end user to view the help manuals of the application and in guiding the end user in using the application.
User Feedback Tracking and Resolution Service
The service shall enable the police personnel in logging the issues/defects occurred while using the system.
Activity Log Tracking and Audit Service
The service shall capture the audit trail resulting from execution of a business process or system function.
User Access and Authorization Management Service
The service shall enable the administrative user in setting the access privileges and will provide authentication and authorization functionality

4.11 Development of CCTNS Core Application Software (CAS)

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

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

In order to achieve the above stated goals of simultaneously ensuring consistency and standardization across States/UTs (where necessary and possible), and enabling States/UTs to meet their unique requirements, CAS will be built as a highly configurable and customizable application. CAS would therefore be a *product-like* application that could be centrally managed and at the same time customized to meet the unique requirements of the States/UTs and deployed in all States/UTs.
In order to achieve the key CCTNS goal of facilitating the availability of *real time* information across police stations and between police stations and higher offices, CAS would be built as a web application. However, given the connectivity challenges faced in a number of police stations, especially rural police stations, the application must be built to work in police stations with low and/or unreliable connectivity.

4.12 Technology Stack for CAS (State)

CAS (State) will be developed in two distinct technology stacks by the Software Development Agency at the Centre. The details of the Technology Stacks are provided as an Annexure I to this RFP. The SI is expected to bid with one of the technology stacks in response to this RFP. SI shall procure all necessary underlying solution components required to successfully implement CCTNS solution for the Meghalaya Police meeting their requirements as per this RFP.

5 ROLE OF SOFTWARE DEVELOPMENT AGENCY (SDA) IN SUPPORTING CAS

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

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

Each of these activities is detailed out below.

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

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

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

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

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

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

Technical Program Management of Implementation of CAS (State)

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

- Preparation of technical manuals to enable the SI to configure, customize, enhance and deploy CAS in States/UTs; to be made available to SIs through the CAS online repository

managed by the SDA.

- Preparation of "CAS Implementation toolkits" that comprehensively covers details on all the aspects of the CAS (State) and CAS (Centre) applications including but not limited to technical details of CAS, configuration, customization, and extension details, infrastructure sizing details, installation, commissioning, maintenance, infrastructure environment turning, and performance tuning details that are required for the SI to successfully commission the CAS (State) application in the State, integrate CAS (State) with external agencies and third party solutions in the State and integrate CAS (State) with CAS (Centre) to seamless transfer the required data to NCRB. The implementation toolkit shall also include the following:
    - All completed and updated training and support material needed for customizing and deploying CAS
    - All completed and updated project documents including FRS, SRS, HLD, LLD and Test Plans
    - Relevant software assets/artifacts (including configuration utilities / tools, deployment scripts to state SIs to deploy CAS (State) in States/UTs)
    - Relevant standards and design guidelines to the SI for customization, further enhancements, and integration of the application with external systems and third party components that will be implemented by the SI at the State
- Conduct of direct knowledge transfer through monthly contact sessions at NCRB covering all State SIs during the contract period. During the contact sessions, the SDA shall conduct structured training sessions on the CAS Implementation Toolkit prepared by the SDA
- *Dedicated State Points of Contact*: Members of the SDA's team shall act as points of contacts for the state level SIs. The number of States/UTs serviced by each SDA contact person shall be determined in consultation between the CAS Core Group and the SDA. The point of contact will be responsible for addressing queries from an SI and in meeting SLA targets (in responding to States/UTs' needs).
- *Helpdesk Support*: SDA shall provide Helpdesk support to the State SIs during customization, deployment and stabilization phases with 8 contact hours (during normal business hours of 10 AM to 6 PM), 6 days (Monday through Saturday, both included). The SDA shall deploy a team of at least 5 qualified and certified resources in NCRB to address the questions from the SIs.
- *Deployment Scripts*: The SDA shall develop the necessary deployment scripts to deploy CAS (State) in States/UTs and provide the same to State SIs
- *Data Migration Utility*: The SDA shall develop a Data Migration Utility/application with all the formats and tools to load the data into the state databases. This will be provided to States/UTs will enable the State SIs to migrate data from legacy/paper based systems to the CAS databases. The data migration tool will be an extension of the one provided by the SDA. In case the Data Migration Tool developed by the SDA does not incorporate support for any state specific formats etc, the Data Migration Tool developed by the SI will have to support these.
- *Language Localization Support*: Proving interface in local languages is a key requirement of CAS (State). The SDA shall build CAS (State) with interfaces in English and Hindi; and also build CAS (State) in such a way that it can be configured for interfaces in other local languages at the State level by the State SIs. It is the responsibility of the SI to customize CAS (State) for development of local language interfaces. However the SDA shall assist the State SIs where ever required only to support the development of such interfaces.
- Supporting the SI to ensure that the CAS (State) that is configured and customized by the SI in the State successfully passes the User Acceptance Testing (UAT) milestone.
    - Configuration of CAS (State)
    - Customization of CAS (State)
    - Data Migration of CAS (State) related data from the legacy systems and / or manual

records to CAS (State)
    - Infrastructure Sizing related to CAS (State)
    - Commissioning and Deployment of CAS (State)
    - Infrastructure Environment Performance Turning related to CAS (State)
    - Maintenance of CAS (State)
    - Integration of CAS (State) with external agency solutions
    - Integration of CAS (State) with additional solutions being integrated by the SI at the State
- Seamless data exchange from CAS (State) to CAS (Centre)
- Troubleshooting, resolution and escalation with State SIs; and ownership of end-to-end data exchange between the CAS (State) and CAS (Centre) needs to ensure seamless and real-time data exchange.

6 SCOPE OF THE PROJECT

The scope of the project envisages a complete turnkey solution which may inter-alia include procurement, installation and maintenance of hardware, system software, application software, third party tools and configuration / customization, parameterization, data digitization/ migration, site preparation, development/ Customization of application software and system integration, training and handholding, and service support for 5 (five) years post go live of the application etc as detailed out in the further sections.

6.1 Geographical Scope

Crime & Criminal Tracking Network Systems (CCTNS) will be implemented and rolled out in the state of Meghalaya. This will help improve the quality of policing system in the state, seamless integration of sharing data on crime and criminals between districts, efficient service delivery mechanism for the benefits of citizen, business, industry, police department, local government etc.

S.No	Category of Police Unit	Indicative Number
1.	Police Stations (including CID P.S.)	39
2.	Circle Offices	19
3.	Sub-Divisional Offices	8
4.	District Headquarters	7
5.	Range Headquarters	2
6.	Police Headquarters	1
7.	State Crime Record Bureau	1
8.	Forensic Science Lab (FSL)	1
9.	Finger Print Bureau (FPB in PHQ)	1
10.	SCRB computer training lab centre	1
11.	PTS/DTCs	8
12.	PCR/SCR (SCR-1,PCR-7)	8
Total		96

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

The aforementioned locations would be covered for implementing CCTNS project including but not limiting to, Site Preparation, procurement, deployment and commissioning of requisite Hardware, Network connectivity, deployment and commissioning of CAS (State) and additional modules (with proper integration) as per the requirement of Meghalaya Police, training & handholding support and further provisioning of the all the services mentioned as per scope of work of this RFP. The following required details for these offices are as follows:

Implementation Plan

It is proposed to roll out CCTNS in phases. Deployment of hardware, connectivity and other infrastructure across all police stations, higher offices and other police units would take place as provided below. The core focuses of each of the phases are delineated below:

CCTNS Phase I – Pilot Phase

During the first phase of the application, CCTNS would be rolled out in 2 districts at various Police stations and higher offices. The roll out would include installation and commissioning of hardware, connectivity, other infrastructure and associated services (such as handholding) etc. as per the scope of work.

Note: The Pilot phase I activities would also include Commissioning and operationalization of IT infrastructure at Data Centre and DR Site

Sr.No	Description	In Phase I
1	Police Head Quarters	1
2	Range Offices	1
3	District Headquarters Offices	2
4	No of Police Subdivisions office	2
5	No of Circles	6
6	No of Police Stations	20
7	SCRB	1
8	PCR	2
9	SCRB computer training lab centre	1
10	PTS/DTCs	8

CCTNS Phase II

During the next phases of CCTNS, the remaining police stations will be covered for the installation and commissioning of hardware, connectivity and other infrastructure and associated services.

The districts where the next phases would be rolled out are provided below.

Sr. No	Description	Number of Locations
1	Range Offices	1
2	District Head Quarters	5
3	No of Police Subdivisions office	6
4	No of Circles	13
5	No of Police Stations	34
6	Forensic Science Lab	1
7	Finger Print Bureau (in PHQ)	1
8	PCR	6
9	SCR	1

Operate & Maintain Phase

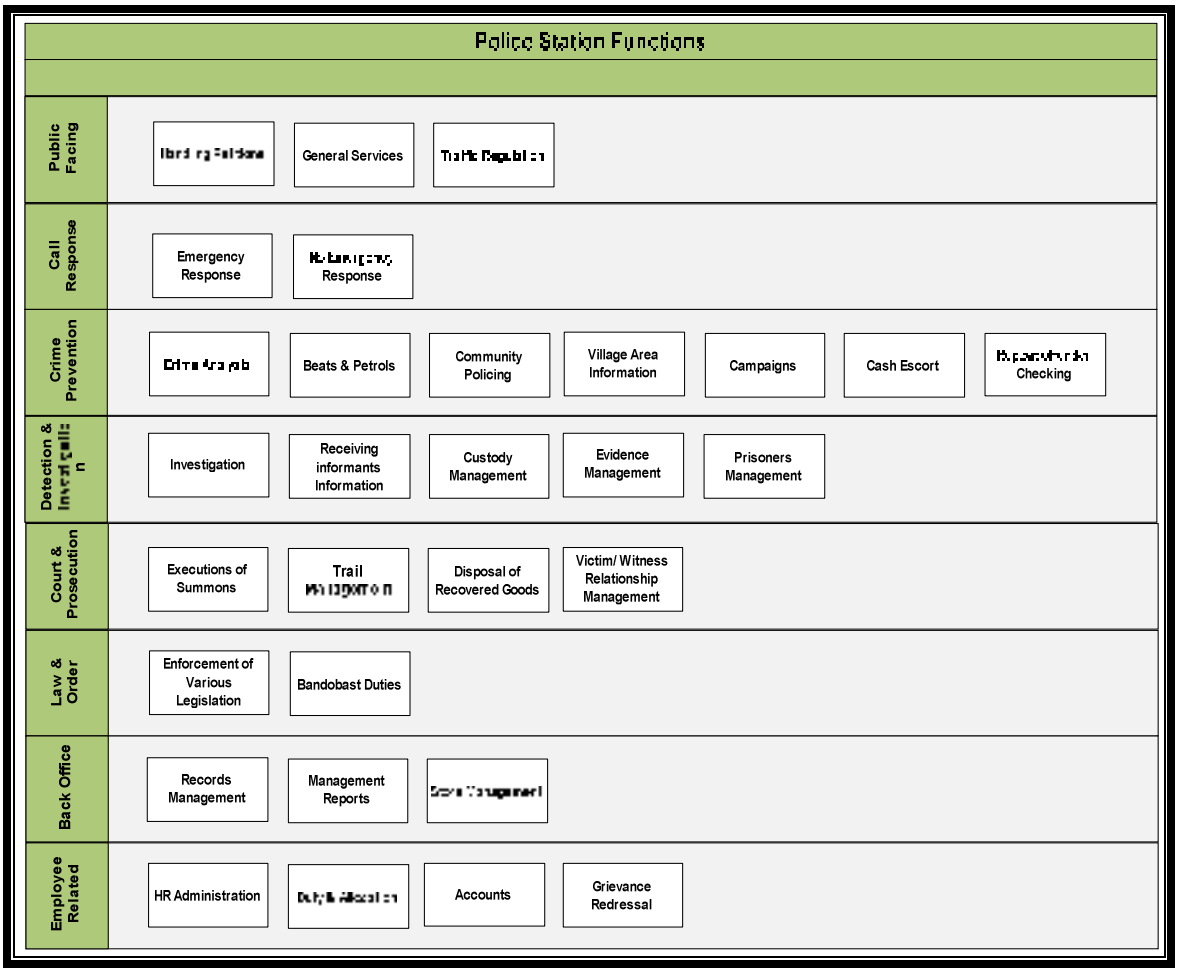
Operate and Maintain phase would be initiated after the successful implementation of CCTNS as per the scope of work mentioned in this RFP. In addition to activities relating to operate and maintain of the comprehensive CCTNS solution, the phase would also include the implementation of subsequent versions, upgrades, patches of CAS as released by NCRB and the other initiatives of Meghalaya Police as part of MMP CCTNS.

6.2 Functional Scope

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, band bust 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.

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



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.

6.2.1 CCTNS Functional Modules

Although a few of the mentioned functions have been mapped under either of the Core Application Software (State) modules[3], the Meghalaya Police has customized the Functional Modules of the CAS (State) as per their requirements. A brief of the customized Functional Modules[4] being proposed as part of the scope of SI under Meghalaya CCTNS Solution is as follows:

Modules Proposed for CAS(State)	Particulars	Description
1.Citizen Portal Service	Functionality	*It will act as a front end window to the citizens where they can request for various online services like* ▪ *Complaint Registration* ▪ *Verifications requests(employment verifications etc)* ▪ *NOC for vehicle theft, Lost cell phone/passport* ▪ *Tracking of status of his petitions/requests etc* ▪ *Licenses for Arms etc.* *It shall provide Informational services like* ▪ *Missing Persons listing* ▪ *Proclaimed offenders listing* ▪ *Stolen/recovered vehicles listing* ▪ *Abandoned/unclaimed/recovered properties listing* ▪ *Most wanted Criminals listing etc* *Shall allow the foreigners to submit C forms; apply for Residential Permit/Residential Certificate.* *Online RTI requests* *Shall allow the hotels to upload information of the customers staying at Hotel.* *Shall allow the citizen to provide sensitive information anonymously.* *Portal services for Police Officials*
	Integration requirement	State Portal, Petition Management services, Registration module, e-form application etc.
2.Petition Management Service	Functionality	*The service shall enable the police personnel to register and process the different kinds of petitions, complaints and general service requests from citizens at the police station.* *Shall be processing/managing various verification requests received from citizen and from external agencies like RPO/SDM office.* *Shall be processing general petitions like NOC for vehicle*

[3] CAS (State) SRS as issued by NCRB shall be referred for the same

[4] Bidders are required to read the FRS/SRS issued by the NCRB, as well as the Indicative FRS of CCTNS Meghalaya attached as Annexure-IV to this document.

Modules Proposed for CAS(State)	Particulars	Description
		theft, lost cell phone etc *Shall allow processing the foreigner's application for Residential Permit/Certificate.*
	Integration requirement	Integration with registration module & Interface with external agency like Transport Department, Passport office etc
3.Unclaimed/Abandon Property Register Service	Functionality	*The service shall enable the police personnel to record and maintain unclaimed/abandoned property registers and match the property with property in lost /stolen registers.* *Shall enable the police department to upload the auction details* *(Auction is carried out if the unclaimed property is kept for more than 6 months)*
	Integration requirement	Registration module, search module
4.Complaint and FIR Management Service	Functionality	*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.* Apart from the cognizable offences, it shall consider the registration of the cases like Missing Persons, Unnatural deaths, etc.
	Integration requirement	Registration module, Prosecution module & Investigation management service module
5.PCR Call Interface and Management Service	Functionality	*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.*
	Integration requirement	Registration module, Prosecution module & Investigation management service module
6.Investigation Management Service	Functionality	*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.* *Shall enable the police personnel to* ▪ *prepare crime detail form,* ▪ *add/view case diary details,* ▪ *add/view case progress report,* ▪ *preparation of arrest memo,* ▪ *preparation of seizure memo,* ▪ *search/view details of seized property,* ▪ *add finger print/forensic report etc details received from external agencies,*

Modules Proposed for CAS(State)	Particulars	Description
		▪ *Preparation of remand request form* ▪ *Prepare interrogation form* ▪ *Generation of final form/ Chargesheet etc.* Shall allow the higher officers to monitor the cases and give their comments/instructions to be followed by the investigating officers. *The module would essentially rely on the data entry by IOs, therefore complete data entry in the system is proposed to be ensured by system generated Charge Sheet after mandatory filling IIF forms No. 2, 3 and 4.* *Shall generate clues/hints through patterns and other details to help the officer in the investigation of crime.*
	Integration requirement	Investigation module, prosecution module, FSL module, AFIS application, Interface with external agency like Transport Department, Health Department etc.
7.Court and Jail Interface & Prosecution Management Service	Functionality	*The service shall enable the police personnel to interface with the courts and jails during the investigation process (producing evidence, producing arrested, and remand) and during the trial process.* *The module shall enable the user to process all the prosecution related details like* ▪ Assigning case number from court ▪ Re-opening and appointment of Investigating officer ▪ Add/View Trial details ▪ Add summon/warrant details issued by court and assign PS/Police officer for its execution ▪ Case Disposal details ▪ Add view Jail release details etc
	Integration requirement	Prosecution module
8.Crime and Criminal Records and Query Management Service	Functionality	*The service shall enable the police personnel to view the several registers and perform basic and advanced queries on the crime and criminal information.* *Manual registers would be replaced by the CAS registers which will be used for quick access to crime and criminal information. Databank services shall allow recording all the crime related information in detail through various registers as indicated in SRS (prepared by SDA).* *Query service shall allow to access all Crime/Criminal and other related information like* *Crime/Criminal Enquiry, Advisory memo,*

Modules Proposed for CAS(State)	Particulars	Description
		Numbered/Unnumbered property search, General service request enquiry, Talash enquiry etc.
	Integration requirement	Search module
9.Police Email and Messaging Service	Functionality	*The service shall enable the police personnel to send / receive both official and personal correspondence.* *The Police Messaging system is role based communication system to help the police personnel send "Faster" and "Secure" official correspondence within / across the multiple wings within / across the Police departments. It would provide general mailbox features such as address book, send / receive mail with attachments, creation / deletion of folders, moving mail to folders, spell check, mail filters, calendar, rich text editor, auto responders, signatures, server side mail filters, spam filters and support the mail protocols (IMAP and SMTP).*
10. Periodic Crime and Law & Order Reports and Review Dashboard Service	Functionality	*The service shall enable the police personnel to view the reports and dashboards required conduct the periodic crime and law & order reviews of the police station(s) under the officer's jurisdiction.* *Dashboard shall be customized according to the requirements*
	Integration requirement	Search module
11. Notification of Alerts, Imp. Events, Reminders & Activity Calendar or Tasks Service.	Functionality	*The service shall capture / generate the required alerts, important events, reminders, activity calendar and tasks.* Alerts to the police officer on the arrival of a new citizen service request, complaint/FIR registration, alert to all the police stations on the report of a missing person/dead person, alert on new comments/remarks by higher officers, alert on reopening of a case, on updation of trial details, non execution of warrant/summon, etc.
12. State-SCRB-NCRB Data Transfer and Management Service	Functionality	*The service shall enable the states to collate, transform and transfer the crime, criminal, and other related data from state to NCRB.*
13. State CAS Administration and Configuration Management Service	Functionality	*The service shall enable the individual states to configure the application to suit to their State's unique requirements.* *With this service, it shall be possible to configure the CAS state according to the requirements like configuration of User Interface, Alerts, messages, Report name/format. Hierarchy level, Work flow, staff with roles & rights etc.*
	Integration	*Configuration module*

Modules Proposed for CAS(State)	Particulars	Description
	requirement	
14. User Help and Assistance Service	Functionality	*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.*
15. User Feedback Tracking and Resolution Service	Functionality	*The service shall enable the police personnel in logging the issues/defects occurred while using the system.*
16. Activity Log Tracking and Audit Service	Functionality	*The service shall capture the audit trail resulting from execution of a business process or system function.*
17. User Access and Authorization Management Service	Functionality	*The service shall enable the administrative user in setting the access privileges and will provide authentication and authorization functionality*

Note: *Detailed Functional Requirement Specifications are attached as Annexure IV to this RFP*

SI will be required to customize the CAS (State) as received from NCRB and shall also be responsible for developing/ deploying other additional Modules meeting the functional requirements mentioned in the Functional Requirement Specifications attached as Annexure to this document and other integration requirements.

SI would be required to develop the following modules:

S.No.	Modules	Description
1.	Grievances Redressal Systems for citizens and employees	This provides various stakeholders a mechanism to get their grievances addressed by appropriate authority
2.	Traffic eChallaning module System	The aim is to make the traffic functioning smooth and traffic operation more compliant to law by extending citizen e-eChallaning facility
3.	FSL Module	The aim of the FSL module is to streamline the workflow between the different divisions of the FSL, right from receipt of samples to dispatch of expert reports, capturing data related to each division to performance monitoring of Mobile Crime Scene teams, etc. DNA databank with cross matching facility will be a part of it.
4.	Cyber Crime Management Service	In order to address the growing incidents of cyber crime, this module will equip police to have a prompt response to any eventualities.
5.	Duty Deployment Management Systems	This would help the police to streamline their forces and utilize the available manpower at the best.
6.	Intra Departmental Communication System	This would smoothen intra departmental communication and would go a long way in improving the service levels.

Selected System integrator will also be responsible for integrating the additional developed modules with CAS (State) and would also be providing the integration interfaces as mentioned in the section 5.2.3 “State Specific Requirements” of this RFP.

6.2.2 Architectural Requirements[5]

National Crime Record Bureau, Ministry of Home Affairs, Government of India is the driving group behind the development of Core Application Software at the Central level, therefore Architecture have been identified at that very level. However, a detailed TO BE state for the ICT Hardware and architecture has been defined for Meghalaya Police with focus on how the solution will enable the Meghalaya Police to provide a consolidated suite of applications that can seamlessly interface with external sources such as other States, Centre, and other external agencies.

CCTNS is deployed on a centralized architecture wherein application would be deployed at the State Data Centre at Shillong and various offices of Police Department will connect to the system through WAN. The overall technology solution would be based upon most relevant and suitable architecture standards including standards for Service Oriented Architecture (SOA), XML services & necessary protocols for internet applications, Data Centre standards etc.

A brief understanding of the Proposed Deployment Architecture, Solution Architecture, Technical Architecture and Application Architecture is provided below:

Deployment Architecture

The proposed overall solution framework for the Department is presented in this section depicting the overall 'Big Picture' of the key target areas of IT initiatives and their inter-relationships. This blue print would be used as a communication tool that provides a snapshot of the overall goal/ direction to be taken up for implementation of CCTNS project to which all the stakeholders could relate to, without getting into the complex details of the internal workings of each of these initiatives. All the modules depicted in the overall solution framework and explained in detail as part of the Functional Requirement Specification – provides the overall goal of the Department, including the adoption of core applications modelled under the CCTNS scheme.

It is required that all the additional modules to be developed by SI should be complying to DIT, GoI standards and guidelines for open standards. This would enable ease of interoperability and also be significantly more economical for the Meghalaya Police. It is recommended that SI will opt for Service Oriented Architecture (SOA) for implementing CCTNS application modules[6].

The SI shall choose the technology such that:

- It can help businesses (Police functions) respond more quickly and cost-effectively to changing market conditions.
- It shall promote reuse at the macro (service) level rather than micro (classes) level. It can also simplify interconnection to - and usage of - existing IT (legacy) assets.
- It shall also support the principles of good design: Granularity, interoperability modularity.
- The issues related to performance, manageability, and scalability shall be well addressed and system shall provide a more manageable system and less contention for resources.

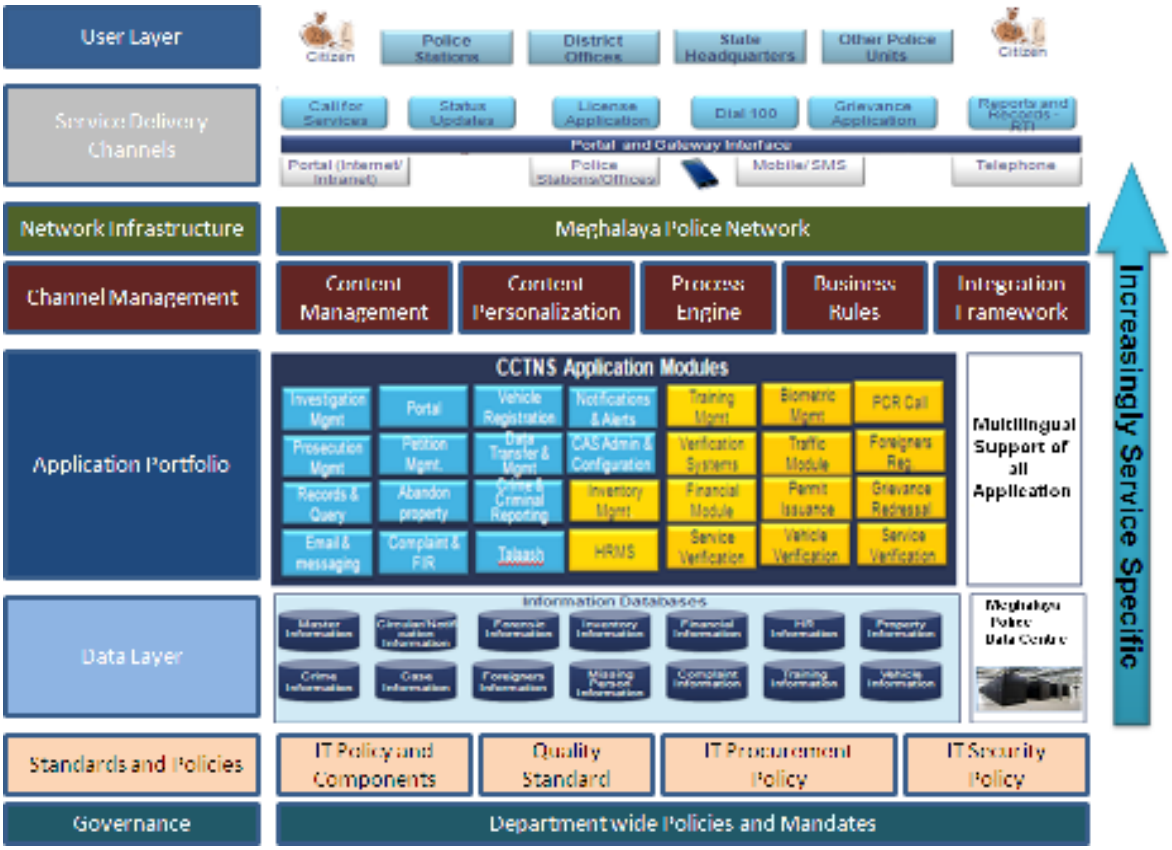
[5] This is an indicative Solution & Technology Architecture. SI will carry out detailed study to develop the exact Solution & Technology Architecture for Meghalaya CCTNS solution considering NCRB guidelines.

[6] CCTNS application modules or CCTNS suite would mean customized CAS (State), additionally developed modules, integrated modules, interfaces, web portal, other application modules under scope of this project.

Solution Architecture

In this section, the major components of the Solution Architecture that are the building blocks of the entire information technology system, have been defined and elaborated in the context of how these information blocks will add up to deliver the envisioned services will be discussed

The overall Solution Blue-print[7] of the Meghalaya CCTNS is depicted in the figure below:



S. No	Component Name	Description
1	Governance	Governance will require robust Service Level Agreements ('SLAs'), either internally or with external vendors, to be defined per service. The infrastructure, delivery and applications could be managed internally or outsourced but the SLAs need to be defined for all of the services keeping in mind the business requirements for servicing the citizens. Some of the IT Governance practices that need to be defined / modified in the processes are: • Availability Management • Service Level Management • Incident Management • Change Management • Configuration Management

[7] Indicative Functionalities of the additionally proposed modules are part of the FRS document, attached as Annexure

S. No	Component Name	Description
2	Standards and Policies	Ensuring sustainability of the processes, some of the policies that need to be defined / modified are:- IT Policy and Components consists of: • Program change; • Selection and procurement procedures; • Project and contract management; • Platforms and systems operation; • Databases; • LAN / WAN; • Program development; • Systems documentation standards; • Access controls; • User management; • Help desk management (With problem escalation path); • Password management; • Virus protection; • Internet usage; and • Backup procedures Quality Standard-A standard quality norms needs to be in place across the Department. IT Procurement Policy- A standard procurement policy needs to be in place. IT Security Policy –The policy needs to be framed in line with the to-be scenario for Identity management of users in Meghalaya Police Department.
3	Data Layer	This layer holds the databases of the various applications/modules built under the CAS. All entered data is stored here, and used for report generation and application functioning. These databases are also interconnected to enable data access by multiple applications.
4	Application Portfolio	The application portfolio is the basket of all applications that are part of CAS (State). As shown in the diagram, this constitutes all the functionalities that the CAS is to perform, and has the business logic for the software. This layer encompasses all the applications that have been built in by the NCRB at the centre, as well as the proposed new modules that would be built at the State by the SI.
5	Channel Management	All the service delivery channels will need information and standardization of data and information wrt CCTNS related data. This should essentially consist of the following sub components viz.: • Content Management - Essentially consisting of Content Creation, Content Management. Publishing and Presentation • Content Personalization - Personalized content is content which matches a particular context, generally around a user. It takes into account information contained in the context to correctly generate

S. No	Component Name	Description
		search queries, which will retrieve the content most appropriate to the context. • Process Engine - The business processes would be translated into BPM working using business process management notations (BPMN), which is modeled in the process modeler and activities are mapped to the services. The process modeler converts the model into a XML file called that is also known as business process execution language (BPEL). The BPM workflow engine interprets the activities in the workflow and attaches it to the services in the service broker. • Business Rules Engine - The business rules of the workflows modeled on in the process engine is stored in a common repository. • Integration Framework - The integration framework would provide integration services from various application portfolios that are part of the enterprise architecture. The integration framework should be compatible to services that follow open standards and also few proprietary standards which are widely followed so that proprietary services may also plug n play in the enterprise architecture though it is not advised. For proprietary standards, the integration framework should provide adapter for the widely used proprietary standards and technologies.
6	Network Infrastructure	A well defined network infrastructure is the backbone for delivering the services through the channels and also to access all vital information related to CCTNS. Since it defines the delivery speed of information / service through the channel, it is an important factor to infuse user confidence and sustain interest in the usage of the channel. For the successful implementation and deployment of the application modules at Meghalaya Police, it is essential that the system is backed up with sufficient connectivity infrastructure. Primary mode of connectivity and backup modes of ensuring connectivity are discussed in details in the deployment section.
7	Service Delivery Channels	Service delivery channels refer to the channels through which the Police department provides service delivery to internal and external stakeholders. These consist of Police Stations, and Other offices of the Meghalaya Police, Email, Online web portal, telephone, SMS, and mobile phones.
8	User Layer	The user Layer consists of the various users of the CCTNS project in Meghalaya. They consist of Citizens, Police Officers, NCRB and other stakeholders mentioned, each of whom access the Applications through respective channels of service delivery.

Technical Architecture

A centralized architecture (servers and processing at single and central location) has been proposed for the Meghalaya CCTNS project. All requests from internal and external users will be sent to the systems, located in a central place for processing. All users will access the application through local or remote

terminals using a browser (through internet for external users and through intranet or VPN for internal Departmental users).

Bidders should clearly understand that the desire of the department is not to create a mere IT Solution but an information infrastructure that will expand, integrate and enhance the functional needs of the department, citizens and other stakeholders. It is in this spirit that the core design and functional requirements are elaborated below:

(a) -**Service Fulfillment–** The objective of the System is to deliver the service from initiation to completion through electronic channels, as far as possible. Processes have been reengineered so that a stakeholder is able to access the system, perform the required tasks which may involve single or multiple back-end application interactions and fulfill the service requests through the complete solution.

(b) -**Single-Sign On –** The Solution should enable single-sign-on so that any user once authenticated and authorized by system is not required to be re-authorized for completing any of the services in the same session. For employees of the Meghalaya Police, the browser based application accessed on the intranet, through single-sign-on mechanism, will provide access to all the core services (based on their roles and responsibilities), Help module, Basic and advanced Reporting etc. Similarly, for external users (Citizens, Hotels, Cyber Cafes, Hospitals, Jails, Transport Department etc), based on their profile and registration, the system shall enable single-sign on facility to apply for various services, make payments, submit queries /complaints and check status of their applications.

(c) -**Support for PKI based Authentication and Authorization** – The solution shall support PKI based Authentication and Authorization, in accordance with IT Act 2000, using the Digital Certificates issued by the Registration Authorities (RA). In particular, PKI based authentication and authorization shall be implemented by the selected Bidder for officials/employees involved in processing key G2B and G2C services, including issuance of notices, receipts and approvals.

(d) -**Interoperability Standards -** Keeping in view the evolving needs of interoperability, especially the possibility that the solution would become the focal point of delivery of services, and may also involve cross-functionality with the e-Government projects of other departments / businesses in future, the solution should be built on Open Standards.

(e) -**Scalability -** One of the fundamental requirements of the proposed solution is its scalability. The architecture should be proven to be scalable (cater to increasing load of internal and external users and their transactions) and capable of delivering high-performance for at-least five years from the date of deployment. In this context, it is required that the application and deployment architecture should provide for Scale-Up and Scale out on the Application and Web Servers, Database Servers and all other solution components.

(f) - **Security -** The Systems implemented for Project should be highly secure, considering that it is intended to handle sensitive data relating to Crime and Criminals. The overarching security considerations are described below.

- ✓ The security services used to protect the Solution shall include: Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols.
- ✓ The solution shall support advanced user authentication mechanisms including Digital Certificates and biometric authentication.
- ✓ Security design should provide for a well-designed identity management system, security of physical and digital assets, data and network security, backup and recovery and disaster recovery system.
- ✓ The solution should provide for maintaining an audit trail of all the transactions without impacting the overall performance of the system
- ✓ The overarching requirement is the need to comply with **ISO 27001** standards of security.

The detailed quality of service requirements are given in the Service Levels attached as Annexure II to this Volume of RFP

Application Architecture

It has been proposed that the Applications designed and developed for the department must follow some best practice and industry standards.

In order to achieve the high level of stability and robustness of the application, the system development life cycle must be carried out using the industry standard best practices and adopting the security constraints for access and control rights. The various modules / application should have a common Exception Manager to handle any kind of exception arising due to internal/ external factors. This will help ease of application maintenance and enhancements. Similarly the modules/ application are to be supported by the Session and Transaction Manager for the completeness of the request and response of the client request. The system should have a module exclusively to record the activities/ create the log of activities happening within the system / application to avoid any kind of irregularities within the system by any User / Application.

Proposed Application Architecture

The 3-tier architecture (also referred to as multi-tier or N-tier architecture) has been proposed for the - Application Solution. -
The entire processing should take place in three layers: -

- ✓ Front-end software (client tier) - responsible for the presentation of information.
- ✓ Middleware (application server tier) - responsible for all the business rules
- ✓ Server Software (database server tier) - responsible for the manipulation and storage of data. Data ranges from text to numerical, to video on demand.

6.2.3 State Specific Requirements

Selected System Integrator would be completely responsible for successful implementation of end to end CCTNS solution in Meghalaya State as per the requirement of Meghalaya Police and on the lines of NCRB, MHA guidelines. It is imperative for System Integrator to understand two basic aspects of this project, i.e. CCTNS Solution as provided by Centre and secondly the specific requirements of the Meghalaya State, for the success of this project. An indicative list of specific requirements is detailed below; however, final specific requirements would emerge from the Detailed System Study to be conducted by System Integrator as also indicated in section 6.3.

Application Specific Requirements

1. Key Customization Requirements[8]:

The functional requirement specifications of each of the modules mentioned above in the functional scope have been defined in the attached Annexure. The functionalities which are coming through the original application has not been tampered and the customization requirements is primarily to be focused on to the configuration that is required in terms of the department's organizational/hierarchical structure, roles and rights of police personnels at various levels, reports and registers that are maintained at the different levels of the organization covering police stations and higher offices, etc. In addition to the configuration requirements, some enhancements are done into the existing modules as required by the state. The details of the enhancements are provided in the functional requirement specifications as given in the annexure.

The enhancements are important to the state for speedy reactions to critical situations and improving the citizen centric services. Some of the indicative enhancements are such as

- The rate of infiltration has always been very high in the state as the state of Meghalaya is bordered by Bangladesh on the south and Assam on the north. So to restrict the illegal entry of the foreigners keeping a track of the foreigner's movement in and out of the country is very important from the state's perspective. It is also required to maintain the registration and permit details of all the foreigners who visit the state and also to allow the foreigner to apply for RC/RP through the citizen service portal.

- Citizens have restricted access to the higher officers if they want to raise their grievances against any harassment caused by junior level policemen. To improve the citizen's satisfaction and faith towards the state police, it is thus a necessity to include the citizen's grievance module into the system. Provisions have been kept for the police officers as well where they can raise their grievances against an officer of higher rank.

- Apart from the regular police services, citizen should be able to take the benefits of RTI services through the portal.

- Citizen should also be able to pay their traffic challans through the citizen service portal.

- The system should allow to search from databases of other departments for speedy actions. E.g. RTO where lots of time and effort is wasted in obtaining vehicle and owner's information.

- External agencies should be able to request for verifications of their employees through a Login account where they can access the verification report/status for various verifications requested for.

These are some of the indicative enhancements which are required. The details are to be referred from FRS attached as annexure.

Apart from these enhancements, the modules to be added such as Grievance module, FSL module, Traffic eChallaning module, Duty Deployment management module, Intra departmental communication module etc are also provided in the FRS attached as annexure.

[8] These are only key customization recommendations, however detailed customization requirements to be done as per the FRS regarding each module.

These are some of the indicative enhancements which are required. The details are to be referred from FRS attached as annexure. Apart from these enhancements, the modules to be added such as Grievance module, FSL module, Traffic eChallaning module, Duty Deployment management module, Intra departmental communication module etc are also provided in the FRS attached as annexure.

2. Multi lingual Support:

System Integrator would be required to configure the complete CCTNS with Multilingual support (English, Hindi and the vernacular language) for User Interface, Font, Data Entry, Search, Report Generation and all types of data transactions, etc.

3. Data Entry:

System Integrator would be required to configure the CCTNS solution in such a manner that it ensures complete data entry in the system by Police officials in such as way that system should generate reports on data entry Police Unit wise, IO wise, by taking a cutoff date and generate the desired reports. In addition to this Integrated Investigation Forms would require the mandatory entry of the data for generation of Police Report to be submitted in the Court. Though it has been proposed that the CAS (State), to be provided by NCRB should be equipped with Dictionary of Common Names of Persons, Places for proper addressing, but in case it does not come equipped with the same, selected SI would be required to prepare such a dictionary of names of persons and places before initiating the exercise of Data Digitization and Data Migration. The idea is to ensure less mistakes during data entry in the names, addresses.

Selected SI is also required to configure the system in such a manner that system should send alerts in case data entry is not being performed appropriately in the modules. For example, data entry in the DDR is a continuous activity, hence in case no data is entered in DDR for 12 hours or more, system should send alerts to concerned DSP and in case no data entry for more than 24 hours, the matter should be escalated and alerts should be sent to concerned SP. Similarly for arrest forms, in case no data is entered in next 48 hours after the registration of FIR, the system should send alerts to concerned SHO.

4. Record Management:

Institutionalizing various ICT tools and technology have a common agenda of eliminating drudgery from the existing system. Automation of all the Police Station registers and system generated reports supported by Business Intelligence & Data Mining tools to empower Police Officers is what CCTNS can offer. SI would be required configure the CCTNS application with Business Intelligence & Data Mining support for Crime Analysis and Crime Pattern analysis as per the requirements of the department.

5. Case Information Recording:

Investigating Officer has always been over loaded with case investigations, and therefore consumes a good amount of time to re-align his investigations details at the day end. Hence we foresee a need for a Case Basket for every case in CCTNS application where IO may store all the case related data, such as Case Diaries, Photographs, scanned documents, audio/ visual recordings, miscellaneous correspondence, etc. at one location for his ready reckoning and anywhere retrieval. SI would be required configure the CCTNS application with this kind of concept for the successful implementation.

6. Local Database:

It would be a false assumption to anticipate seamless connectivity at all Police Stations. Therefore, local databases at Police Station to record and register complaints, has been proposed during no connectivity. As the offline mode switches back to the online mode, data recorded in local database at Police Station would automatically synchronize with central data repositories and information stored locally would be sent to the central repository.

7. Weeding out of Records:

SI would be required to configure the CCTNS system, to enforce Meghalaya Police specific requirements for weeding out of records.

6.2.4 Integration and Interfacing Requirements

CCTNS is deployed on a centralized architecture wherein various offices of Police Department connect to the system through SWAN and BSNL from State Data Centre.

The interfaces to be developed within CAS (State) should provide proper information and data sharing with external agencies, but not limiting to, Transport Authority, Jails, Courts, Hospitals, Mobile Service Providers, etc. External Interfacing shall also be State Common Service Centres (CSC), eforms applications (project in progress) (of State portals and Service Delivery Gateway), State Universities, Cyber Cafes of the State, Hotels of the State and other external government departments etc. to facilitate electronic exchange of information. System Integrator would be required to study the interfacing requirements with CAS (Centre), external agencies and other state departments for seamless integration and information exchange, as part of Detailed System Study.

It is necessary for the System Integrator to conduct a detailed study for deriving the Integration and Interfacing requirements of CAS (State). At the outset, System Integrator would also be required to study the National Level initiatives or projects for interfacing and integration requirements with CAS (State), such as but not limiting to, initiatives by Department of IT, GoI, Ministry of External Affairs, GoI, AFIS project, LIMS project, Age progression, Mobile Number Portability, etc.

National Service Delivery Gateway (NSDG)/ State Service Delivery Gateway (SSDG): The System Integrator at the state level shall register as a Service Provider with the NSDG or SSDGs on behalf of the respective State Government and provide CCTNS based services. Initially if NSDG/SSDG services are not available the CCTNS application shall access services through the existing broadband networks and SDA shall develop APIs for the required departments during CAS development to enable interoperability and interconnectivity for its eventual integration with NSDG/SSDG. C-DAC as Gateway Service Provider of NSDG/SSDG shall provide connectors/Adapters and guidelines for hosting services through NSDG/SSDG after the SI register as a Service Provider on behalf of the State/UT Governments.

Indicative types of data/ information exchange with external agency, with which interfacing of CCTNS solution will be required are as follows:

S. No.	Name Of Agency/Application
1.	**VAHAN** and **SARATHI** applications at RTO.
2.	**Passport Office (Citizen verification requests, Foreigner's visit information etc)**
3.	**State Jails**(Bail order details, Data of prisoners/ jail inmates, Data regarding movement of prisoner/ under trial/ convict/ parole, Data regarding discharge of under-trial/convict who are accused in cases figuring on the list of monitored cases or who are listed as dangerous prisoners from Jail on furlough/parole etc.)
4.	**State Courts** (Charge Sheet acknowledgement, Data of Case Trials, etc., Data of summons/warrants issued by court, next date of hearing, status of accused (whether on bail or in custody with name of jail, PO, bail jumper etc)., Court permissions, judgments, sentences, etc. against cases)
5.	**State Government Hospitals** (Medico Legal Reports, Post Mortem Reports and other requests)
6.	**Mobile Service Providers** (Data associated with the mobile subscribers)
7.	**E-services** (E-services is a state initiative done by NIC which will enable set of citizen centric services including PRC/Domicile, SC/ST Certificates, Permission for special events etc. This project is in Pilot phase and SI is expected to integrate the CAS application for smooth and effective delivery of services requiring police intervention.)

6.3 Scope of Services during Implementation Phase

The scope of the "bundled services" to be offered by the SI during project Implementation phases, includes, but not limiting to the following:

a. - Project planning and management
b. - System study and Design
c. - Configuration Customization and Extension (New Modules) of CAS (State) and Integration with CAS (Center) and External Agencies
(Note: 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).
d. - Procurement, Deployment and Commissioning of IT infrastructure at the Data Center and Disaster Recovery Center including the necessary networking components.
(Note: SI shall procure all the necessary underlying solution components required to deploy the CAS (State) solution for Meghalaya)
e. - Data migration and Digitization of Historical Data
f. - Migration of CIPA and CCIS Police Stations / Higher Offices to CCTNS
g. - Site preparation at the Client site locations (Police Stations, Range offices, Zones, SCRB, SDPOs, District HQ, and State HQ)
h. - Procurement, Deployment and Commissioning of IT Infrastructure at Client site locations (Police Stations, Range offices, SCRB, SDPOs, District HQ, and State HQ)
i. - Network and Connectivity for Police Stations, Higher Offices, Training Centers (DTC/RTC/PTC/Police Academy) for CCTNS project
j. - Capacity building and Change Management
k. - Handholding Support for end users
l. - Requirement and adherence to Standards
m. - Support to 3rd party/ User acceptance testing, audit and certification

In implementing the above, the SI shall strictly adhere to the standards set by the MHA, NCRB, and the State with respect to implementing this project. The project will be managed out of the Meghalaya Police HQ, Shillong.

Note: At all points in the execution of the project, key senior resources including the project manager must be based at Meghalaya Police HQ. Bidder to provide details of the proposed team and Governance structure duly in line with the evaluation criteria provided in RFP Volume II and applicable SLAs as per Annexure II. It is important to note that requirement with respect to proposed team and governance structure should be adhered at all times during the execution of Project.

6.3.1 Project Planning & 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 very critical and hence SI is required to design and implement a comprehensive and effective project planning and management methodology together with efficient & reliable tools. Project planning exercise would essentially commence with the start of the project, however, project management exercise would commence at the start of the project and shall continue till the currency of the project by selected SI.

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

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

The Project plan prepared by the SI at the initial stage of the project would be reviewed by the Governance Structure (please refer to Annexure III on details on Governance Structure in the State) in the State and approved by the Apex / Empowered Committee on the advice of the State Mission Team and SPMC/ SPMU.
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 Meghalaya Police or appointed representatives.

Requirements Traceability Matrix

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

Through the duration of the project, the State Mission Team will periodically review the

Traceability Matrix. State Governance Structure would provide the final approval on the advice of the State Mission Team and SPMU once they are satisfied that all requirements are met.

Project Documentation

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

Project documents include but are not limited to the following:

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

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

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

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

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

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

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

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

Issue Tracker: The SI shall employ a suitable and proven off-the shelf tool for tracking issues (with perpetual and unrestricted redistribution licenses) through the execution of the project. The SI shall install the Issue Tracking System at Meghalaya Police's /SCRB Premises to enable State's users to access and use the same.

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

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

6.3.2 System study and design

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

.

6.3.2.1 System and Software Requirements Specifications (SyRS & SRS)

For the additional functionality that the State / UT wants to be added to CAS(State), the SI shall carry out a detailed systems study to refine the Functional Requirements Specifications provided as Annexure IV to this RFP and formulate the System and software Requirements Specifications (SyRS & SRS) incorporating the functional specifications and standards provided by the NCRB and the state-specific requirements. The SRS preparation shall take into account the BPR recommendations suggested by the NCRB. The SI shall also study CAS-State and CAS-Center being developed at NCRB and / or already running application in the State during the system study

phase. The study should also include different integration points of CAS state with identified applications as per state requirement. The SRS preparation shall take into account the BPR recommendations suggested by the State.

Note: *The vendor is required to update the FRS/ SRS/ SyRS as and when any enhancements/ modifications are made to CAS (State) application till the completion of project.*

6.3.2.2 Preparation of Solution Design document would include:

High Level Design (HLD):

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

Detailed (Low Level) Design (LLD):

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

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

CAS (State) contains functionality that is common across all State. CAS (State) would be configured, customized, extended by the SI based on the unique requirements of the State and deployed at the State Data Centre. In order to ensure consistency between States and facilitate the exchange of crime and criminal's related information between State and the Center and between States/UTs, NCRB would develop, own, and maintain the CAS.

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

Briefly describing the tasks to be carried out by SI as part of CAS (State) configuration, customization, extension and integration basis requirements of the state:

1. - Deployment of Core Application Software (State) as provide by NCRB, MHA
2. - Conduct Closed Room Pilot
3. - Solution development/ Customization & Configuration of CAS
4. - Integration of CAS (State) with CAS (Centre) and External Agencies and their external applications
5. - Development of reports
6. - Testing of the configured solution (CAS) and additional functionalities.

6.3.3.1 Deployment of Core Application Software (State)

As the initial step, the selected SI will be responsible for deployment of CAS (State) application as such provided by NCRB, MHA in the development environment for further studying the exact requirements of the State in consultation with Meghalaya Police or its nominated agencies/ representatives and further customizing the deployed CAS to meet the requirements of Meghalaya Police. Such a deployment exercise will be completely different from the deployment exercise to be carried out by the SI at the time of Pilot Roll-out and Go-Live in Meghalaya; however deployment at these stages would mean deployment of customized CAS (State) in the State Data Centre for the application to be accessed by respective concerned Police Units and other stakeholders.

As part of deployment of CAS application, 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.

6.3.3.2 Conduct Closed Room Pilot

Based on all the requirement specifications finalized by System Integrator, the SI will conduct a Closed Room Pilot (CRP). The objective of the closed room pilot is to receive feedback from groups of end users on the requirement specifications of the application; and on the proposed GUI design and navigation scheme of application in a closed room setting. Based on the feedback, the SI would finalize the requirement specifications and design which shall be followed by customizing the CAS (State) as received by NCRB.

Format of the CRP

- CRP Round – I, during which different user categories would assemble and test the closed room prototype. The SI shall interact closely with the user groups and gather detailed feedback
- During the CRP, an exhaustive set of scenarios and associated GUI screens covering all the functionalities developed would be presented by SI
- The SI will analyze the feedback and incorporate applicable feedback into the requirement specifications for CRP Round II.
- CRP Round – II, during which the original user group that participated in Round – I would reassemble to test the updated prototype. The SI shall once again interact closely with the user groups and gather feedback
- The requirement specification documents and the GUI screens including navigation schemes are updated based on the CRP feedback.

User Groups

The following user groups have to be represented during both rounds of the CRP:

- Representatives from State Police Headquarters (Senior police officers)
- State Project Nodal Officer
- Representatives from SCRB
- Senior police officers at district level: SP/SSP, DySP
- Station House Officers (SHO)
- Investigation Officers (IO)
- SPMU
- Officials as identified by State empowered Committee

Other Details

- The CRP would be conducted at Police Headquarters, Shillong
- Police Headquarters, Shillong would provide logistical support and play a facilitating role
- The functionalities of CCTNS system to be covered during CRP should be comprehensive.
- Each round of the CRP will be conducted over a week
- SI would be required to provide details of required logistics arrangements well before and assist the police personnel in making such arrangements

6.3.3.3 Solution Development/ Customization of CAS

The selected System Integrator will be responsible for the solution development and customization of end-to-end CAS (State) application software including additional functionalities, integration with CAS Center and external agencies on the basis of the FRS, SyRS, SRS and solution design. The bidder will ensure that the Best Practices for Software Development and Customization are used during the software development / customization and implementation exercise. This would at a minimum include:

(a) -Software development / customization based on the functional requirement specifications, system requirement specifications, software requirement specifications and solution designs finalized for the services or customizing the existing application as per the approved requirements. Wherever necessary, the system integrator shall be responsible for developing additional functionality/modules in order to meet the business requirements of the department.

(b) -Delivering the customized CAS (State) software, along with all of the necessary modules and additional modules/ integrated COTS products, utilities, system drivers and documentation consistent with proven standards, including product updates, technology upgrades and patches to run on the selected operating system(s) and hardware according to the solution.

(c) -Deployment and commissioning of customized CAS (State) with all the necessary solution elements for implementing Pilot phase at pilot districts and associated offices. Selected SI will prepare a detailed phasing out plan for CIPA/ CIMS and CCIS as part of their Implementation Plan before the implementation of Pilot phase of CCTNS system, which would be duly verified and approved by Meghalaya Police assisted by SPMC/ nominated agencies or representatives.

(d) -Deliverance and implementation of a back up facility to be used in disaster recovery scenarios.

(e) -Provide a user friendly interface for administrative tasks of the application. Only Authorized user(s) should be able to "Modify/ Delete" data[9] from the system. Such an authorization would be provided by Director General of Police only, and shall remain undisclosed. "Deletion of the data by authorized user may or may not have audit trails. Crime and Criminal data captured though various IIFs shall not be permitted to be deleted by any other user who is not authorized. All other data as per the requirement of the Meghalaya Police shall be configured to get deleted by authorized users. However it is required to have a provision of preserving the specific data required by Police officials (SHO and above ranks only).

(f) - Provision for Police officers to login into the system remotely from any location via a secure private network. Initially this facility would be available for Officers above the rank of ASI but later it would be provided to all the Police Officers. There should be a mechanism to especially include Police Officer(s) of any rank under this facility on the approval and discretion of project Nodal Officer.

(g) -Implement all necessary access security and data validation controls during the customization/ development of the CAS solution

(h) -Preparation of necessary User and Trouble Shooting manuals for the Solution.

(i) - Finally, Integration of all modules for seamless sharing of data across all users (internal and external)

[9] Data regarding crime and criminal captured though IIFs shall not be permitted for deletion by any user.

At each of the above phases, the SI would have the deliverables (including documentation) reviewed and approved by the Meghalaya Police or its nominated agencies/ representatives on the advice of State Mission Team /SPMU. State Police headquarters/Nodal officer will sign off on the deliverables; only then should the vendor commence with the next phase. Software modifications / development will be considered completed only after formal acceptance provided by Meghalaya Police.

Configuration of CAS (State):

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

1. Developing Local Language Interfaces (on the lines of CIPA) and Support
2. Configuring users
3. Configuring Police Stations / Higher Offices
4. Configuration of the User Interfaces as required by the Meghalaya Police

The collection of the data required for the configuration of the CAS (State) shall be the responsibility of the SI. SPMC in coordination with the Meghalaya Police shall validate the data collected by SI as part of study under this RFP.

6.3.3.4 Integration of CAS (State) with CAS (Centre) and External Agencies

The System Integrator would be required to carry out comprehensive application integration for CCTNS solution including CAS (State) and additional developed/ deployed modules with CAS (Centre) and the applications of External Agencies. Integration requirements are also mentioned in the section 6.2.4

6.3.3.5 Development of Reports

As part of CAS configuration, customization, extension and integration, the System Integrator would also be responsible for facilitating reports[10] from CAS. The SI would be required to provide / facilitate centralized MIS reports to meet the reporting requirements of the Meghalaya Police

6.3.3.6 Testing of the configured solution (CAS) and additional functionalities

Creation of Test Plans

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

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

Application Development and Unit Testing

[10] Reports to be generated by CAS (State) are provided as part of the FRS released in RFP for selection of SDA at Centre. Bidders are requested to refer the same.

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 entire CCTNS suite in accordance with the approved test plans and test cases. It is important to mention that SI will be required to conduct all the tests approved by Meghalaya Police initially during Pilot Phase and finally during the complete rollout of CCTNS integrated solution. The SI shall consider the local language support and prepare necessary configuration files for both CAS and additional functionalities/modules developed as part of implementing CCTNS in Meghalaya Police.

The SI would also implement the changes[11] proposed in the Change/Reference document to Core Application Software and carry out a thorough regression testing includes running some of the previously executed scripts for the functionality from the traceability matrix provided by NCRB/State.
The SI shall also develop a Data Migration Utility/application for the additional functionalities with all the formats and tools to load the data into the state databases. This will migrate data from legacy/paper based systems of the new modules to the CAS databases.

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

Regression, Integration, System and Functional Testing

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

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

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

The SI along with SPMC/ State Mission Team/ SPMU[12] 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 SPMC/ State Mission Team/SPMU/Empowered Committee for validation.

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

[11] SI shall implement all the suggestions/ changes proposed by Meghalaya Police without considering it as part of the Change Control till the completion of one year of Handholding support by SI.
[12] SPMU shall be in place for undertaking all the responsibilities as per NCRB, MHA guidelines post Pilot Phase implementation of Meghalaya CCTNS

User Acceptance Testing (UAT)

Test Plans for Initial and Final UAT would be prepared by the SI in collaboration with the SPMC/ State Mission Team /SPMU/ domain experts. The SI will plan all aspects of UAT during both phases (including the preparation of test data/ reports) and obtain required support from State Police Headquarters to ensure its success. SPMC/ 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 or any other component of entire CCTNS solution to ensure that UAT is successfully conducted.

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. SI shall be responsible for all the arrangements required for testing, including but not limiting to Site visits, preparation of test reports, printing the test reports, presenting the test reports, etc.

6.3.4 Procurement, Deployment and Commissioning of IT infrastructure at the Data Center and Disaster Recovery Center including the necessary networking components

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

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

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

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

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

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

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

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

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

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

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

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

1. - Rack
2. - Power and Cooling
3. - UPS, DG set power backup
4. - Bandwidth and Connectivity
5. - LAN
6. - VPN
7. - Firewall
8. - Intrusion Protection System
9. - Fire prevention
10. Physical security surveillance
11. Network Operation Centre
12. Common Data Centre facility Maintenance and Support

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

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

SI shall develop / procure and deploy an EMS tool that monitors / manages the entire enterprise wide

application, infrastructure and network related components. The SI shall also deploy a backup software to - periodically backup all data and software. -
SI would be responsible for procurement and deployment of the indicative servers at the SDC and DRC - site. The SI shall also deploy a backup software to periodically backup all data and software.. -
Note: *The SI will ensure that all the licenses of proposed application / system software etc. procured for this project are procured in the name of Meghalaya Police and shall be full use perpetual licenses.*
Given below is an indicative format for Technical Bill of Materials for DC and DR site

Item Description	Qty.
Data center: SAN Storage including SAN Switch & SAN Storage Management Software, Backup Software	1
Disaster Recovery Site: SAN Storage including SAN Switch & SAN Storage Management Software, Backup Software	1
Data Center Servers	
Web Server	1
Directory Server + Access Manager	1
Application Server	2
Database Server	2
Management Server	1
Enterprise backup Server	1
DR Center Servers	
Web Server	1
Application Server	2
Database Server	2
Automated Tape Library (ATL) for Data Center with Backup Software	1
Software for Data Center and DR Center	
Software and Licenses	As Required
Project management Information System (PMIS)	1
Project Management Tool	1
Configuration Management	1
Issue Tracker	1

Note: The technical specifications of Web Server, Application Server, Database Server, Storage etc has been provided in **Annexure X.**

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

Data Migration Requirements

1. Since there could be structural differences in the data as stored currently from the new system there should be a mapping done between the source and target data models that should be approved by Project Nodal officer from Meghalaya Police
2. Carry out the migration of legacy electronic data by using data migration utility
3. Carry out the migration of the data available in the existing registers, reports, case files,etc.(Physical Copies) by data digitization
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 empowered Committee/ Identified official from Meghalaya Police for verification, including number of records, validations (where possible), other controls / hash totals. Highlight errors, abnormalities and deviations.
6. Incorporate corrections for the errors discovered during verification process, as proposed
7. Get final sign off from Meghalaya Police / Empowered Committee for migrated / digitized data
8. At the end of migration, all the data for old cases and registers must be available in the new system

Scope of Data Migration

CIPA was implemented in 17 Police Stations of the State of Meghalaya. Therefore data regarding Registration, Investigation and Final Report is digitized in these Police Stations for the last three years. Data would be required to migrate from CIPA Police Stations to the new CCTNS system.

Names of the Police Stations covered under CIPA are attached as Annexure VIII. Although data migration utility would be provided to the Meghalaya Police from MHA, GoI, SI would be required to assess it and if required customize it to meet the requirements of Meghalaya Police, with respect to data migration at no additional cost to the department. It is important to mention that SI shall be responsible for the quality of data migrated from existing systems and should meet the expectations of Meghalaya Police. SI will be required to provide support for acceptance testing of data migrated to the new system and shall carryout all the changes, proposed as feedback after acceptance testing with no additional cost to the department.

Note: SI would also be required to carryout the data reconciliation and de-duplication 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 Project Nodal Officer from Meghalaya Police.

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: All the steps to be undertaken as part of data migration strategy shall be exercised in consultation with representatives from Meghalaya Police or its nominated agency/ group.

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. SI shall be required to adopt a comprehensive methodology for Data verification/ validation. An indicative methodology is provided in subsequent section, however SI will be required to improve upon the methodology and get the final methodology approved from Meghalaya Police or its nominated agency/ representatives.
h) - Test the success of the data take-on by doing system test. It is important to mention that correctness of data digitized and migrated is of the utmost importance to Meghalaya Police, therefore SI is required to follow the SLAs specifically defined for Data Digitization & Data Migration.

3. Data Take–On

Take–On phase will be initiated when the proposed solution is ready to be deployed at Pilot phase. 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 -

Note:

In case at Pilot phase implementation data is found to be erroneous/ non acceptable in nature, SI will be required to make necessary changes/ modifications in the data at no additional cost to the department

Additional Guidelines for Data Migration

1. - SI shall migrate/convert/digitize the data at the implementation sites of Meghalaya Police.
2. - SI shall formulate the "Data Migration Strategy document" which will also include quality assurance mechanism. This will be reviewed and signed–off by Meghalaya Police or its nominated agency/ representatives prior to commencement of data migration.
3. - SI shall incorporate all comments and suggestions of Meghalaya Police 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 ensure accuracy and completeness of the data as per approved data verification/ validation strategy.
8. - SI shall convey to Meghalaya Police 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 Meghalaya Police
9. - In the event Meghalaya Police is unable to obtain all the mandatory fields as conveyed by SI, SI shall suggest the most suitable workaround to them. SI shall document the suggested workaround and sign-off will be obtained from Meghalaya Police for the suggested workaround. SI shall implement the suitable workaround for Meghalaya Police at no additional cost to the department.
10. SI will be responsible for developing data entry programs / applications that will be required for the purpose of data digitization in order to capture data available with / obtained by Meghalaya Police in non – electronic/ manual format.
11. SI -shall support in conducting the acceptance testing and verifying the completeness and accuracy of the data migrated from the legacy systems to the proposed solution.
12. Meghalaya Police 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 and 100% data of convictions). 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).

Sl. No.	Data	Details
Unit 1	Case Files	All the 7 IIF Forms, FIR Copy, Case Diaries, Extract Copies/Forward letters, Seizure Lists, Charge Sheet/ Final Form, Case Result etc and various associated registers where data from FIRs are recorded like Conviction register, Surveillance Register, Absconders Registers, Crime against property, Malkhana Register, etc. Number of cases recorded in the last 10 years approximately is 20000
Unit 2	VCNB Registers	Village Crime Notebooks record the data from First Information Reports on crime and process of enquiry/ information on people identified as Bad Characters and crime against property details The number of estimated records are approximately around 15000
Unit 3	Non-FIR Registers + other registers at PS(like Missing Person/Vehicle Missing/Arms Register etc)	Registration of all the petty cases. It will make the crime database more robust in nature. The number of estimated records are approximately around 25000
Unit 4	Verification Records	Service Verification, SC/ST/OBC/Domicile/PR certificate Verification, Passport Verification, Verifications related to Arms License, Driving License, Vehicle Permit, Motor Vehicle Verification, Contractor, Agents. The number of estimated records are approximately around 25000

Unit 5	Foreigner's registration Records	Registration Forms like Form A, RC Form etc and the associated registers. Foreigners' details are very important as the state of Meghalaya is surrounded by Bangladesh on the south and the infiltration rate is quite high. For the prevention and quick action, the foreigner's database is very important. The number of estimated records are approximately around 1500

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.

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

The SI will be responsible for carrying out the comprehensive migration of the Police Stations and Higher Offices currently operational on CIPA and CCIS to CCTNS Solution as part of the CCTNS implementation in the State of Meghalaya. Migration exercise shall include transition from the existing manual and CIPA/ CCIS based systems to new solution in such a fashion that the day to day activities of the Police officials are not impacted. SI shall prepare a complete transition plan for migrating from existing system to the new system, which would get approved from Meghalaya Police or its nominated agencies. It is important to mention that SI shall take all due caution to prepare the transition plan in such a way that the new system properly sustainable and commissioned enough to phase out the existing system.

The transition plan to migrate from existing systems shall consist of planning for both the phases i.e. Pilot and complete roll-out. SI shall be responsible for successful transitioning from existing system to the new one.

Once the migration exercise is successfully completed for each phase, SI shall inform formally to the Meghalaya Police for its acceptance, The acceptance testing for the migration exercise shall be carried out individually for both the phases at all the concerned locations. Meghalaya Police or its nominated agencies shall perform the acceptance testing exercise based on the Test cases and plans submitted by SI and SI shall provide all the required support for conducting the acceptance testing.

In case acceptance testing results in unsatisfactory performance, SI shall carryout all the necessary changes or perform all the necessary actions to undertake a successful migration exercise at no additional cost to the department.

Note:
At any point of time during the course of project implementation Meghalaya Police or its nominated agencies feels that the Acceptance Testing Plans and Cases are insufficient/ incapable to assess the system, SI shall carryout the necessary modifications/ changes in the test plans and cases to meet the requirement of Meghalaya Police at no additional cost to the department.

6.3.7 Site Preparation at the client site locations (Police Stations, Range offices, Zones, SCRB, SDPOs, District HQ, and State HQ)

The Meghalaya Police shall provide the necessary minimum constructed rooms/ space permanent construction/ prefabricated construction, to the SI. The SI would be responsible for conducting a site survey to identify the exact situation of the sites for ensuring site readiness for the institutionalization of the CCTNS infrastructure and commissioning of the same. The SI would prepare 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. SI would be responsible to prepare the client sites for setting up the necessary client site infrastructure

Scope of Site Preparation is as per the activities provided below and the requirements mentioned in **volume II**

Site preparation for various CCTNS locations:

i. - **Setting up of Local area network :** SI will be required to set of Local Area Network in Police Stations and Higher Offices. This would involve, but not limiting to laying down the structured cabling using CAT-6 UTP cable, crimping of cables, creation of patch panels, proper fixing of LAN cables in PVC conduits or raceways along with all the necessary accessories. SI shall be responsible for testing and certifying the structured cabling at each location and finally commissioning the LAN by installing all the network components. (active and passive) to fully support the functioning of CCTNS solution in the location.

ii. - **Electrical cabling and earthing requirements:** This includes Point wiring to be done using ISI approved PVC Conduit / Casing Capping, 1.1 KV grade 2.5 square meter FRLS Cu, supply and installation of switch, socket, and all necessary hardware & accessories.

iii. - **Adequate power Points**: SI is expected to ensure adequate power points with proper safety in adequate numbers at all the site

iv. - **Adequate Furniture: computer workstations:** 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.

SI to provide at the minimum at all locations one computer table and one chair to be supplied against each Desktop computer provisioned and one Storage cum top for Printers/ Multi functional device

(Please refer **Annexure X** for technical specification for various components)

6.3.8 Procurement, Deployment and Commissioning of IT Infrastructure at the client site locations (Police Stations, Range offices, Zones, SCRB, SDPOs, District HQ, and State HQ)

The premises for offices will be provided by the department at respective locations. SI will be responsible to procure, install and commission the CCTNS infrastructure required at the locations statewide.

At each such location the following shall be carried out.

1. - Supply of the hardware, software, networking equipments, UPS, DG set to the location as per the requirements
2. - Ensure adequate number of power points with proper electric-earthing (In case the adequate number is not there, SI shall be responsible for undertaking this exercise of providing adequate number of power points with proper electric-earthing)
3. - Network Connectivity - Ensuring last mile connectivity and testing. (At some locations SWAN may be available, SI may propose to use the existing SWAN connectivity or implement VPN over broadband.
4. - Installation, Testing and Commissioning of UPS, DG-Set[13]
5. - Physical Installation of all the equipments such as Desktops, Printers, Scanners/ MFP, Network devices including Switch- Connecting peripherals, Digital Pen, etc.
6. - Operating System Installation and Configuration for desktops and servers at all locations
7. - Installation of Antivirus and all other support software/ drivers, if any
8. - Configuring the security at the desktops, switch and broadband connection routers
9. - Network and browser Configuration
10. Test accessibility and functionality of CCTNS application from the desktops
11. Ensuring all the systems required are supplied, installed, configured, tested and commissioned and declaring the site to be operational.

[13] SI will be completely responsible for DG Set's maintenance, insurance and warrantee, However Meghalaya Police will be responsible for diesel required for DG Set. A log book shall be maintained at each location by SI detailing the fuel consumption for each DG Set.

12. In addition to the above, supply and fixing of furniture like computer tables, chairs and other items shall be carried out to ensure successful site preparation and installation of CCTNS at every location

It shall be the responsibility of the Selected SI to bring all the installation equipments and tools required for the aforementioned all activities. CCTNS application will be accessed and used at various access locations across the state like Police Stations, Sub Division office, District Office, Range Offices and other higher offices.

In terms of procuring, installing and commissioning of the CCTNS infrastructure required at each of the locations, statewide, following would be the responsibilities of the SI:

(i) - The Selected SI shall be responsible for end-to-end implementation and shall quote and provide/supply; any items not included in the bill of materials but required for successful commissioning of the CCTNS project in the State, Meghalaya Police shall not pay for any such items, which have not been quoted by the Selected SI in their bid but are required for successful completion of the project.

(ii) - The selected SI would be responsible for delivering the equipments to all the respective locations.

(iii) - The Selected SI shall supply all the installation material/ accessories/ consumables (e.g. screws, clamps, fasteners, ties anchors, supports, grounding strips, wires etc.) necessary for the installation and commissioning of all the systems.

(iv) - The selected SI has to prepare and submit a state wide delivery report including details of components supplied in each office. The delivery report would be validated and sign-off would be provided by the Meghalaya Police/ Project Nodal Officer assisted by SPMC/ SPMU/ State Mission Team.

(v) - Bidder shall be responsible for taking care of any geography specific requirements.

(vi) - Selected SI shall be responsible for providing all the necessary support for undertaking the exercise of acceptance testing for IT Infrastructure provided at all the locations. Any equipment(s) found unaccepted by Meghalaya Police during acceptance testing shall be replaced by new accepted equipment(s) at no additional cost to Meghalaya Police.

(vii) - Selected SI shall be responsible for providing all the aforementioned infrastructure with a warrantee and AMC as mentioned in section 6.5, “Scope of Services - Post implementation”. All the system software/ COTS product provided as part of this project shall have full use perpetual enterprise edition in the name of Meghalaya Police.

Given below is an indicative format for Total quantity required for the Technical Bill of Materials for all Police locations (PHQ, Ranges, DHQ, SDPOs, SCRB, SCR/PCR, FPD, PS etc)

Item Description	Qty.
Client Systems (4 per PS)	294
HDD 320 GB – Serial ATA – 7200 rpm (min 150 Mbps data transfer rate)	39
Duplex Laser Printer (1 item)	39
Multi-Function Laser (Print/Scan/Copy)	164
2kVA UPS for 120min backup	79
10 kVA UPS for 120min backup	8
2 KVA Generator Set	39
16-Port Switch	79
24 -Port Switch	8
Fingerprint Reader	39
Digital Camera(1 item)	39

Item Description	Qty.
Electronic Pen(1 item)	39

Please refer volume II of the RFP for the details of the requirement as per various offices / Police Locations & Annexure X for Specification

6.3.9 Network and Connectivity for Police Stations, Higher Offices, Training Centers (DTC/RTC/PTC/Police Academy) for CCTNS project

The Networking solution of CCTNS project shall be based on a Hybrid Model which will consist of State Wide Area Network (SWAN) operated by State/UT under SWAN scheme and Data network operated by Bharat Sanchar Nigam Limited (BSNL) which consists of Point to point leased lines, VPNoBB, WiMax, VSAT and MPLS technologies. BSNL shall be providing the Networking & Connectivity services along with Operations & Maintenance for all the locations implemented by BSNL in that State/UT. BSNL shall also provide connectivity on MPLS VPN network for aggregated bandwidth at each State/UT SDC (State Data Center) for the locations connected on VPNoBB, WiMax and VSAT network and also provide connectivity for SDCs (State Data Centre) at State Head quarters (SHQs) to the National Data Centre (NDC) of NCRB. Further BSNL shall provide MPLS VPN network for connecting SDC and Disaster Recovery Centre (DRC) of the State/UT.

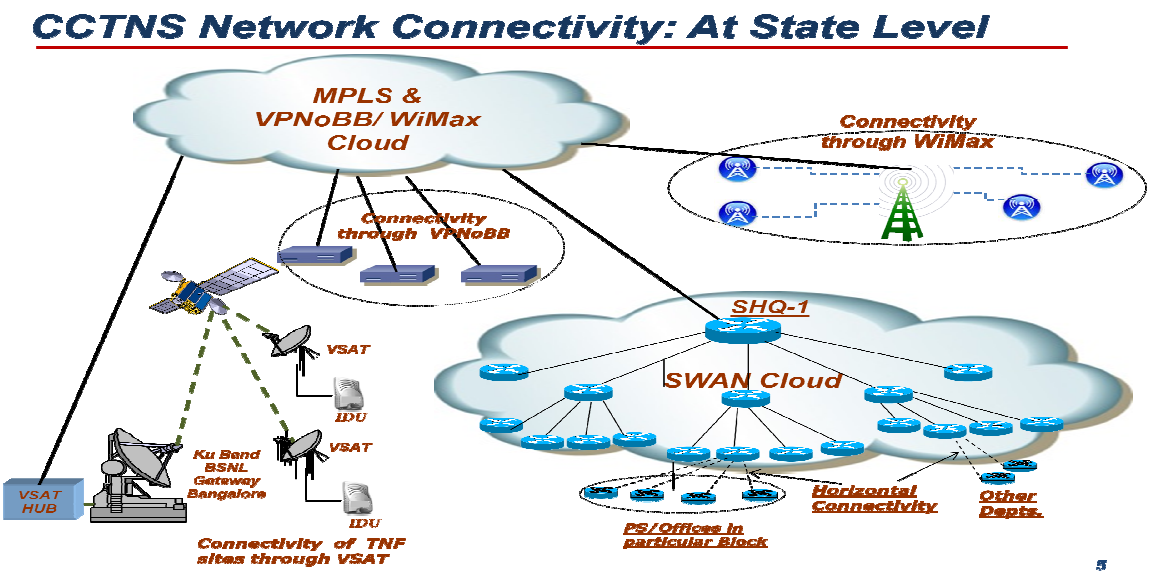
Scope of work for BSNL:

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

- Provisioning of 2Mbps Point to Point Lease Line (P2PLL) for locations to be connected with the nearest SWAN POP.
- Provisioning of WAN connectivity on VPNoBB/WiMax/VSAT for locations which are not feasible to be connected directly with the SWAN on P2PLL.
- 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.
- Provisioning of Aggregated bandwidth on MPLS network at each States/UTs SDC for the locations connected on VPNoBB, WiMax and VSAT network.
- Provisioning of MPLS connectivity between State/UT SDCs and DRC.
- Provisioning of MPLS connectivity between NDC and State/UT SDCs
- Maintaining the network including hardware supplied for minimum period of 3 years.

Network Deployment Architecture:

CCTNS is to be deployed on a centralized architecture wherein various offices of Police Department connect to the system through the Data Centre.



Role of System Integrator:

The SI shall coordinate with BSNL and the State/UT 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.

- Site preparation at all locations for establishment and installation of networking and connectivity solution.
- 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.
- Coordination with BSNL for ensuring Operations and Maintenance of networking hardware to ensure compliance to the SLAs as offered by BSNL.
- 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.
- The Police Stations and Higher Offices which are within the proximity of SWAN PoP (Point of Presence) will be connecting on LAN directly from SWAN PoP. The SI shall also coordinate with SWAN operator (Appointed under SWAN project) for Installation, Configuration, Testing and Commissioning of LAN connectivity for sites co-located within the SWAN PoP and LAN connectivity from SWAN NOC (Network Operation Centre) to the SDC. The SI shall be coordinating with SWAN operator for SLA Monitoring, Fault Reporting & Troubleshooting of the LAN links as per SWAN SLA.
- SI shall also coordinate with State CCTNS Nodal Officer (State Police Department) for finalizing Police stations lists for the connectivity options, issuing commissioning report for demand note/payment clearance, reporting SLA and providing for link status updates.

Note: The process of finalization for signing of contract with BSNL as Service provider for CCTNS project is in progress and detailed guidelines on implementation of Networking and Connectivity will be sent to all States.

Disaster Recovery Centre:

As per discussions with the State IT department that manages the SDC, the disaster recovery centre for the Meghalaya CCTNS Project would be located in the disaster recovery centre of the Meghalaya SDC. The DRC location would be finalized by the States and the SDCs of other States may be mutually considered as DRCs of each other.

6.3.10 Capacity building and Change Management

Capacity Building is a highly critical component of CCTNS. The objective of CCTNS Capacity Building (CB) initiatives is to empower the direct users and other stakeholders of CCTNS to optimally use CCTNS and enhance outcomes in crime investigation, criminals tracking and other core police functions; and also ensure a smooth functioning of CCTNS.

Building capacities at various levels is critical to the successful implementation of the recommended IT initiatives. The break-up of the police force in the State of Meghalaya is provided below:

Break up of Police Personnel in the Meghalaya	
Group	No. of personnel
Group A - Senior Police officers	**128**
Group B - officers of Inspectors, SIs and ASIs rank	**1213**
Group C - All Head Constables, Constables and clerks	**9992**
Total	**11333**

Identification of Trainers (Internal)

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

Identification of Trainers (Police Training Colleges)

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

Identification of Trainees

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

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

- **Group II:** Identify the key officers **(IG, DIG, 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.
  - Role-based training will be carried out for these officers at suitable location in the State Headquarters and respective Districts by the System Integrator -
  -
- **Group III:** Identify the key officers **(SHO, SI, ASI,)** in the Police Stations and Higher Offices who will use CCTNS for police station management, filing the necessary investigation forms, and utilize the basic and advance search features of CCTNS to facilitate their investigation process.
  - *In addition to the computer awareness training, role-based training will be carried out for these officers at District Training Centers in the respective Districts (if any) by the System Integrator*
  - *Refresher training can be carried out by the internal trainers subsequent to the System Integrator trainings*

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

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

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

The SI holds the responsibility for creation of training material, designing the training programs and their delivery to the target group. The State 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 *Meghalaya Police/SPMU* covering the training strategy, environment, training need analysis and role

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

Develop Training Material

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

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

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 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.

Number of Personnel to be trained on various Modules

Indicative number of people to be trained on various modules is as provided below:

S. No.	Module description	Number of Personnel to be trained
1	Awareness and sensitization of benefits of IT	288
2	Basic Computer Awareness & Role based training for application users	5128
3	Trainers Training	85
4	System Administration and support Training	460

Note: The indicative number is based on the initial assessment of training requirement and is provided to bidders to assess their efforts requirement while responding to RFP. Meghalaya Police reserves the right to change the training requirements and the number of people to be trained for each training category.

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 specialized training should also be able to provide the participant a clear comparison between the old way of crime and criminal investigation against the post CCTNS scenario. This training needs to be conducted by the SI at the very end when all the other trainings are successfully completed. This training may seem similar to role play training mentioned in the section above however, in this simulated training, the SI would ensure that the IO's are provided an environment that would be exactly similar at a Police Station post CAS (State) implementation.

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

An ILT course will have the following components:

- Course Presentation (PowerPoint)
- Instruction Démonstrations (CAS - Application training environment)
- Hands-on Exercices (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.

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

The State Nodal Agency shall form various stakeholder groups to address the Change Management Initiative. Stakeholders are all those who need to be considered in achieving project goals and whose participation and support are crucial to its success. A key individual stakeholder or

stakeholder group is a person or group of people with significant involvement and/or interest in the success of the project. Stakeholder analysis identifies all primary and secondary stakeholders who have an interest in the issues with which the CCTNS project is concerned. The stakeholder groups will be the set of core users (Change Agents) who will directly participate in the awareness and communication initiatives, workshops, and provide feedback to the District and State Mission Teams.

Change management

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

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

Communication and Awareness

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

S NO.	Activities	Detail	Frequency
1	Develop detailed communication plan	• SI shall prepare a detailed communication plan for the program in line with the implementation timelines of	Once

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

Change Management Workshops

SI shall conduct Change Management workshops build appreciation of change management and develop change leadership across the stakeholder groups. SI shall design the necessary content (reading material, presentations) in English and 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) at all the Districts (at the District Headquarters) covering at least 3 officers/constables (SHO, SI/ASI/HC, and Station Writer) from each police station in the district.
The SI is required to conduct the Change Management Workshops for all the identified Police personnel in a phased manner in line with the overall implementation plan. These workshops shall be conducted at the locations provided by the State. The workshop content & material shall be designed with specific focus on the requirements of the personnel. SI shall conduct workshops for each group of personnel in sync with the training plan and as part of the training module. SI is required to provide the necessary material for the workshops including presentations, training

material etc in both soft and hard copy formats.

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

6.3.11 Handholding Support for end users

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

Handholding and project support would be required only after the successful commissioning of Core Application (CAS) and the necessary infrastructure and completion of capacity building and change management initiatives in respective locations. Information of all Police locations regarding engagement of handholding personnel has been provided in Geographical scope in this RFP.

Eligibility Criteria for Handholding staff

Handholding Staff	
Qualification & Experience	• B.E/ B. Tech/ MCA/ BCA/ PGDCA/ M.Sc./ B Sc/ Diploma • 2+ years of experience in Application Software/LAN/WAN/PC troubleshooting • Working proficiency on office suite • Good communication skills and proficient in English language (Local language like Khasi/Garo desirable)
Location	Police Stations
Minimum manpower	39 (1 per Police station)
Service Window	9 x 6

Code of Conduct of Handholding personnel as Police Stations:

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

6.3.12 Requirement on Adherence to Standards

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

Compliance with Industry Standards

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

Portal development	W3C specifications
Information access/transfer protocols	SOAP, HTTP/HTTPS
Interoperability	Web Services, Open standards

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

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

6.3.13 Support to 3rd Party/ User 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, Test cases and Requirements Mapping review
2. Infrastructure Compliance Review.
3. Availability of Services in the defined locations.
4. Performance and Scalability.
5. Security.
6. Manageability and Interoperability.
7. SLA Reporting System.
8. Project Documentation.
9. Data Quality Review

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

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

2. Infrastructure Compliance Review:

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

3. Security Review:

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

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

4. Performance:

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

5. Availability:

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

6. Manageability Review:

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

7. SLA Reporting System:

SI shall design, implement/customize the Enterprise Management System (EMS) and shall develop any additional tools required to monitor the performance indicators listed under SLA Prescribed in this RFP. The Acceptance Testing & Certification agency shall verify the accuracy and completeness of the information captured by the SLA monitoring system implemented by the SI and shall certify the same.

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

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

Note: SI shall provide requisite support and coordinate with the Meghalaya Police for Audit, User acceptance and Certification**.**

6.4 Scope of Services - Post-Implementation Phase / Operate and Maintain Phase

The SI shall be responsible for the overall management of the system including the application and entire related IT Infrastructure. SI shall develop / procure and deploy an EMS tool that monitors / manages the entire enterprise wide application, infrastructure and network related components.

SI shall provide the Operations and Maintenance Services for period of five years following the deployment and "Go-Live" of the solution in the State. Since Phase I locations will be declared Go-Live earlier, the Operations and Maintenance Services for these locations for a period of five years will start immediately and for the phase II locations, The Operations and Maintenance Services for a period of five years will start after the Go-Live of Phase II locations.

*(**Note:** Though the requirement for operation and maintain phase is for 5 years, Meghalaya Police reserves the right to provide work order only for initial 3 years and make the payments accordingly. Further Meghalaya police may extend the support requirement by 2 years with the same SI or may involve any other agency as per the requirements of the state)*

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

1. **Warranty support**
2. **Annual Technical Support (ATS)**
3. **Handholding Services**

The services shall be rendered onsite from the State designated premises. To provide the support for the police stations, sub-divisional offices, district headquarters, ranges, zones, State police headquarters and other locations across the State, where the software, hardware, and other infrastructure will be rolled out, SI is expected to provide experienced and skilled personnel at each location. The SI will also ensure that there is a **Service Center available or setup** at each district or a group of districts of the State, as per mutual understanding between State and the SI.

6.4.1 Warranty support

As part of the warranty services SI shall provide:

1. - SI shall provide a comprehensive warranty and on-site free service warranty for 5 years from the date of Go Live.
2. - SI shall obtain the five year product warranty and five year onsite free service warranty on all licensed software, computer hardware and peripherals, networking equipments and other equipment.
3. - SI shall provide the comprehensive manufacturer's warranty in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. covered by the RFP. SI must warrant all hardware, equipment, accessories, spare parts, software etc. procured and implemented as per this RFP against any manufacturing defects during the warranty period.
4. - SI shall provide the performance warranty in respect of performance of the installed hardware and software to meet the performance requirements and service levels in the RFP.
5. - SI is responsible for sizing and procuring the necessary hardware and software licenses as per the performance requirements provided in the RFP. During the warranty period SI shall replace or augment or procure higher-level new equipment or additional licenses at no additional cost to the State in case the procured hardware or software is not adequate to meet the service levels.
6. - Mean Time between Failures (MTBF) If during contract period, any equipment has a hardware failure on four or more occasions in a period of less than three months or six times in a period of less than twelve months, it shall be replaced by equivalent or higher-level new equipment by the SI at no cost to State. However, if the new equipment supplied is priced lower than the price at which the original item was supplied, the differential cost should be refunded to State. For any delay in making available the replacement and repaired equipments for inspection, delivery of equipments or for commissioning of the systems or for acceptance tests / checks on per site basis, State reserve the right to charge a penalty.
7. - During the warranty period SI shall maintain the systems and repair / replace at the installed site, at no charge to State, all defective components that are brought to the SI's notice.
8. - The SI shall as far as possible repair the equipment at site.
9. - In case any hard disk drive of any server, SAN, or client machine is replaced during warranty
10. / AMC the unserviceable HDD will be property of State and will not be returned to SI.
11. Warranty should not become void, if State buys, any other supplemental hardware from a third party and installs it within these machines under intimation to the SI. However, the warranty will not apply to such supplemental hardware items installed.
12. 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.
13. 1SI shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.
14. The SI shall ensure that the warranty complies with the agreed Technical Standards, Security
15. Requirements, Operating Procedures, and Recovery Procedures.
16. 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.
17. 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).
18. The SI shall develop and maintain an inventory database to include the registered hardware warranties.

6.4.2 Annual Technical Support (ATS)

As part of the ATS services SI shall provide:

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

6.4.3 Handholding Services

Handholding services will include the following:

a. - **Operations and maintenance services at the Data Center and Disaster Recovery Center** for the server and related infrastructure supplied and commissioned by the SI for the application.
b. - **Central Helpdesk** from the State designated premises.
c. - **Support for the end users as provided in section 6.3.11**
d. - **Software maintenance and support services.**
e. - **Application functional support services**

Operations and maintenance services for the server and related infrastructure

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

The scope of the services for overall IT infrastructure management as per ITIL framework shall include 365x24x7 on site Monitoring, Maintenance and Management of the server and related infrastructure supplied and commissioned by the SI for the application at the Data Center and Disaster Recovery Center. The business hours in State will be from 0830 hours to 2030 hours on all days (Mon-Sun). SI will plan these services accordingly. The SI shall provide the MIS reports for all the devices installed in the Data Center and Disaster Recovery Center in format and media as mutually agreed with the State on a monthly basis. Whenever required by State, SI should be able to provide additional reports in a pre-specified format. The indicative services as part of this support are as below:

(a) -System Administration, Maintenance & Management Services
(b) -Application Monitoring Services
(c) -Network Management Services
(d) -Backend Services (Mail, messaging, etc)
(e) -Storage Administration and Management Services
(f) - IT Security Administration Services and Services for ISO 27001 and ISO 20000 compliance
(g) -Backup and Restore Services

Note:

Eligibility Criteria for manpower requirements

Handholding Staff	
Qualification & Experience	• B.E/ B. Tech/ MCA/ BCA/ PGDCA/ M.Sc./ B Sc • 2+ years of experience in Application Maintenance, Database Maintenance, Data Centre Maintenance • Working proficiency on office suite • Good communication skills and proficient in English language (Local language desirable)
Location	SDC
Manpower requirement	The minimum indicative manpower requirements at data center for operation and maintenance services for the server and related infrastructure are 2 nos. × 3 shift for 3 Years i.e 216 Man Months. Bidders to propose adequate manpower as per the indicative requirement and in order to meet the associated SLAs as provided Annexure II

Central Helpdesk

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

1. - The service will be provided in the local language of the State.
2. - The help desk service that will serve as a single point of contact for all ICT related incidents and service requests. The service will provide a Single Point of Contact (SPOC) and also resolution of incidents. State requires the SI to provide Help Desk services to track and route requests for service and to assist end users in answering questions and resolving problems related to the software application, network, Data Center, Disaster Recovery Center, Client side infrastructure, and operating systems at all locations. It becomes the central

collection point for contact and control of the problem, change, and service management processes. This includes both incident management and service request management.

3. - SI shall provide a second level of support for application and technical support at police stations, circle offices, sub-divisional offices, district headquarters, range offices, state police headquarters and other locations across the State where the software, hardware, and other infrastructure will be rolled out.
4. - For all the services of State within the scope of this RFP, SI shall provide the following integrated customer support and help.
5. - Establish 12X6 Help Desk facility for reporting issues/ problems with the software, hardware and other infrastructure.
6. - SI shall maintain and support to all client side infrastructure including hardware, networking components, and other peripherals.
7. - SI shall provide maintenance of Hardware, including preventive, scheduled and predictive Hardware support, as well as repair and / or replacement activity after a problem has occurred.
8. - SI shall track and report observed Mean Time Between Failures (MTBF) for Hardware.
9. - SI shall provide functional support on the application components to the end users.
10. SI shall also provide system administration, maintenance and management services, LAN management services, and IT security administration services.

Software maintenance and support services

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

1. - The Software Maintenance and Support Services shall be provided for all software procured and implemented by the SI. The SI shall render both on-site and off-site maintenance and support services to State to all the designated locations. The Maintenance and Support Services will cover, all product upgrades, modifications, and enhancements.
2. - Updates/Upgrades/New releases/New versions. The SI will implement from time to time the Updates/Upgrades/New releases/New versions of the software and operating systems as required after necessary approvals from State about the same.
3. - Tuning of application, databases, third party software's and any other components provided as part of the solution to optimize the performance.
4. - The SI shall apply regular patches to the licensed software including the operating system and databases as released by the OEMs.
5. - Software Distribution. SI shall formulate a distribution plan prior to rollout and distribute/install the configured and tested software as per the plan.
6. - Software License Management. The SI shall provide for software license management and control. SI shall maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements, and maintenance. SI should perform periodic audits to measure license compliance against the number of valid End User software licenses consistent with the terms and conditions of site license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions and report to State / UT on any exceptions to SI terms and conditions, to the extent such exceptions are discovered.
7. - The SI shall undertake regular preventive maintenance of the licensed software.

Application functional support services

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

1. - The Application Functional Support Services shall be provided for all software procured and implemented by the SI. The SI shall render both on-site maintenance and support services to State from the development center in State.
2. - Enhancements and defect fixes. SI shall incorporate technological changes, and provide enhancements as per the requests made by State. SI shall perform minor changes, bug fixes, error resolutions and minor enhancements that are incidental to proper and complete working of the application.
3. - Routine functional changes that include user and access management, creating new report formats, and configuration of reports.
4. - 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.
5. - The SI shall migrate all current functionality to the new / enhanced version at no additional cost to State and any future upgrades, modifications or enhancements.
6. - The SI shall perform user ID and group management services.
7. - The SI shall maintain access controls to protect and limit access to the authorized End Users of the State.
8. - The services shall include administrative support for user registration, creating and maintaining user profiles, granting user access and authorization, providing ongoing user password support, announcing and providing networking services for users and providing administrative support for print, file, directory and e-mail servers.

Note: Bidders to propose adequate manpower for meeting the operation and maintenance requirements as identified above and in line with associated SLAs as provided Annexure II

Exit Management and Transition – Capacity Building at State

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

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

7 IMPLEMENTATION AND ROLL-OUT PLAN

7.1 Indicative Activity-wise Implementation and Project Roll-Out Plan:

S. 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 Meghalaya 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	T + 8 Weeks
3.	Detailed assessment of functional requirements and MIS requirements		
4.	Finalization/ Vetting of FRS	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	
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 Meghalaya Police and incorporating all the functional specifications, standards provided by the NCRB, Meghalaya Police specific requirements and different integration points with CAS (Centre), external agencies and other applications of Meghalaya Police x. List of additional features proposed in complete CCTNS	

S. No.	Project Activity	Deliverables	Timelines (T from date of signing of contract)
		Application xi. CAS (State) Implementation document w.r.t. Configuration, Customization, Extension and Integration as per Meghalaya Police's requirements	
6.	Procurement of IT infrastructure at Data Centre and DR		T + 8 Weeks
7.	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/ GoS xv. CCTNS Application Test Plans and Test Cases	T + 10 Weeks
8.	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
9.	IT infrastructure sizing	xvii. Final BoM with Technical specifications for the IT Hardware, Network and other IT Infrastructure Requirements xviii. Strategy for Data Centre and DR Site xix. Report on the reusability of existing infrastructure	T + 11 Weeks

S. No.	Project Activity	Deliverables	Timelines (T from date of signing of contract)
		xx. Hardware procurement & Deployment plan	
10.	Others	xxi. Data Migration Strategy and Methodology	T+11 Weeks
11.	Commissioning and operationalization of IT infrastructure at Data Centre and DR		T + 11 Weeks
Implement (This shall only begin after CAS (State)[14] has been received from NCRB, MHA) – T1			
12.	Study and analyze the CAS (State) system as received from NCRB against the requirements of Meghalaya Police and conduct Closed Room Pilot (CRP) based on the requirement specifications	xxii. Feedback Report based on CRP I and CRP II	T1 + 4 Weeks
13.	Finalization of requirement specifications	xxiii. Final FRS, SyRS, SRS and other requirements with all the Solution Design documents	T1 + 6 Weeks
14.	Configuration & Customization of CAS (State) and development of additional modules		T1 + 14 Weeks
15.	Integration with CAS (Centre)		T1+ 14 Weeks
16.	Data migration and digitization of historical data		T1 + 14 Weeks
17.	Migration of CIPA and CCIS Police Stations/ non-CIPA and CCIS Police Stations/ Higher Offices to CCTNS		T1 + 15 Weeks
18.	Testing of configured & deployed solution (CAS) and additional functionalities		T1 + 16 Weeks
19.	Site preparation at Pilot Phase Client site locations		T1 + 18 Weeks
20.	Procurement, Commissioning and Operationalizing the IT infrastructure at Pilot phase Police locations		T1 + 20 Weeks
21.	User Acceptance and Testing of Pilot Phase implementation		T1 + 20 Weeks

[14] As per the guidelines of CCTNS MMP, Core Application Software (State) would be provided by NCRB.

S. No.	Project Activity	Deliverables	Timelines (T from date of signing of contract)
22.	User Training on Pilot Phase CCTNS Solution		T1 + 22 Weeks
23.	Pilot rollout (Phase I)	xxiv. Report on amendments / enhancements / modifications made based on inputs of Meghalaya Police	T1 + 22 Weeks
24.	Go-Live of Pilot	xxv. Pilot phase Acceptance from Meghalaya Police	T1 + 24Weeks
25.	Improvement of application according to the experience of Phase I	xxvi. Pilot phase Go-Live Report including a. Site Preparation and Infrastructure Deployment / Commissioning Report for Pilot Sites, Data Centre and DR Site b. Data Migration report for Pilot phase c. Performance and Load Testing Report for Pilot phase	T1 + 24 Weeks
26.	Handholding services at each Police Station for the End users for the Phase I site locations		6 months from the day of Go-live of Phase I
27.	CCTNS Solution customization for Phase II and integrating with external agencies		T1 + 32 Weeks
28.	Site preparation at Phase II Client locations		T1 + 42 Weeks
29.	Procurement, Commissioning and Operationalizing of IT infrastructure at Phase II Client locations		T1 + 42 Weeks
30.	Capacity Building and Change Management		T1+ 44 Weeks
31.	User Training on complete CCTNS Solution		T1 + 44 Weeks
32.	State wide rollout of Phase II	xxvii. Report on amendments / enhancements / modifications made based on inputs of Meghalaya Police / Third Party's Acceptance Testing for State-wide Roll-Out	T1 + 45 Weeks
33.	Handholding services at each Police Station for the End users for the Phase I site locations		6 months from the day of Go-live of Phase II
34.	3rd party Acceptance testing, audit and certification of complete CCTNS Solution	xxviii. Third Party Acceptance Testing Certificate	T1 + 48 Weeks
35.	SLA and Performance Monitoring Plan	xxix. Detailed plan for monitoring of SLAs and performance of the overall system	Before "Go-Live"

S. No.	Project Activity	Deliverables	Timelines (T from date of signing of contract)
36.	Help desk setup	xxx. Operational helpdesk	
37.	Go-Live for complete CCTNS Solution	xxxi. Go-Live Acceptance from Meghalaya Police xxxii. 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**
1.	Project Operation and Maintenance	xxxiii. Fortnightly Progress Report on Project including SLA Monitoring Report and Exception Report xxxiv. Project Quality Assurance report xxxv. Details on all the issues logged	**5 Years from the date of "Go-Live" of Complete CCTNS Solution**

7.2 Detailed Implementation and Roll-out Plan

SI shall prepare a detailed roll-out plan for each of the Districts in the Phase and get the same approved by the Meghalaya Police. SI is also responsible for conducting workshops for the key officers (State Mission Team, District Mission Team, and District Core Team) of the Districts / State for presenting the District-Wise roll-out plan and get the approval from the District Teams before getting the final approval of the State Nodal Officer. The SI shall also provide the necessary assistance for the key officers (State Mission Team, District Mission Team, and District Core Team) of the Districts / State during the design and implementation of CCTNS in the Meghalaya Police. A detailed rollout checklist should be maintained for migrating application to production as well as for location readiness.

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

8 SERVICE LEVELS

The SI shall monitor and maintain the stated service levels to provide quality service to Meghalaya Police. The Service levels are provided in Annexure-II of this RFP.

ANNEXURE I: DETAILS OF TECHNOLOGY STACKS - CAS(STATE) AND CAS (CENTRE)

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

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

CAS (State) Solution - Stack 1

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

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

CAS (State) Solution - Stack 2

	Proposed Solution by Software Development Agency	Version and Year of Release	Original Supplier	Description (include major features/ services only)	Support to be Provided By
Webserver	IIS	6	Microsoft	Web & App Server	Microsoft
Application Server	IIS	6	Microsoft	Web & App Server	Microsoft
Database Management System	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

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

CAS (State) Offline Solution

The below list is indicative only	Proposed Solution by Software Development Agency	Version and Year of Release	Original Supplier	Description (include major features/ services only)	Support Provided By
Synchronization Solution	Custom Built	N/a	N/a	N/a	N/a
Application Container	Apache Tomcat	6.0	Apache Foundation	J2EE Application Container	
Database Management System	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 Year of Release	Original Supplier	Description (include major features/ services only)	Support Provided By
Webserver	Sun Java System Web Server 7.0	7.0	SUN	HTTP Server	SUN
Application Server	Glassfish Application Server	3.0	SUN	J2EE Application Server	SUN
Database	Sybase IQ Enterprise	15.1	Sybase	ETL	Sybase
Operating System	Solaris				
Others					
Reporting Engine	Jasper Reports	3.7	Jasper	Reporting Services	
Search Engine	Search: Unstructure data: using Alfresco search features Structured Data: Sybase DB Search Engine & Custom application interface	N/a	N/a	N/a	N/a
Portal Server	Glassfish Application Server	7.0	SUN	HTTP Server	SUN
Workflow Engine	jBPM	4.0	JBoss	Workflow engine	
Rules Engine	Custom Built	N/a	N/a	N/a	N/a
Directory Services	Sun Directory Services	7.0	SUN	LDAP	SUN
DMS/CMS	Alfresco				
Email/Messaging	N/A				
Security	Physical Security, Network Sercurity, DB Encryption (MySQL), DB Access Controls, Role Based Access Control (Custom Developed), LDAP (Sun Directory Services),	N/a	N/a	N/a	N/a
Identity Management	Open SSO	7.0	SUN	LDAP	SUN

The below list is indicative only	Proposed Solution by Software Development Agency	Version and Year of Release	Original Supplier	Description (include major features/ services only)	Support Provided By
Audit	log4j, Custom Built	N/a	N/a	N/a	N/a
ETL + Data Quality	Sybase ETL	15.1	Sybase	ETL	Sybase

ANNEXURE II: SERVICE LEVELS

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

2. Definitions.

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

(b) -**"Scheduled operation time"** means the scheduled operating hours of the System for the month. All scheduled maintenance time on the system would be deducted from the total operation time for the month to give the scheduled operation time. The total operation time for the systems and applications within the Primary DC, DRC and critical client site infrastructure will be 24X7X365. The total operation time for the client site systems shall be 18 hours.

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

(d) -**"Availability"** means the time for which the services and facilities are available for conducting operations on the Meghalaya Police system including application and associated infrastructure. Availability is defined as:

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

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

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

(g) -**" Error"** in data digitization or data migration exercise, refers to the mistakes made intentional/ unintentional by SI which may or may not change the actual meaning of the subject.

3. Interpretations.

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

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

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

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

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

(f) - The SLA parameters shall be monitored on a monthly basis as per the individual SLA parameter requirements. However, if the performance of the system/services is degraded significantly at any given point in time during the contract and if the immediate measures are not implemented and issues are not rectified to the complete satisfaction of the Meghalaya Police or an agency designated by them, then the Meghalaya Police will have the right to take appropriate disciplinary actions including termination of the contract.

(g) -A Service Level violation will occur if the SI fails to meet Minimum Service Levels, as measured on a half yearly basis, for a particular Service Level. Overall Availability and Performance Measurements will be on a monthly basis for the purpose of Service Level reporting. An “Availability and Performance Report” will be provided by the SI on monthly basis in the Meghalaya Police suggested format and a review shall be conducted based on this report. A monthly Availability and Performance Report shall be provided to the Meghalaya Police 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 Meghalaya Police upon review and signoff by both SI and the Meghalaya Police. 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 Meghalaya Police 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 Meghalaya Police and will be performed by the Meghalaya Police or the Meghalaya Police 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 Meghalaya Police on a monthly basis. The tool should also be capable of generating SLA reports for a half-year. Meghalaya Police will audit the tool and the scripts on a regular basis. SPMC shall assess the EMS requirements and include the same in the RFP.

(j) - The Post Implementation SLAs will prevail from the start of the Operations and Maintenance Phase. However, SLAs will be subject to being redefined, to the extent necessitated by field

experience at the police stations / higher offices and the developments of technology practices globally. The SLAs may be reviewed on an annual/bi-annual basis as the Meghalaya Police decides after taking the advice of the SI and other agencies. All the changes would be made by the Meghalaya Police in consultation with the SI.

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

(l) - Following tables outlines the key service level requirements for the system, which needs be ensured by the SI during the operations and maintenance period. These requirements shall be strictly imposed and either the Meghalaya Police 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	All the trainees within each of the training program should pass the training exam with more than 80% or more marks conducted after their training Severity of Violation: High This service level will be monitored and measured on a per District basis through online examination of each trainee and their result 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/ Digitization	Error rate in a batch should be less than 0.5%. Severity of Violation: High 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.

Delivery Related Service Level Agreement (SLA) Criteria								
Explanation: The deduction mentioned in this table shall be made from the next due payment to the vendor for services provided on Statewide basis.								
S. No.	**Service Metrics Parameters**	**Baseline**	**Lower Performance**		**Violation of Service level agreement**		**Basis of Measurement**	**Remarks**
		Metric	**Metric**	**Deduction**	**Metric**	**Deduction**		
1	Delivery of the reports/ deliverables due for this section	As per the dates as mentioned in the contract	One week after the due date	Rs. 10,000	>1 week after the due date	Rs. 20,000 for every week of delay	Dates for delivery of reports as mentioned in the contract	
2	Development, deployment and testing of CAS (State) application	5.0 months from date of signing of contract	5-7 months	100,000 Rupees	More than 7 months	Rs. 1,00,000 per month of delay	Months taken after beginning of the assignment to develop and test the application at the Data center by the Operator, not including the software audit by TPA	The centralized application should be tested for desired functionalities, security, and completeness as well as compliance with SLA, within the period
	Supply, installation and Commissioning of hardware at offices	3 months	3-4 months	For non-compliance at each point of deployment: Rs. 30,000	> 4 months	For non-compliance at each point of deployment: Rs. 45,000	Months after taking over of the office site for project	The deduction shall be made per site basis, where criterion is not satisfied
	Supply, installation and Commissioning of	6 months from the date of signing of	6-7 months	Rs. 100,000	More than 7 months	Rs. 100,000 for every month of delay	Months taken after beginning of the	Meghalaya Police may conduct

Delivery Related Service Level Agreement (SLA) Criteria								
Explanation: The deduction mentioned in this table shall be made from the next due payment to the vendor for services provided on Statewide basis.								
S. No.	**Service Metrics Parameters**	**Baseline**	**Lower Performance**		**Violation of Service level agreement**		**Basis of Measurement**	**Remarks**
		Metric	**Metric**	**Deduction**	**Metric**	**Deduction**		
	the Data Center Equipment	contract					assignment	independent audit to verify that the data center is as per the specifications.
	Capacity building	All the trainees should pass the online training exam with more than 80% marks	Less than 80% and more than 60% marks	Rs. 1500 / trainee/ training program	Less than 60% marks	Rs. 3000 per trainee/ training program	Results from Online examination test post training course	The feedback of the attendees must be taken after every training session/ program and this feedback should be leveraged for improving the capacity building program
	Data Digitization	Error rate in a batch should be less than 0.5%.	High impacting error: if the error rate is between 0.5% to 1%	5% of the Payment due for Data Digitization	if the error rate is above 1%	10% of the Payment due for Data Digitization	This service level will be measured on a monthly basis for each Police Station / Higher Office	Error rate is measured by percentage of the records with corrections marked by designated officials

Delivery Related Service Level Agreement (SLA) Criteria								
Explanation: The deduction mentioned in this table shall be made from the next due payment to the vendor for services provided on Statewide basis.								
S. No.	**Service Metrics Parameters**	**Baseline**	**Lower Performance**		**Violation of Service level agreement**		**Basis of Measurement**	**Remarks**
		Metric	**Metric**	**Deduction**	**Metric**	**Deduction**		
	Maintenance phase	All the issues reported regarding hardware, software etc. should be resolved within 24 hours (within 1 working day)	Resolution of issues within 2 working days of reporting	Rs. 500	Resolution of the issue after 2 working days	Rs. 1000 for every day delay over and above beyond	Time and date of reporting of the issue	
	The above list of Service levels is indicative. The Meghalaya Police should add more service levels / modify the above service levels as per their requirements							

3. Violations and Associated Penalties

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

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

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

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

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

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

Post Implementation Phase SLAs

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

(a) **Production CAS Systems**. The failure or disruption has a direct impact on the Meghalaya Police's ability to service its police stations / higher offices, ability to perform critical back-office functions or a direct impact on the organization. This includes but not limited to:-

(i) Storage and related switches at Primary DC and DRC.
(ii) Web, Application, Database, and Backup Servers at Primary DC and DRC.
(iii) Primary DC to DRC connectivity.
(iv) Primary DC and DRC network infrastructure.
(v) Primary DC and DRC security infrastructure.

(b) **Non-CAS Systems in Production and Non Production Systems (Development, QA, and Training)**. The failure or disruption has no direct impact on the Meghalaya Police's ability to serve its police stations / higher offices, or perform critical back-office functions.

(vi) Production Non CAS Servers.
(vii) Test, QA and Training Servers.
(viii) Helpdesk infrastructure & applications.
(ix) EMS Infrastructure.

(c) **CAS Solution Components**. The failure or disruption has a direct impact on the Meghalaya Police's ability to service its police stations / higher offices, ability to perform critical back-office functions or a direct impact on the organization.

(d) **Non ERP Solution Components**. The failure or disruption has no direct impact on the Meghalaya Police's ability to serve its police stations / higher offices, or perform critical back-office functions.

(e) These service levels will be monitored on a monthly basis.

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

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

Severity of Violation: High
<table><tr><td>Availability over the six-month period</td><td>Violations for calculation of penalty</td></tr><tr><td>< 99% & >= 98.5%</td><td>1</td></tr><tr><td>< 98.5% & >= 98%</td><td>2</td></tr><tr><td>< 98%</td><td>3</td></tr></table>
In addition to the above, if the service level in any month in the six-month period falls below 98%, one (1) additional violation will be added for each % drop for each such month to the overall violations for this service level.</td></tr>
<tr><td>Infrastructure Availability</td><td>Availability of non-CAS systems in production and non-production systems shall be at least 97%.

Severity of Violation: Medium
<table><tr><td>Availability over the six-month period</td><td>Violations for calculation of penalty</td></tr></table></td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>
<table>
<tr><td>< 97% & >= 96.5%</td><td>1</td></tr>
<tr><td>< 96.5% & >= 96%</td><td>2</td></tr>
<tr><td>< 96%</td><td>3</td></tr>
</table>
In addition to the above, if the service level in any month in the six-month period falls below 96%, one (1) additional violation will be added for each % drop for each such month to the overall violations for this service level.
</td></tr>
<tr><td>Infrastructure Availability</td><td>RTO shall be less than or equal to six (6) hours.

Severity of Violation: High

Each instance of non-meeting this service level will be treated as one (1) violation.</td></tr>
<tr><td>Infrastructure Availability</td><td>RPO (zero data loss in case of failure of Primary DC) should be zero minutes

Severity of Violation: High

Each instance of non-meeting this service level will be treated as two (2) violations.</td></tr>
<tr><td>Infrastructure Performance</td><td>Sustained period of peak CPU utilization of any server crossing 70% (with the exception of batch processing) shall be less than or equal to 30 minutes.

Severity of Violation: High

Each occurrence where the peak CPU utilization of any server crosses 70% (with the exception of batch processing) and stays above 70% for time more than 30 minutes will be treated as one (1) instance.
<table>
<tr><td>Number of instances over the six month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>>0 & <=3</td><td>1</td></tr>
<tr><td>> 3</td><td>2</td></tr>
</table>
In addition to the above, if the number of instances in any month in the six-month period exceeds 3, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Infrastructure Performance</td><td>Sustained period of peak I/O utilization of any server crossing 70% (with the exception of batch processing) shall be less than or equal to 30 minutes.

Severity of Violation: High

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

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

Severity of Violation: High

Each occurrence where the peak memory utilization of any server crosses 70% (with the exception of batch processing) and stays above 70% for time more than 30 minutes will be treated as one (1) instance.
<table>
<tr><td>Number of instances over the six month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>>0 & <=3</td><td>1</td></tr>
<tr><td>> 3</td><td>2</td></tr>
</table>
In addition to the above, if the number of instances in any month in the six-month period exceeds 3, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Application Availability</td><td>Availability of CAS solution components measured within the Data Center shall be at least 98%

Severity of Violation: High

This service level will be monitored on a monthly basis.
<table>
<tr><td>Availability over the six-month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>< 98% & >= 96%</td><td>1</td></tr>
<tr><td>< 96% & >= 94%</td><td>2</td></tr>
<tr><td>< 94%</td><td>3</td></tr>
</table>
In addition to the above, if the service level in any month in the six-month period falls below 99%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Application Availability</td><td>Availability of non-CAS solution components measured within the Data Center shall be at least 97%

Severity of Violation: Medium

This service level will be monitored on a monthly basis.
<table>
<tr><td>Availability over the six-month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>< 97% & >= 96%</td><td>1</td></tr>
<tr><td>< 96%</td><td>2</td></tr>
</table>
In addition to the above, if the service level in any month in the six-month period falls below 96%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td></td></tr>
<tr><td>Application Performance</td><td>Average application response time during peak usage hours as measured from a client terminal within the Data Center shall not exceed 4 seconds.

Severity of Violation: High

The list of critical business functions and peak usage hours will be identified by the Meghalaya Police during the Supply and System Integration Phase.

This service level will be monitored on a monthly basis.
<table>
<tr><td>Average application response time over the six-month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>> 4s & <= 5s</td><td>2</td></tr>
<tr><td>> 5s & <= 6s</td><td>4</td></tr>
<tr><td>> 6s</td><td>5</td></tr>
</table>
In addition to the above, if the average turnaround time in any month in the six-month period goes beyond 6s, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
</table>

2. <u>Client Site Infrastructure Systems</u>

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

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

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

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

3. Handholding Support: Client Site Support

(a) - **Level 1 Incidents**. The incident has an immediate impact on the Meghalaya Police'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 Meghalaya Police's ability to service its police stations / higher offices that while not immediate, can cause service to degrade if not resolved within reasonable time frames

(c) - The severity of the individual incidents will be mutually determined by the Meghalaya Police and SI.

(d) - The scheduled operation time for the client site systems shall be the business hours of the Meghalaya Police.

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

(f) - The tables on the following page give details of the Service Levels the SI is required to maintain.

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td>Client Site Support Performance -</td><td>80% of the Level 1 Incidents at each site should be resolved within 2 business hours from the time call is received / logged which ever is earlier. The maximum resolution time for any incident of this nature shall not exceed 8 business hours.

Severity of Violation: Medium

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

If the performance in a month for an implementation site falls below the minimum service level, it will be treated as one (1) instance. The total number of instances for the six-month period will be the cumulative number of instances across all the months across all sites in the six-month period.

Average number of instances per month = (Total number of instances for the six-month period) / 6
<table>
<tr><th>Average number of instances per month</th><th>Violations for calculation of penalty</th></tr>
<tr><td>>0 & <=4</td><td>1</td></tr>
<tr><td>>4 & <=8</td><td>2</td></tr>
<tr><td>>8 & <=12</td><td>3</td></tr>
<tr><td>>12</td><td>4</td></tr>
</table>
</td></tr>
<tr><td>Client Site Support - Performance -</td><td>80% of the Level 2 Incidents at each site should be resolved within 6 business hours from the time a call is received / logged which ever is earlier. The maximum resolution time for any incident of this nature shall not exceed 48 hours.

Severity of Violation: Medium

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

If the performance in a month for an implementation site falls below the</td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>minimum service level, it will be treated as one (1) instance. The total number of instances for the six-month period will be the cumulative number of instances across all the months across all sites in the six-month period.

Average number of instances per month = (Total number of instances for the six-month period) / 6
<table>
<tr><th>Average number of instances per month</th><th>Violations for calculation of penalty</th></tr>
<tr><td>>0 & <=4</td><td>1</td></tr>
<tr><td>>4 & <=8</td><td>2</td></tr>
<tr><td>>8 & <=12</td><td>3</td></tr>
<tr><td>>12</td><td>4</td></tr>
</table></td></tr>
<tr><td>Client Site Support Performance</td><td>Replacement of hardware equipment shall be done within 7 days of notification by the Meghalaya Police. These equipments would have failed on four or more occasions in a period of less than three months or six times in a period of less than twelve months. (Mean Time Between Failure Condition)

Severity of Violation: High

Each instance of non-meeting this service level will be treated as one (1) violation.</td></tr>
</table>

4. <u>Handholding Support: Application Support</u>

(a) -**<u>Level 1 Defects</u>**. The failure to fix has an immediate impact on the Meghalaya Police's ability to service its police stations / higher offices, inability to perform critical back-office functions or a direct impact on the organization.

(b) -**<u>Level 2 Defects.</u>** The failure to fix has an impact on the Meghalaya Police'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) -**<u>Level 3 Defects.</u>** The failure to fix has no direct impact on the Meghalaya Police's ability to serve its police stations / higher officers, or perform critical back-office functions.

(d) -The severity of the individual defects will be mutually determined by the Meghalaya Police and SI.

(e) -This service level will be monitored on a monthly basis.

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

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td>Application Support Performance</td><td>95% of the Level 1 defects shall be resolved within 4 business hours from the time of reporting full details.

Severity of Violation: High

This service level will be monitored on a monthly basis.
<table>
<tr><th>Performance over the six-month period</th><th>Violations for calculation of penalty</th></tr>
</table></td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td></td><td>
<table>
<tr><td>< 95% & >= 90%</td><td>1</td></tr>
<tr><td>< 90% & >= 85%</td><td>2</td></tr>
<tr><td>< 85%</td><td>3</td></tr>
</table>

In addition to the above, if the service level in any month in the six-month period falls below 85%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Application Support Performance</td><td>95% of the Level 2 defects shall be resolved within 72 hours from the time of reporting full details.

Severity of Violation: High

This service level will be monitored on a monthly basis.
<table>
<tr><td>Performance over the six-month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>< 95% & >= 90%</td><td>1</td></tr>
<tr><td>< 90% & >= 85%</td><td>2</td></tr>
<tr><td>< 85%</td><td>3</td></tr>
</table>

In addition to the above, if the service level in any month in the six-month period falls below 85%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Application Support Performance</td><td>100% of the Level 3 defects shall be resolved within 120 hours from the time of reporting full details.

Severity of Violation: High

This service level will be monitored on a monthly basis.
<table>
<tr><td>Performance over the six-month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>< 100% & >= 90%</td><td>1</td></tr>
<tr><td>< 90% & >= 80%</td><td>2</td></tr>
<tr><td>< 80%</td><td>3</td></tr>
</table>

In addition to the above, if the service level in any month in the six-month period falls below 80%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Application Support Performance</td><td>Up to date of the documentation of the design, modifications, enhancements, and defect-fixes in the half-yearly period.

Severity of Violation: Medium

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

Service Level Description	Measurement
	violation.

5. Network Uptime:

Severity of Violation: High -

This service level will be monitored on a monthly basis. -

The below tables gives details on the Service Levels the SI should maintain. -

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

6. Handholding Support: Helpdesk and Data Center Support

(a) **Level 1 Calls**. The failure to fix has an immediate impact on the Meghalaya Police'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 Meghalaya Police'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 Meghalaya Police'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 scheduled operation time for the Helpdesk shall be 24X7

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

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

Severity of Violation: High

This service level will be monitored on a monthly basis.
<table>
<tr><td>Performance over the six-month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>< 98% & >= 90%</td><td>1</td></tr>
<tr><td>< 90% & >= 80%</td><td>2</td></tr>
<tr><td>< 80%</td><td>3</td></tr>
</table>
In addition to the above, if the service level in any month in the six-month period falls below 80%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Helpdesk Performance</td><td>98% of the incidents within helpdesk resolution capacity shall be resolved in a cycle time of 24 hours

Severity of Violation: High

This service level will be monitored on a monthly basis.
<table>
<tr><td>Performance over the six-month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>< 98% & >= 90%</td><td>1</td></tr>
<tr><td>< 90% & >= 80%</td><td>2</td></tr>
<tr><td>< 80%</td><td>3</td></tr>
</table>
In addition to the above, if the service level in any month in the six-month period falls below 80%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Helpdesk Performance</td><td>98% of the non SI supported incidents shall be routed to the appropriate service provider within 30 minutes.

Severity of Violation: Medium

This service level will be monitored on a monthly basis.
<table>
<tr><td>Performance over the six-month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>< 98% & >= 90%</td><td>1</td></tr>
<tr><td>< 90% & >= 80%</td><td>2</td></tr>
<tr><td>< 80%</td><td>3</td></tr>
</table>
In addition to the above, if the service level in any month in the six-month period falls below 80%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
</table>

<table>
<tr><th>Service Level Description</th><th>Measurement</th></tr>
<tr><td>Helpdesk Performance</td><td>80% of the Level 1 calls shall be resolved within 2 hours from call received / logged which ever is earlier. The maximum resolution time for any incident of this nature shall not exceed 8 business hours.

Severity of Violation: High

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

Severity of Violation: High

This service level will be monitored on a monthly basis.
<table>
<tr><td>Performance over the six-month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>< 80% & >= 70%</td><td>1</td></tr>
<tr><td>< 70% & >= 60%</td><td>2</td></tr>
<tr><td>< 60%</td><td>3</td></tr>
</table>
In addition to the above, if the service level in any month in the six-month period falls below 60%, one (1) additional violation will be added for each such month to the overall violations for this service level.</td></tr>
<tr><td>Helpdesk Performance</td><td>80% of the Level 3 calls shall be reported on status and action to be communicated within 24 hours from call received / logged which ever is earlier. The maximum resolution time for any incident of this nature shall not exceed 72 hours.

Severity of Violation: High

This service level will be monitored on a monthly basis.
<table>
<tr><td>Performance over the six-month period</td><td>Violations for calculation of penalty</td></tr>
<tr><td>< 80% & >= 70%</td><td>1</td></tr>
<tr><td>< 70% & >= 60%</td><td>2</td></tr>
<tr><td>< 60%</td><td>3</td></tr>
</table>
In addition to the above, if the service level in any month in the six-month</td></tr>
</table>

Service Level Description	Measurement
	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 Meghalaya Police. These equipments would have failed on four or more occasions in a period of less than three months or six times in a period of less than twelve months. (Mean Time Between Failure Condition) Severity of Violation: High Each instance of non-meeting this service level will be treated as one (1) violation.
Datacenter Support Performance	Up to date of the documentation of the design, modifications, enhancements, and fixes. Severity of Violation: Medium This service level will be measured on a half-yearly basis. Each instance of non-meeting this service level will be treated as one (1) violation.

7. Reporting

(a) The below tables gives details on the Service Levels the SI should maintain for client site systems availability.

Service Level Description	Measurement
Availability and Performance Report	Provide monthly SLA compliance reports, monitoring and maintenance related MIS reports by the 5th of the following month. Severity of Violation: Medium This service level will be monitored on a monthly basis. If the monthly SLA compliance report related to the service level metrics is not provided in the given timeframe, it will be treated as one (1) instance. The total number of instances for the six-month period will be the cumulative number of instances across all the months in the six-month period.

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

Service Level Description	Measurement	
	> 3	2

8. Credits for Successful Application Uptake

The below tables gives details of the credits that can gained by the SI for successful uptake of the application in the State/UT. The credits will not be calculated for the first reporting period and would commission from next 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-objection certificate and Informational such a requesting the status of a case) 2. - Number of active users profiles in CCTNS 3. - Number of read-write transactions on CCTNS system 4. - Number of Searches carried out on data in CCTNS 5. - Total number of FIRs prepared through CCTNS 6. - Total number of Crime Details Forms prepared through CCTNS 7. - Total number of Key Investigation Forms prepared through CCTNS 8. - Total number of Arrest Cards prepared through CCTNS 9. - Total number of ChargeSheets prepared through CCTNS 10. Quality (recency and accuracy) of information available in CCTNS 11. Number of cases reported to be solved because of the availability of CCTNS 12. Number of ad-hoc requests successfully responded to using CCTNS 13. Turnaround Time for submitting the monthly and annual crime/criminal information to NCRB from the State/UT A credit will be gained for each of the above parameters if the uptake for that parameter shows significant improvement. The following table applies for each of the above parameters:

% increase over the measurement in the last reporting period	Credits
>5 & <=10%	2
>10 & <=15%	3
> 15%	4

9. Violations and Associated Penalties

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

(b) -A six monthly performance evaluation will be conducted using the six monthly reporting periods of that period.

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

(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.

a. - 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.

b. - 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 Meghalaya Police shall have the right to terminate the contract.

ANNEXURE III: GOVERNANCE STRUCTURE (STATE LEVEL)

This section provides the governance structure that will be created at the State level to monitor the implementation of the CCTNS project. 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

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	• Formulating Project Proposals • Hardware rollout and operationalization • 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
State Police Core Team	• To work in tandem with SPMC, SPMU and SI as internal domain of experts • Provide Operational Support to State Mission Team • Collect and analyze feedback from end users, at regular intervals • Recommend State Mission Team on improving delivery services under the project
District Mission Teams	• 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 Suggested

Member 1 (Chairperson)	**Chief Secretary, Govt of Meghalaya**
Member 2	Addl. Chief Secretary (Home)
Member 3	Finance Commissioner
Member 4	Secretary, IT&TE
Member 5	Secretary, NCRB
Member 6	Representative of NIC
Member 7	Representative of GOI,MHA
Member 8 (Convener)	State Nodal Officer, (CCTNS Project)
Member 9	Any other member Co-opted from the field of IT, Telecom etc

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

Members	**Composition Suggested**
Member 1 (Chairperson)	**Director General of Police**
Member 2 (Co-Chairperson cum Nodal Officer)	Head of SCRB
Member 3	Representative of NCRB
Member 4	Representative from Home Department(State Level)
Member 5	Representative from Finance Department
Member 6	Representative from IT& TE Department
Member 7	Representative of NIC
Member 8	Representative of State Implementation Agency
Member 9 (Convenor)	Nodal Officer
The Committee may co-opt any other member whenever, felt necessary.	

The composition of **State Mission Team** is as following:

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

The composition of **State Police Core Committee** is as following:

Members	**Composition Suggested**
IGP\Armed Police	Chairman
DIG\Range	Member Secretary
SSP\CID	Member
SSP\Training	Member
CO\SAP	Member
SSPs of Districts	Members

JD/T&C	Member

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

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

ANNEXURE IV: FUNCTIONAL REQUIREMENT SPECIFICATIONS

This section has been intended to present the indicative functional requirement specification of all the application modules including the Core Application Software (State) and all the additional modules proposed by Meghalaya Police. The functionalities mentioned are only indicative in nature. SI is expected to study the SRS/ FRS provided by NCRB for CAS and the indicated FRS provided below and do the necessary vetting/ assessment for possible enhancements:

Functionalities - To Be Delivered By Centre:

Citizen Service Portal		
The Citizen Portal Service should enable Citizens to track the progress of their General Service Petitions and Citizen Services online. General Service Petitions/Citizen Services include passport verification requests, NOC (No Objection Certificates, NOC for vehicle theft, Lost Cell Phone Certificate, etc.)		
S. No.	**Functionalities**	**Integration Requirements**
	CAS(State)	
1.	Should allow user (citizens) to access Citizens' Services portal via the internet	
2.	Should allow users (citizens/petitioners) to search for their request on the basis of Service Request number or petitioner details.	
3.	Should display petition/service request details and status on the screen based on the user search	Petition Management Service, Complaint and FIR management service
4.	Should allow users to save the status as a PDF file and/or print the status	
5.	Should allow the users to provide comments and feedback on online services	
6.	System should provide the user with the following Transaction Services through the online portal 1. Complaint Registration 2. Tenant Verification 3. Servant Verification 4. Permission request for rallies and processions 5. Passport Verification Status 6. Arm License Verification Status 7. Application for Character Certificate 8. Lost Cell Phone Certificate 9. Registration of Missing Persons, Un-natural death, Unidentified Dead Body, Lost Property, Unclaimed/ Abandoned Property. 10. NOC for purchase second hand vehicle System should provide the user with the following representative Information Services through the online portal 1. Missing Persons Listing (with Photographs) 2. Proclaimed Offenders Listing 3. Stolen/ Recovered Vehicles Listing 4. Unidentified Dead bodies (with photographs) Listing 5. Abandoned / Unclaimed/recovered Properties Listing 6. Most Wanted Criminals Listing (with photographs)	
7.	System should allow the user	

	1. To download all applicable forms as e-forms and submit the same System should provide the user to download forms for following services through the online portal 1. Complaint Registration 2. Tenant Verification 3. Servant Verification 4. Permission Request for Processions and Rallies 5. Application for Character Certificate Submit e-form once the user has connectivity	
8.	System should provide the user with an Online Help facility 1. Frequently Asked Questions on workflow of applications 2. User Manual on procedures to avail police services 3. Relevant police documents (library) 4. Up to date information on the location of the Police Station/ Other Police Offices along with the Landmark and the contact details. 5. Should allow user (citizens) to view menu of services available	
9.	System should allow the user to input the following details for complaint registration on the online portal (at least 2 should be andatory) 1. Mobile Phone Number 2. Address 3. Identifications 3.1 Ration Card Number 3.2 Passport Number 3.3 Bank Account Number 3.4 Voter ID Card Number 3.5 PAN Number 3.6 Unique ID Number 3.7 Electricity Bill Number 3.8 Landline Telephone Number 3.9 Email ID	
10.	System should provide an acknowledgement to the complainant (once the application has been submitted online) through 1. Mobile Phone (SMS) 2. Email 3. On Screen	
11.	System should generate a complaint reference number for retrieval of complaint status information (such as the use of *CAPTCHA* feature)	
12.	1. System should allow the user to select their relevant (as per jurisdiction) police station from a list (in case the PS is known) 2. System should forward the complaint to the relevant PS or appropriate authority based on address of the complainant (in case the PS is not known)	

13.	System should allow the user to lodge an anonymous information (in case the user does not want to disclose personal details) 1. User should be able to select from '*Tip*'	
14.	System should allow the user to submit C-form to register foreigners 1. Provide for notices to foreigners (leave India notices) 2. Alerts to Interpol 3. Overstay checks and alerts 4. Alerts to immigration database (interface once created)	
	Enhancements	
15.	Should allow citizens to have dynamic user names and passwords for accessing the system and registration of complaints/ requests ensuring privacy and anonymity of the user. For example, Private Sector Organizations can request for employee verification through the portal.	
16.	Should have the facility of online payment of fine for Traffic Challans.	Traffic eChallaning module System
17.	Should provide the functionality to the Hotel owners of registering their Hotel details - Name of the Hotel - Owner/ Manager valid identification details - Staff identification details - Staff Verification details - City - District - Nearest Police Station Tax Identification Number or any other Registration Number	Petition Management Service
18.	Should allow periodic uploading of following information of the customers staying at Hotel: - Customers Name and Identification Proof - Address - Nationality (for non-Indian nationals Passport Number is mandatory) - Customer journey details (From Place, Destination, Purpose of Travel, No. of days to stay) ***Note:*** *The System should also allow the hotels to upload the details of foreigners staying in the hotels along with the Form C details.* System should be able to auto-populate the information of hotel residents based on previous entries, if any	
19.	Should have space for publicity of commendable work done by citizens in assisting the police.	
	RTI Services	
20.	Should be able to provide RTI Act mandated information.	
21.	System should allow receipt of online RTI application and online payment of fees.	
22.	System should allow the facility to digitize the manual application and forward it to the SPIO for further processing.	
23.	System should assign a Unique ID for each RTI request/ application. ID can be used by applicant for tracking the status	
24.	System shall allow classification of requests/ applications according to the Police units to deal with it.	

25.	System should have standard templates for replying to the requests	
26.	System to automatically transmit the requests to the SPIO and further allows SPIO to transfer the request to concerned Police Unit	
27.	System to allow concerned officer to get the reply verified against request from their respective supervisors	
28.	System shall allow the concerned officer to retrieve the information from central repository as desired against the RTI. The system shall offer facility for searching and retrieving the required data by using pre defined parameters	
29.	The system shall allow taxonomy based search in case the officer concerned wants to view similar RTI queries responded	
30.	The system shall throw alerts when the request is pending for a period exceeding a pre-defined time limit	
31.	The system shall be able to generate report in the form of RTI register for all the RTI requests received at any time it is requested for.	
32.	The system shall have the capability to upload the final response of the department on the web portal or provide to the applicant, as required.	
33.	System to have interface with payment gateway to receive minimal fees for filing RTI System to have functionality of calculating charges for providing the information under RTI and communicating the same to requester.	
	Portal Services for Police Officials	
34.	Should allow Police Officers to access the portal via the Internet/ Intranet	
35.	Should allow the police officers to register their grievances.	
36.	Facility of Single Sign-on and allowing the Police Officers to log in to the departmental modules through Portal	All modules of CAS (State) and other additionally proposed modules
37.	Should provide role based access to the various modules and sub modules of the proposed CAS (State) and other additionally proposed modules to all the Police Officials.	All modules of CAS (State) and other additionally proposed modules
38.	Should provide the Police Officials with the help module to assist them in using the Portal/ CAS (State) and other additionally proposed modules	User Help and Assistance Service
39.	Should provide the Police Officials with comprehensive Search capability to access any type of information which is desirable for e.g.) e-learning course material, area specific information, crime & criminal information, etc. Search would run on the knowledge base using business intelligence methods.	
	Petition/Verification/Request Management Service	
General Service Petition can be any of No Objection Certificate (NOC) for job, NOC for vehicle theft, NOC for lost cell phone/passport, Licenses for arms, processions etc		
S. No.	**Functionalities**	**Integration Requirements**
	CAS(State)	
1.	Should allow the user (police staff) to capture the general service petitions of the citizens based on their request. The general service requests can be any of the following No Objection Certificates, verification of passport, service, tenant, servant, Lost cell phone, arms license, permissions for procession, rallies, mikes, etc.	

	1. Employee Verification 2. Tenant Verification 3. Servant Verification 4. Permission Request for Processions and Rallies 5. Passport Verification Status 6. Arm License Verification Status 7. Application for Character Certificate	
2.	Should have different templates/forms to record the details of service requests of different kinds. E.g. NOC, Certificates for Loss of things, Permissions Requests etc.	
3.	Should allow uploading of any relevant documents such as scanned documents/images.	
4.	Should allow the user to assign the petition to police personnel for Preliminary enquiry.	
5.	Should allow the user (police staff) to record notes/remarks to the petition at various levels.	
6.	Should allow the user to search the existing repository of previous cases/petitions before responding to the petitioner.	Crime and Criminal Records and Query Management Service
7.	Should allow for approval by the concerned officer before issuing the certificate.	
8.	Should provide the user to entrust/re-entrust the petition and close the petition	
9.	Should allow the user (police staff) to generate the certificate or report or permission or the response to the petitioner.	
10.	Should allow the user to link / de-link petitions.	
11.	Should allow the user to merge petitions in case of duplicate petitions.	
12.	Should provide the reports and search capabilities on the petitions to both the user as well as senior officers	Crime and Criminal Records and Query Management Service
13.	System should forward a request for verification of a stranger (in case the permanent and present address are different) to the relevant police station (be it in a different state)	
14.	System should dispatch the response of a petition / service request via 1. Email and/or 2. Post 3. SMS And update the status of the application in the system	
15.	Should allow the user to view timeline within which to resolve the issue (process step) System should generate an alert if no action is taken on a petition within 24 hrs (for complaint and FIR) and 7 days for general verifications, and sent to higher officers. If 24 hrs / 7 days time limit has been breached a non-compliance report should be generated automatically to all higher offices	
16.	System should allow multiple agencies to carry out verification concurrently such as	

	passport verification by PS and by CID / district police office should be concurrent	
17.	System should allow to capture request for Foreigner - Registration Certificate - Registration Permit	
18.	System should allow user to generate RC & RP	
	Enhancements	
19.	Should have parameterized search capabilities and generate parameterized reports	Crime and Criminal Records and Query Management Service
20.	Should have provision for searching all databases with the name and other details provided	Crime and Criminal Records and Query Management Service
21.	Should allow the user to make modification of the templates/ forms as per his requirement while retaining essential queries in the form as uneditable.	State CAS Administration and Configuration Management Service
22.	Should allow the higher authorities to track down the verifications requests which are pending for a long time.	
23.	Should have web enabled functionality to capture online application and details of various kinds of application for verification (where citizens can directly apply)	
24.	Should have the interface with the other department (Regional Passport Office/ SDM Office/ etc.) for Police Verification. System should allow the user to receive online service request applications from other agencies (such as RPO).	Passport Office Application, SDM Office Application
25.	Should have provision of generating dynamic user id and password for providing details of person, to be verified Password to be sent in email as a message	
26.	Should be linked with payment gateway for receiving fees against providing service verification.	
27.	Should provide acknowledgement to the requester office post receiving request for verification.	
28.	Should be able to provide updated status on the verification exercise on a real time basis.	
29.	Should allow the user (citizen) to check the status of his application and to view the instructions of the OC to visit PS for signature authentication etc.	
30.	Should have provision to help assign a verification request to an Verifying Officer.	Duty Deployment Management service
31.	System to have functionality of a checklist which can be filled during physical visit and take witnesses (witness at verification location) signatures, pictures or thumb prints (as required).	
32.	Should have all functionalities for sending request along with document proof to respective authorities, depending on the type of verification requested.	
33.	Should carry warn to the citizen he is liable to be prosecuted for malicious complaint or content in accordance with the law in force.	

34.	Should capture the details of the arrival, departure, passport and visa status, purpose of visit, places visited including the information relating to their stay in the state.	
35.	Should prompt identification of persons detained in the course of investigatory actions by police, including identification of absconders.	
36.	Should have the facility to perform parameterized search and to generate parameterized report for the foreigner's registration/arrival related information.	
37.	Should be able to generate various monthly/quarterly reports of the foreigner's registration department.	
38.	System should have linkage with Intelligence database for any verification of the foreigner.	
39.	Should have the option of alerting Interpol or other security agencies of the country.	

Unclaimed/Abandon Property Register Service		
The Lost/Stolen property registers will maintain the unclaimed/abandon property. Police personnel would search the registers to identify, if the unclaimed property is reported lost or stolen for different case.		
S. No.	**Functionalities**	**Integration Requirements**
	CAS(State)	
1.	Should allow the user to capture the unclaimed/abandoned property details.	
2.	Should allow uploading of any relevant documents such as scanned documents/images	
3.	Should present different templates/forms for different kinds of property (vehicles, cultural, fire arms, cell phones etc.,)	
4.	Should allow user to search the lost/stolen property in different case or different police station within the repository.	
5.	In case a match is found the system should link the unclaimed/abandoned property with the case	
6.	In case if the property wasn't claimed for more than 6 months then the system should prompt & record the auction details after requisite approvals.	
7.	Should provide the reports and search capabilities on the unclaimed/abandon property	Crime and Criminal Records and Query Management Service
8.	System should allow the user to search for stolen / abandoned property (based on access rights)	
9.	System should generate an alert for the concerned IO if the property seized is already involved in a crime	
10.	Should allow the user to view the details of the sale proceeds deposited in Govt treasury once the property is auctioned off after requisite approvals (SHO and higher officers)	

Complaint and FIR Management Service		
Citizens approach police station to log the complaints which can be of cognizable, non-cognizable etc., The police personnel will register the complaint and generate an FIR/NCR.		
S. No.	**Functionalities**	**Integration Requirements**

CAS(State)		
1.	System should provide the user to log the complaint details. The complaints could be of different nature (Cognizable and Non-Cognizable; Criminal Incident, Missing Person, Stolen Property, Deserter etc.,)	
2.	Should allow uploading of any relevant documents such as scanned documents/images.	
3.	Should present different templates/forms for different kinds of complaints.	
4.	For example, the system should provide different forms for missing person report, unnatural death report, unidentified dead body report, unclaimed/ abandoned property report.	
5.	Should allow the user to assign the complaint to police personnel for preliminary enquiry.	
6.	Should allow the user to record notes/remarks on the complaint.	
7.	Should allow the user to search the existing repository of previous complaints before acting on the complaint.	
8.	Should allow for approval by the concerned officer before issuing the FIR.	
9.	Should provide the police personal to create the FIR/complaint report (for other cases) or a report for juvenile case.	
10.	Should allow the user to transfer an FIR falling in other jurisdiction.	
11.	System should facilitate the closing of a complaint for those complaints which do not proceed for investigation.	
12.	System should allow the user to link / de-link complaints.	
13.	System should allow the user to merge complaints in case of duplicate complaints.	
14.	The complaints can also be registered through the PCR Call Interface and Management Service.	PCR Call Interface and Management Service
15.	Should present the station writer a dashboard with the report summary table consists of new cases, court disposal, cases pending arrest etc.,	Periodic Crime and Law & Order Reports and Review Dashboard Service
16.	Should provide the reports and search capabilities on the complaints registered.	
17.	System should display the name of the police station / higher office where the compliant was originally registered	
18.	System should allow the user to edit the Act and Section for a registered FIR (an alert should be sent to higher office and judiciary) (only with alteration memo / amended FIR)	
19.	System should allow the user to link Unidentified Dead Bodies with Missing Persons	
20.	System should provide for automatic dispatch of notifications to Airports & Seaports (ports of entry and exit) on criminal movements	
21.	System should allow the user to capture 1. Signature of the complainant (using a digital pen or paper scanner) 2. Thumb impression of the complainant (using a paper scanner) 3. Signature of the approving authority (using digital pen and paper scanner)	

22.	System should allow the user to send copies of the FIR to a distribution list through email	
23.	System should allow the user to create and forward special reports to DIG / IG Range, CID and DGP (in cases of heinous crime)	
24.	System should allow the user to link FIRs with MLCs / Missing Persons / Unnatural Deaths (since they can be converted into FIRs)	
25.	System should allow the user to have information on 1. Hartals 2. All types of Agitations The investigation of such cases also to be viewed / reported to DySP / Assistant Commissioner and Narcotic Cell	
26.	The complaint passed from PCR can be acted upon by PS staff by registering compliant on suo moto basis depending upon the nature of the compliant otherwise PCR is not the FIR receiving window	
27.	Provision may be given to show the wings / units like Vigilance and Anti Corruption Bureau / CBCID in the FIR - to be taken in context of entering data pertaining to an agency where the case is being transferred	
	Enhancements	
28.	System should allow the user to capture the 'Alias' of complainant, accused, witnesses etc. in the FIR	
29.	Should allow the user to see the list of police stations with jurisdictional areas to file complaint in appropriate PS	
30.	System should be able to log complaint and FIR on cognizable sections of laws in major acts, minor acts, special and local laws etc. [SI has to get the full details of such acts from Meghalaya Police and have to add them in the application.]	
31.	Should enable the user to refer to the library of laws to refer as a ready reckoner.	
32.	System should show the status of a complaint including FIR filed with that much of information being provided in this application which the law such as RTI permits.	
33.	Should have the facility of enabling the user to ask for FIR registration and the investigation report.	
34.	System should facilitate the closing of a complaint for those complaints which do not proceed for investigation, however FIR can't be closed.	
35.	System should pop up an erroneous message if the no reason is inputted while closing a case.	
36.	Should allow the citizen to view the list of cognizable and non cognizable cases to allow him to approach court direct without wasting time filling the complaint in PS/Ops.	
37.	Should allow the authorized user to reopen a closed case with the permission of court.	

PCR Call Interface and Management Service
The Complaints are also registered through the Central Police Control Room at the State Headquarters that is accessible to the public through Emergency Contact number (100). The system should provide an interface for the

Police Control Room personnel to capture the call and caller details in the Complaint Management System.		
S. No.	**Functionalities**	**Integration Requirements**
	CAS(State)	
1.	System should provide an interface to the Police Control Room (PCR) and Police Station users to capture the details of the complaint and the caller / complainant through a "quick capture complaint form" relevant for a complaint that is reported in through a phone call, email, walk-ins in emergency or a non-emergency situation. The system should also have the provision for recording the call along with the timestamp and capture in the system.	
2.	The system should display all the unanswered calls and the call/caller details to the user.	
3.	System should arrange the incoming calls in the order that come in.	
4.	The system should allow the user to answer /respond to the call through the user interface.	
5.	Should allow the user to record the call with the prior approval of the other respondent that the call will be recorded.	
6.	In case the call(s) comes in for an already registered complaint, the system should allow the user to link the call(s) to the registered complaint.	Complaint and FIR Management Service
7.	In case the caller reports a complaint that is within the jurisdiction of the PCR (either State HQ or District), the system should allow the user to identify the appropriate police station or available patrol vehicle and transfer the call to the same for response.	
8.	In case the caller reports a complaint that is outside the jurisdiction of the PCR (either State HQ or District HQ), the system should allow the user to transfer the calls to the appropriate police control room that has the jurisdiction.	
9.	The system should allow the user to record the details of complaint assignment and the action taken by the responder on the complaint.	Complaint and FIR Management service.
10.	Should provide the reports and search capabilities on the call registered/logged	
11.	Should have the facility to perform parameterized search and to generate parameterized report also.	

Investigation Management Service		
After a complaint is registered, police initiates the investigation process. The case is assigned to an Investigation Officer (IO). During the course of investigation, additional details are captured to build further to the information gathered during the registration phase. Investigation module should provide all the functionalities mentioned in CCTNS FRS by NCRB including the following requirements:		
S. No.	**Functionalities**	**Integration Requirements**
	CAS(State)	
1.	In case of NCR (Non Cognizable Report), the system should allow user to capture the investigation details relevant to a non cognizable offence and the approval from the court and prepare a final report for closure of the NCR	
2.	System should allow the user to generate an alteration memo and subsequently modify the acts and section details of the complaint.	
3.	Should allow uploading of any relevant documents such as scanned documents/images linked to the case under investigation/ inquiry	
4.	System should allow the user to record and transfer a case that does not fall under jurisdiction of the present police station after proper registration	
5.	Should present customized templates/forms for the type of complaint under	State CAS

	investigation.	Administration and Configuration Management Service
6.	Should allow the user to assign the FIR to other police personnel.	
7.	Should allow the user to record notes/remarks on the complaint.	
8.	System should change the case status depending on the progress of the investigation.	
9.	System should allow the user to record the remarks on the status/case progress.	
10.	System should associate pre-defined tasks / activities that are required during the investigation to the case. The tasks / activities should be customizable by the administrator to the type of the case under investigation. The user should be able to add / modify tasks / activities to the pre-defined list associated with the case. The administrator should be able to add / modify the super-set of tasks / activities defined in the system and make them default to a type of the case.	State CAS Administration and Configuration Management Service
11.	Should allow the user to capture the details of the investigation relevant to the type of the complaint.	
12.	Indicative details captured during investigation are given below. ▪ Crime scene details ▪ Victims Details ▪ Accused Details ▪ Witness Details ▪ Property Details (stolen/seized) ▪ Evidence details ▪ Forensics details ▪ Medico Legal Case Details ▪ Other details in the crime details form	
13.	System should allow preview and printing of all the required forms (7 IIF's, forms required for preparing the case dairy and other forms necessary for submission to the external entities such as courts).	
14.	In case of death, system should allow the user to capture results conducted for inquest (whether person was hurt, details of clothing etc.,) and generate an inquest report.	
15.	System should capture the inquest report generated by the magistrate in case of death in police or judicial custody or death of lady within 7 years of marriage.	
16.	System should allow the user to prepare, preview, print requests/forms that are sent to external agencies (FSL, FPB, hospitals, RTA etc.,) for expert opinion. The request/forms should be made available to the user as templates that are managed (created/edited) through administration functionality.	FSL module
17.	System should provide the feature to capture the response in the form of parameterized data and scanned documents received from different external agencies.	
18.	System should allow the user to prepare, preview and print arrest card.	
19.	System should allow user to capture the court surrender details	
20.	Should allow the user to capture the interrogation details as summary and parameterized data.	
21.	System should allow the user to capture the custody/remand details related to the decision of the court on the arrested that are produced before the court.	
22.	System should allow the user to view the detailed and summary views of the case	
23.	System should allow the user to prepare the final report (charge sheet, undetected,	

	untraced, mistake of fact, civil nature).	
24.	System should allow the case to be reopened and reassigned to a different investigating officer. In case of reopening, the case history should be maintained.	
25.	System should also track the remarks/suggestions posted by higher officers during investigation.	
26.	System should present the IO dashboard of under trials, under investigation, rep-opened cases to user based on their roles and their jurisdiction.	Periodic Crime and Law & Order Reports and Review Dashboard Service
27.	System should provide the dashboards to higher officials about the case progress and metrics about PT cases etc.,	Periodic Crime and Law & Order Reports and Review Dashboard Service
28.	System should allow the SSP & Senior Officers to view the summary of cases based type of case and cases falling in their jurisdiction	
29.	System should present the SHO & Senior officials about the details of the cases based on the status like open, closed, re-open, disposed, unresolved and case pending for trial.	
30.	Should provide the reports and search capabilities on the case progress.	Crime and Criminal Records and Query Management Service
31.	System should allow the user to record details of the property released during investigation	
32.	System should allow the user to record details of partial recovery of properties during investigation	
33.	System should allow the user to update the status of case property as 1. Released 2. Transferred 3. Sent to Police Station 4. Sent to Forensic Lab / Forensic Medicine Department 5. Sent to Court (as evidence)	
34.	System should be able to add the report details received from external agency.	
35.	System should allow the user to prepare a dossier of the criminal (as per procedures, where ever required)	
36.	System should allow the user to capture victim information under 1. Number of persons deceased 2. Number of persons seriously hurt 3. Number of persons with simple hurt 4. Number of non-injured persons 5. Gender 6. Age 7. SC / ST 8. Economic Strata 9. Educational Qualification 10. Nationality 11. Rel igion 12. Identity 13. Address 14. Contact Details (Telephone / Mobile / Email)	
37.	System should provide the user (investigating officer) with 1. Crime and criminal information 2. Address tracking of mobile users 3. Help book on investigating procedures through his / her mobile phone	

38.	System should allow the user to capture the case diary details (in a parameterized format)	
39.	System should prompt the police user with the list of documents and list if witnesses required for filing a charge sheet.	
40.	Provision for 'Dying Declaration' under 32 Indian Evidence Act to be made	
41.	Property Seizure Form 1. Linkage of confession statement with items confessed 2. Facility to add GD number against un-linked property under the same FIR number. 3. Tool -tip for confession statement during property linkage	
42.	System should provide for digitization of Bad Characters Roll A - SHO of the PS will be required to enter the details of a bad character under surveillience (in case the person is in the same district) Bad Characters Roll B - SHO fills in the roll B in case the person moves out of the district	
43.	Investigation - Disclosure of the Accused person may reveal Co-accused For this purpose Section 82 and Section 83 of the CrPC may be referred System should provide for - capture of details for co-accused - Attachment of assets of the co-accused (absconder) under Section 83 CrPC	
44.	System should provide to add multiple entries under MLC report	
45.	System should provide to add multiple entries for 'Victims eligible for compensation' - would need to be flagged individually	
	Enhancements	
46.	System should be able to mark special cases as SR cases which can be tracked/monitored/retrieved by the supervising officers of the Crime Branch and the officers above.	
47.	System should provide for an alert to the user in cases where accused identity is not known, but 1. Similar case has been registered, where accused identity is found to be near description 2. Similar case is registered with same modus operandi 3. An arrest has been made in an another case with similar accused description	
48.	System should send alerts in the below cases, to concerned District SPs and SP CID 1. Murder Cases where no significant progress is made even after 72 hours of investigation 2. In all murder cases in which the accused are not identified in FIR 3. Explosions in which more than one person is killed. 4. All cases of seizure of spirit in which the seized quantity exceeds 5000 litres. 5. All cases of seizure of Narcotic and Psychotropic Substances other than Ganja, except those where the quantity of the substance seized does not exceed the prescribed "minimum for personal consumption or small quantity". 6. Cases of theft of Government Arms and Ammunitions and theft or loss of Government property over Rs. 10 lakhs. 7. All Women Trafficking Cases having interstate linkages. 8. Cases of Cheating or fraud by private financial institutions where the total transactions involved or the deposits collected by the accused exceed Rs. 2 Crores in that particular case or other cases of a similar nature involving the same accused. 9. Cases other than traffic accident	

	cases in which Police Officers of and above the rank of CI figure as accused except petitions endorsed by Courts under Sec. 156(3) CrPC. 10. All counterfeit currency cases as per practice followed now in respect of such cases	
49.	While preparing any document relating to case investigation (e.g. Arrest Card) system should pre populate the details. (e.g. User enters the arrest related info like 1. Date and time of arrest 2. name of the police personnel who made the arrest etc)	
50.	System should allow the user to enter/ capture the unique identification details of the convicts like IRIS, Fingerprints and Facial patterns.	
51.	Should be able to link the finger print into the accused/victim details.	
52.	System should prompt the user with the list of documents required for filing a charge sheet.	
53.	System should not allow the Computer Operator/ Investigating Officer to get the system generated copy of the Charge Sheet until he has filled the other IIF forms (No. 2, 3 and 4)	
54.	Multiple Chargesheets should be able to be submitted in a single FIR. In a single case supplementary chargesheet may also be prepared and submitted (even during trial)	
55.	System should be able to generate the information on the criminal (his previous convictions) at the time of generation of Charge sheet.	
56.	An alert should be sent to the concerned officer by the system when a higher officer adds some comments on a case.	
57.	System should allow to export any report to a spreadsheet, word or a pdf	
58.	User should be able to add a task in a calendar with a brief description	Notification of Alerts, Imp. Events, Reminders & Activity Calendar or Tasks Service.
59.	Should alert an IO of the activities to be done within a stipulated period of time. E.g. filing a charge sheet	Notification of Alerts, Imp. Events, Reminders & Activity Calendar or Tasks Service.
60.	System should be able to display an alert/notify of important activity to be done	Notification of Alerts, Imp. Events, Reminders & Activity Calendar or Tasks Service.

Court and Jail Interface & Prosecution Management Service

At the end of the investigation, a Charge Sheet or Final Report is filed in the court. Interfacing with the courts during the prosecution of cases is an integral part of the responsibility of police personnel. This will help the police personnel in preparing the charge sheet and recording the prosecution / trial details.

S. No.	Functionalities	Integration Requirements
	CAS(State)	
1.	System should allow the user to capture the charge sheet acknowledgement details (interim and final) received from the court after the submission of the Charge Sheet.	
2.	System should allow the user to capture the Trial update / Court disposal form. Indicative details captured during trial day of the case are given below ▪ Court Disposal Details ▪ Next hearing date ▪ Trial Status of the persons involved (Attendance, Examination, ▪ Bail Plea, Required for Next Hearing…) ▪ Bail ▪ Accused Status ▪ Next Hearing date ▪ Court Order	
3.	System should allow the user to capture the summons/warrants issued by court.	
4.	System should allow the user to assign the summons/warrants to police personnel/police station.	Duty Deployment Management system
5.	System should allow the user to record the status of execution on the summons/warrants.	
6.	System should allow for generation of alerts on unexecuted warrants	
7.	Special Warrants - 'Type of Warrants' (for National / International Criminals) - DW Warrant (Distress Warrant) - BW Warrant (Bailable Warrant) - Notices - Red Corner Notice - Blue Corner Notice - Yellow Corner Notice - Others	
8.	System should allow the user to capture details if the convicted appeals in the higher court.	
9.	System should allow the user to capture the status (granted retrial, appeal denied) of the appeal.	
10.	System should allow the user to proceed for re-investigation if ordered by the court.	
11.	Incase if accused applied for bail, system should allow the user to record the bail details	
12.	System should allow the user to capture jail / remand related information (release from jail, sent on judicial remand, sent to police custody …).	
13.	System should provide an alert to the SHO and IO on cases of 'impending expiry of remand period'	
14.	The system should allow the prisoner / suspect / arrested / convict / acquitted movements into and out of jails.	
15.	System should allow the user to manage and handle the split cases.	
16.	System should provide for 'Tracking of Appeal Cases'	
17.	System should provide for 'Change of IO' 1. In most of the cases IO can be changed	
18.	The solution should provide the IO to view the tasks that he/she had set in calendar, the court appointments, and Administrative related tasks.	

19.	System should present court constable dashboard include court appointment schedule, summary of charge sheets, case disposed by court, summons and warrants.	Periodic Crime and Law & Order Reports and Review Dashboard Service
	Enhancements	
20.	System should notify the concerned officers in case of re-investigation. System should change the status to "Under Investigation".	Investigation management Service
21.	System should allow the user to file a separate charge sheet in case of a spilt case.	
22.	System should allow to send messages to local police station in case of discharge of under-trials/convicts from Jail on furlough/parole etc	

Crime and Criminal Records and Query Management Service		
This functionality will help the police personnel in searching (Quick & Advanced) the complaint, crime, criminal, abandoned / unclaimed property, stolen / lost property, missing persons, arrested, released from jails, convicted, acquitted, pending warrants, pending summons and other investigation-toolkit-data (Vehicle Registration, Driver License, Cell Phone Numbers, Voter Details, Education Data, …) repository.		
S. No.	**Functionalities**	**Integration Requirements**
	CAS(State)	
1.	Should provide the user to search the repository based on FIR No, Beat area, case category, date range and year/month/week. It should also provide the user to select multiple values for a single field.	
2.	Should provide the user a quick search for given case ID	
3.	System should also provide an advanced search capability and allow user filter the search to a greater detail like crime details, suspect details, victim details, modus operandi and property.	
4.	The system should allow the user to configure / build a query on the searchable data through query builders.	
5.	System should provide the ability to store, load and delete custom queries to each user for easy retrieval.	
6.	System should allow the user to organize the search results sort by clicking on table header	
7.	System should organize the search results in paged manner. It should also provide user the flexibility to navigate to the required page.	
8.	System should provide standard formats for the data from external sources (Vehicle Registration, Driver License, Phone (cell and land line from multiple providers) Numbers, Voter Details, Educational / Academic Certification Data) and a utility to capture the data into the investigation toolkit- data repository.	
9.	System should provide for capturing the updates or a complete feed of the external data and capture only the updates since the last feed in case of a complete data set is re-fed into the system.	
10.	System should maintain the history of data in case of modifications (ex, vehicle transferred to a new owner, an old cell phone number acquired by a new user)	
11.	System should provide the user with an ability to search (full and partial strings) the investigation-toolkit-data repository. This search interface should be made available both as a separate interface and as well as an integrated interface, integrated with the crime and criminal search interface.	
12.	In case the searched entity has a history of ownership, the same should be presented	

	in the search results.	
13.	System should provide the user to export the search results in the format selected by the user like doc, pdf, xls, and spreadsheet in printer friendly format with page numbers printed on every page.	
14.	If a user performs a quick or advanced search, the System must never include in the search result list any record which the user does not have the right to access. If a user requests access to, or searches for, a case which he does not have the right to access, the System must provide one of the following responses (selectable at configuration time): display title and metadata; display the existence of a case but not its title or other metadata; Do not display any case information or indicate its existence in any way. These options are presented in order of increasing security. Note that the requirement in the third option (i.e. the most stringent) implies that the System must not include such cases in any count of search results; this level of security is normally appropriate for cases dealing with matters such as national security.	
15.	System should have an interface with FSL module	FSL module
16.	System to provide the option with —"Do you mean this" with relaxed matches of searched category/ parameter	
17.	System should provide facility for automated correlation of 'missing / found / dead persons' - will forward the correlated items to the queue of the officer who has registered the case.	
	Enhancements	
18.	Vehicle Tracking system: This consists of Search in the Database of Vehicle and ownership details.	Transport Department Application
19.	System should provided up to date information on the Vehicles with Red light permits/ tinted glasses permit.	Transport Department Application
20.	System should provide up to date information on the security category of the VVIP vehicles (for example X, Y, Z, Z+, SPG protégé)	Transport Department Application
21.	Driving Licenses: This consists of Search in the Database of Driving Licenses.	Transport Department Application
22.	Telephone (Land line) Tracking System: This consists of Search in the Database of all Land lines.	Service Provider Database
23.	Mobile Tracking System: This consists of Search in the Database of all Mobile Telephones, both pre-paid and post-paid.	Service Provider Database

24.	Ration Card Search: This consists of search in the Database of all Ration Cards issued in each District.	
25.	Find FSL Report Status: This consists of search in the Database of all samples examined at Meghalaya State FSL to track when the samples have been received at FSL and when the expert opinion / report has been dispatched to the Court etc.	FSL Module (DNA Profiling)
26.	Find case Status in HC/ SC: This consists of search in the cause list of Meghalaya High Court and Supreme Court for knowing the date of hearings in Writ Petitions etc. This module also gives all the judgments of Supreme Court and High Courts.	Prosecution Module
27.	Tracing Case Law: This Database consists of all Acts and judgments of Supreme Court and High Courts which can be searched based on various parameters. The Search also can be done based on citations, judge, advocate, petitioners, case no. etc.	Prosecution Module
28.	Voter List Search: This Database consists of all Voters list throughout the State which can be searched based on various parameters.	

Police Email and Messaging Service

The Police Messaging system is role based communication system helps the police personnel to send "Faster" and "Secure" official correspondence within / across the multiple wings within / across the Police Departments. It should provide the general mailbox features such as address book, send / receive mail with attachments, creation / deletion of folders, moving mail to folders, spell check, mail filters, calendar, rich text editor, auto responders, signatures, server side mail filters, spam filters and support the mail protocols (IMAP and SMTP).

In case of email, the system should offer all the features of the police messaging systems. However, the emails will be personal emails / authentication identity that are created at the time of creation / addition of the user into the system and not role based.

S. No.	Functionalities	Integration Requirements
	CAS(State)	
1.	Should allow the user to create or import the organizational hierarchy and the users of the police department	
2.	Should allow the user to select the user list from the organization hierarchy	
3.	Should allow the user to create personal address book, groups	
4.	Should allow the user to send messages to groups.	
5.	Should allow the user to create & select templates for message standardization	
6.	Should allow the user to choose the option for read receipt	
7.	Should allow the user to search the messages from the archive based on message subject and between two dates	
8.	System should allow the user to choose the option of encrypting the message	
9.	System should allow the user to print the message in printer friendly format	
10.	System should allow the user to subscribe to alerts on cell phone in case of receiving a new email in the inbox.	
11.	System should show the usage statistics at all levels and departments.	
	Enhancements	
12.	User should be able to create folders with rule based redirection of incoming emails	
13.	System should provide a way through which the user is able to sort emails by clicking on any attribute header	

14.	System should allow a facility through which all emails with common subject line is seen/ shown together in a common thread.	
15.	System should allow the user to search for email address of any other member of the service on the basis of personal particulars (Name, Rank, Posting place etc.)	
16.	Email address scheme to be specified in consultation with Meghalaya Police	
17.	User should be able to create folders with rule based redirection of incoming emails	
18.	System should provide a way through which the user is able to sort emails by clicking on any attribute header	
19.	System should allow a facility through which all emails with common	

Periodic Crime and Law & Order Reports and Review Dashboard Service		
This functionality will help the police personnel to view the snapshot of the various statistics within and across police stations on petitions, cases, NCR, FIR, warrants, wanted offenders/suspects etc.,. This will also be used by the higher officers at all levels/roles to conduct periodic reviews of the police stations in their jurisdiction.		
S. No.	**Functionalities**	**Integration Requirements**
	CAS(State)	
1.	System should present customized dashboards to the users based on their role (Duty Constable, Court Constable, Station Writer, IO, SHO, Circle Inspector, ACP, DCP, Sub-Divisional Officer, CP,SP, higher officers in the Range/Region/ Chief Office	
2.	System should present various statistics such as summarized information, current progress, monthly numbers, comparative statements, trends with charting capability, exception reports, crime maps indicating the hot spots.	
3.	System should allow the user to view on alerts/events/reminders	
4.	System should present the user with statistics of all petitions	
5.	System should present the user with statistics on “Newly Registered complaints”	
6.	System should present the user with statistics on NCR’s (Non Cognizable cases).	
7.	System should present the user with statistics on FIRs with different statuses such as New/Under Investigation/ Pending Trial/ Re-opened	
8.	System should present the user with statistics on Warrants & Summons	
9.	System should present the user with court calendar which includes details on court appointment schedule, information on the cases under trial.	
10.	System should present the user with activity calendar.	
11.	System should present the user with statistics and list of “high priority FIR” (Grave Crime Details)	
12.	System should present the user with list of Pending Arrests & Wanted Offenders/Suspects	
13.	System should present the user with statistics of charge sheets & Court Disposal	
14.	System should present the user with list of latest happenings across police stations such as missing persons & unidentified dead bodies	
15.	System should present the user with prisoner movement updates	
16.	System should present the user with Major and Minor head wise statistics	
17.	System should present the application usage statistics that provide indicators on the application uptake and usage by the police personnel	
18.	System should allow the user to drill down to a granular level to a complaint or suspect from the information presented in the dashboard.	
19.	System should provide the user an interface to enable the senior officers to conduct periodic reviews of the police station (citizen services, law & order, crime…)	

20.	System should allow the user to generate comparative statements of the above said statistics during monthly crime reviews.	
21.	System should allow the user to review the pending or overdue actions such as "filing a charge sheet within a defined time limit from the time of registering the case", arrest of known accused etc.	
22.	System should allow the user to create additional tasks / alerts / reminders on the actions items for investigating officers and track its progress in next monthly review.	
23.	System should consolidate and generate statistics based on the role and jurisdiction.	

Notification of Alerts, Imp. Events, Reminders & Activity Calendar or Tasks Service		
Alerts and Events will help the police personnel to know about the latest information about arrest, vehicles recovered, un-known dead bodies, Date of VIP bandobast etc.,		
S. No.	**Functionalities**	**Integration Requirements**
	CAS(State)	
1.	System should automatically generate alerts (suspect in one case person or wanted either because of pending warrants / summons apprehended / arrested in a different case, vehicle reported lost in one case is either recovered or found abandoned, dead body details captured in the system matches the details for a missing person reported in a different case, suspect in one case / person wanted either because of pending warrants / summons sent on remand or released in a different case, complaint of certain kind (attention diversion gangs) registered in a police station, in case a general petition for a procession or road work has been approved, an alert on the same well in advance to the affected police station(s), alerts in case an activity is pending for more than a week or an advance alert in case the stipulated time is about to expire (ex, police remand about to expire and the IO has to file for remand extension), a case coming up for trial where the IO has to be present as a witness, …)	
2.	System should automatically generate reminders of any pending or overdue actions on the cases that are pending registration / investigation / trail.	
3.	System should allow the user to create and send user alerts / events / reminders to identified group / subscribed users / police stations.	
4.	System should allow the user to schedule the activities and maintain the calendar with reminders.	
5.	The alerts / events / reminders are either sent to the respective IO / SHO handling the case or in charge of the police station with the jurisdiction of the case.	
6.	The alerts / events / reminders should be available to be sent in the form of an email, or SMS to the registered phone or as an alert in the application once the user logs into the system or all available modes.	

State SCRB NCRB Data Transfer and Management Service		
This functionality will enable the states to transfer the crime and criminal data from states, to organize it suitably to serve NCRB requirements. As part of the scope of the SDA, the SDA has to design common formats for maintenance of crime and criminals' records that will be used across all Police Stations in the country; and would facilitate the usage of these formats for the creation of sharable crime and criminals' related databases at Police Stations, Districts, States and at the national level.		
S. No.	Functionalities	Integration Requirements
	CAS(State)	
1.	Should extract the crime, criminals, and other related data or updates from the previous extraction from States and UTs database at regular and pre-specified periods. The periodicity might differ from data group to data group.	

2.	The data extracted from States/UTs must be transformed into standard formats required by NCRB.	
3.	The data should be run through a quality process to identify any possible duplicates or wrong data before sending to NCRB	
4.	Transformed and cleansed data must be uploaded on to NCRB databases	
5.	The system should provide the flexibility to cleanse and transform data	
6.	The system should support automatic extraction of data	
7.	System should provide an option to monitor and manage data extraction, Transformation and loading process	
8.	System should allow the user to kick start the load process manually in the absence of load failure	
9.	System should allow reconciling those records which failed during the load process.	

State CAS Administration and Configuration Management Service

This functionality will help the individual states to configure the application to suit to their requirements. The configurability should be by a business user through the user interface of the application or through a technical user by changes to the master data at the database without any requirements of changes to code or redeployment of the application.

S. No.	Functionalities	Integration Requirements
	CAS(State)	
1.	The solution should provide the user to customize the application without affecting the core.	
2.	System should allow the user to change the look and feel like font, skins, images of the application	
3.	System should provide the flexibility in creating/modifying and deleting the user Hierarchy and should allow the admin to assign roles as proposed by Districts, Ranges, Zones and police stations.	
4.	System should allow the user to define the organization all its units (police stations, districts, range, zone) and user hierarchy	
5.	System should present the data elements based on major and minor heads selected by user.	
6.	System should generate reports based on roles defined.	
7.	System should allow the user to add/modify/delete/modify-order of acts, sections and local laws.	
8.	System should provide the user to add/modify/delete/modify-order if MO/property-type/castes/tribes details.	
9.	System should not allow the user to delete/modify/modify-order of the master data provided by the centre.	
10.	System should allow the user to maintain different templates as per the directive of local governments or standard guidelines.	
11.	System should allow the user to maintain case specific service levels/time limits/measurable indicators for each step in the case progress from registration to investigation to trial.	
12.	A change in service levels/standards/benchmarks should be maintained/tracked by the system with start and end dates	
13.	A change in role/designation should be maintained/tracked with start and end dates	

User Help and Assistance Service

This functionality will help the user in providing the details about each page and also help in guiding the police personnel in capturing the data.

S. No.	Functionalities	Integration

		Requirements
	CAS(State)	
1.	The solution should provide detailed context-sensitive help material for all the possible actions and scenarios on all user interfaces in the application.	
2.	The solution should provide context based help facilities and also on-line help at functions, screen and field level that can be customized by the State.	
3.	The solution should have comprehensive help facility wherein the users can obtain system specific technical / functional help on line	
4.	The help should be accessible to the users both in the offline and online mode	
5.	The system should maintain and make available to user a database of frequently asked Questions	

User Feedback Tracking and Resolution Service		
This functionality will help the police personnel in logging the issues/defects occurred while using the system on to Issue Tracking system.		
S. No.	**Functionalities**	**Integration Requirements**
	CAS(State)	
1.	The solution should provide an interface for the user to log any defects or enhancement requests on the application and track thereafter.	
2.	The solution should send alerts (e.g., email, SMS) to the user if the user chooses to whenever any action has been taken on the alert	
3.	The solution should enable the user to track the submitted defect or enhancement request.	
4.	The solution should enable the help-desk user to view the reports on the submitted defects or enhancement requests category-wise, status-wise, and age-wise.	
5.	The support solution should be accessible to the users both from within the application and also outside the application through a different interface (ex, in case the CAS application is down).	

Activity Log Tracking and Audit Service		
The Audit Trail is a sequence of audit records, each of which contains evidence directly pertaining to and resulting from execution of a business process or system function.		
S. No.	**Functionalities**	**Integration Requirements**
	CAS(State)	
1.	An audit trail is a record of actions taken by either the user or the system triggers. This includes actions taken by users or Administrators, or actions initiated automatically by the system as a result of system parameters. The System must keep an unalterable audit trail capable of automatically capturing and storing information about: ▪ All the actions (create/read/update/delete) that are taken upon the critical entities (case, suspect, property,…) in the system ▪ The user initiating and or carrying out the action; ▪ The date and time of the event. ▪ Administrative parameters The word “unalterable” is to mean that the audit trail data cannot be modified in any way or deleted by any user; it may be subject to re-department and copying to removable media if required, so long as its contents remain unchanged.	
2.	Once the audit trail functionality has been activated, the System must track events without manual intervention, and store in the audit trail information about them.	

3.	The System must maintain the audit trail for as long as required, which will be at least for the life of the case to which it refers.	
4.	The System must ensure that audit trail data is available for inspection on request, so that a specific event can be identified and all related data made accessible, and that this can be achieved by authorized external personnel who have little or no familiarity with the system.	
5.	The System must be able to export audit trails for specified cases (without affecting the audit trail stored by the System). This functionality can be used by external auditors, who wish to examine or analyze system activity.	
6.	The System must be able to capture and store violations (i.e. A user's attempts to access a case to which he is denied access), and (where violations can validly be attempted) attempted violations, of access control mechanisms.	
7.	The System must at a minimum be able to provide reports for actions on cases organized: ▪ By case; ▪ By user; ▪ In chronological sequence.	
8.	Any access to cases and all other activities involving the cases and related documents or data should also need to be stored in the audit trail to ensure legal admissibility and to assist in data recovery.	

User Access and Authorization Management Service		
This functionality will clearly differentiate users based on their access privileges with the system and also help in authenticating and authorizing the user to access specific set of functionalities.		
S. No.	Functionalities	Integration Requirements
	CAS(State)	
1.	The system must allow the user to create / update / delete user and user profile.	
2.	The System must allow the user to limit access to cases to specified users or user groups.	
3.	The system should provide for role-based control for the functionality within the system.	
4.	The System must allow a user to be a member of more than one group.	
5.	The System must allow only admin-users to set up user profiles and allocate users to groups.	
6.	The System should allow a user to stipulate which other users or groups can access cases.	
7.	The System must allow changes to security attributes for groups or users (such as access rights, security level, privileges, password allocation and management) to be made only by super-user.	
8.	System should allow the user to those functionalities that he/she is authorized to access.	
9.	System should allow a maximum of three attempts to login.	
10.	System should allow the user to regenerate a lost password/reset password with set of hint questions	
11.	System should encrypt the user passwords	
12.	System should allow creation of new users, transfer of postings for existing users and any other actions that affect their authentication and authorization settings.	
13.	System should allow changes in roles/ authorization with the transfer / promotions of staff	

Additional Modules to be developed:

Grievances Redressal Systems for citizens/Police Employees:

The module is envisaged to protect citizens against exploitations, and to increase efficiency of the government in handling citizen grievances more effectively.

Sl. No.	Functionalities	Integration Requirements
1.	Should allow citizen/Police Employees to post grievances online. Should have an option which allows choosing the user to register as a citizen or as a Police Personnel. In Case of Police Personnel, details specific to Police personnels such as the post, rank, location etc be taken care of	
2.	Should allocate an unique grievance no to the filer for tracking the grievance	
3.	Should have an administrative module (role based) to set the name of a person responsible for handling grievance at department/section/area etc level, to define SLAs, to categorize grievances etc.	
4.	Should have an option to assign the grievances automatically as well as manually to person(s) (in charge officer of district and section or Police or Grievance Cell) so that a grievance never remains unattended / unassigned at any point of time till the resolution of the issue	
5.	Should store all relevant information like intimation date, assignment date, current status, update details incl. status, update date, person name etc. at any point in a grievance life cycle	
6.	Should support quick retrieval of grievances as and when required	
7.	Monitoring of all grievances lying at different level in terms of area wise, department wise, status wise, person wise, issue wise etc.	
8.	Should be mapped with people management system so that the assignment can be done efficiently	
9.	Should have parameterized search capabilities	
10.	Should generate parameterized reports.	
11.	Should be able to track the status of the action taken against the grievance.	

Traffic eChallaning module System

Sl. No.	Functionalities	Integration Requirements
1.	Should have the facility of finding the information on the vehicle and/ or the driving license on the basis of its Registration number/ Driving License no. / Name and Fathers Name/ Date of Birth.	RTO
2.	Should have the feature of finding the details of previous challan(s) if any on the vehicle/ driving license/ driver/ any other individual and take necessary action (if required)	
3.	Should have the functionality of challaning, money collection from the offender, updating of challan information and compounding of challan at the scene of offence	
4.	Should support Handheld devices for – issuing challan, accessing databases, reporting violation, acknowledging receipt of documents obtained from the offender, Compounding of challan on the spot, etc.	
5.	Should have the facility to give the system generated copy of the Challan, receipt for documents or payment receipt to the offender (optional)	
6.	Should have the facility of automatic update of Challan information in the	

	Traffic Violation Database.	
7.	Should have provision of accessing the database of crime and criminals and lost and stolen vehicles using the hand held device at the scene of offense	Crime and Criminal Records and Query Management Service
8.	Should have the facility of online payment of challan using the internet portal.	Citizen portal service
9.	Should have the facility to pay the challan money at the kiosks at the Traffic Police Office. The money from the Kiosks at the Traffic Police office would be collected in cash and the system would be updated	
10.	Should have the information on the status of Challan payment by the offender(s)	
11.	System should allow capturing of information relating to violations compounded by the court (in case of offenders who prefer going to court).	
12.	System should show pendency of challans in courts (more than 1 year, 6 months, 3 months, 2 months etc.) and generate reports	
13.	Should have provision of recording the offence against driver/ owner and maintaining the record for suspension/ cancellation of licenses	Prosecution Module
14.	Should create automatic alerts for offenders who have not paid their Challan fees for more than a month when they are caught next time	Prosecution Module
15.	Should have the facility of updating the database once the documents of the offender have been sent to court.	
16.	Should have interface with Police for criminal database, Transport for vehicle and drivers data, SCRB for stolen vehicles	
17.	Should allow violations/ challaning database to be shared with Transport department to allow them to cancel the driving license.	
ANPR module		
18.	Should support capturing of vehicle with its number plate appropriately that the vehicle can be searched on following parameters: (a) Full Plate (b) Half Plate (c) Category of vehicle Color (d) Category of vehicle	
19.	Should be able to provide information on the vehicle (Ownership, Details of previous offends (if any) on the basis of its registration number.	RTO
20.	Should be able to compare the data from the lost/ stolen/ wanted vehicles database on the basis of information received from within/outside state on the criminals/ suspects/ convicts traveling the vehicle.	
21.	System should be able to generate an alert as soon as a lost/ stolen/wanted vehicle passes through the system.	
22.	Should support counting vehicles in and out of premises, leaving a list of all vehicles on site (say a parking).	
23.	Should support the length of time a vehicle is on a particular premise.	
24.	Should support capturing Vehicle speed (from two cameras).	
25.	Should record in e Form the vehicle documents and the driver's license. The expired documents of the vehicle such as insurance certificate or driver's license expiry should be allowed to beep in the PCR/PS/Traffic Police Office/SCRB.	
City Wide Surveillance System		

26.	Easy to use interface and clear display of images on the monitor	
27.	Support to display video images from a cluster of cameras installed at one place	
28.	Should have the provision of displaying images / controlling the cameras from PHQ/DHQs through IP configuration/setup	
29.	Should provide the option to zoom and control the images through software application as well	
30.	Should have the capability to search and show the recording based on the time of a day	
31.	Should update the traffic violations detected in the CCTNS database.	

Duty Deployment Management Systems

Sl. No.	Functionalities	Integration Requirements
1.	Should have the following features • Multifunctional multi-duty planning and maintenance • Ease of use • Complies with Police Regulations • Shift planning to nearest minute • Absence control facilities • Compliance with Working Time Regulations • Major Event Planning/Operational Orders Module	
2.	Should have functionality for senior officers to check deployment details of personnel	
3.	Should capture the following details: • Details of various forces • Strength available in various jurisdictions • Specialized trained forces • Armed and riot equipment available • Communication sets available	

Intra Departmental Communication System

Sl. No.	Functionalities	Integration Requirements
1.	Should have functionality to send messages/circulars/notifications to appropriate recipients	
2.	Should have functionality to uniquely identify every officers/branch	
3.	Should generate unique id for each circular/messages/notifications	
4.	Should have the functionality to search any circular/message/notification	
5.	Should have functionality to highlight new alert when the recipient logs into the application or already using the application	
6.	Should have functionality to send alert of receiving new circular/notification through email & sms	
7.	Should be able to capture notes on any given circular	
8.	Should be able to forward the circular with notes to the other recipients for their information/necessary action	
9.	Should also be able to send scanned copy of document of circular/notification	

FSL Module

The aim of the FSL module is to streamline the workflow between the different divisions of the FSL, right from receipt of samples to dispatch of expert reports, capturing data related to each division to performance monitoring of Mobile Crime Scene teams, etc. FSL experts should also get access to case related data and also the Database of crime and criminals, missing persons, Unidentified Dead Bodies, Post Mortem reports, etc. and be able to give more informed opinion.

Sl. No.	Functionalities	Integration Requirements
1.	DNA Databank Management Sub Module	
2.	Should be able to add new DNA profiles along with details of reported convicts/ suspects/ missing persons (or their parents/ siblings), Unidentified dead bodies/ any other person.	
3.	Should be able to add missing person data automatically from the Citizen Portal Database.	Citizen portal service
4.	Should maintain database of missing persons, convicts and suspects (with case details E.g. FIR number) along with their DNA profiles.	
5.	Should have linkage with all the other databases maintained for searching match (missing persons/ unidentified dead bodies/ convicts and criminals) against the DNA profile obtained.	
6.	Should have the facility to compare and cross match the DNA Profiles stored in the database.	
7.	Should be able to link/ cross match DNAs of past crime/ criminal activity and generate reports (exact and relaxed match).	Investigation management
8.	Should have the facility to update the complaint on the basis of the DNA matching result	
9.	Should have provisions of making recommendations based on the search results by FSL team	
10.	FSL team should only have access to the results of DNA profiling and search exercise	
11.	Interface with the citizens to notify police on the missing person/unidentified dead body	Citizen portal service
12.	PS/ Other Offices/ Hospital should have an interface through which they can be informed of any unidentified dead body	
MIS Sub Module		
13.	Should have the Management Information System (MIS) to streamline the workflow between the different divisions of the FSL.	
14.	MIS should have the following functionalities: - To accept samples (Capture details of case, IO and the exhibit) - Give every exhibit an ID for tracking - Track movement of exhibit between Divisions - Generate Report and Despatch	
Note: MIS should help the IOs/ SP's to put in priority request; Also to track progress of analysis; MIS should also allow IO to put in supplementary queries, further analysis requests.		

Cyber Crime Management Service

Sl.	Functionalities	Integration

No.		Requirements
1.	Maintain a database (catalogue base) of cyber crime information related to latest virus/phishing attack	
2.	Send notification to all government department in case of latest threat in internet, mobile etc	
3.	Track the life cycle of a cyber crime case in the state	
4.	Maintain a list of cyber criminals inside or outside the state	
5.	Option to lodge a cyber crime complaint online	
6.	Display information about various types of cyber crime and cases, and prevention of cyber crime on a website	
7.	Store and display details of cyber crime training (in CDAC centre), list of trainees and experts	

ANNEXURE V: GENERAL REQUIREMENTS FOR CAS(STATE)

1. Ease of Use

To provide a User friendly interface to the users/ citizens of the CCTNS system the following functionalities have been envisaged:

S. No.	Functionality
1.	All error messages produced by the System must be meaningful, so that they can be appropriately acted upon by the users who are likely to see them. Ideally, each error message will be accompanied by explanatory text and an indication of the action(s) which the user can take in response to the error.
2.	The Interface should be simple, soothing to eye, attractive, uncluttered
3.	The System must employ a single set of user interface rules, or a small number of sets to provide a familiar and common look and feel for the application.
4.	The System must be able to display several entities (cases, suspects) simultaneously.
5.	The interfaces must be made customizable or user-configurable to the extent possible. (e.g., the displayed columns in the table, move, resize, modify the appearance). Such configurations must be saved in the user profile.
6.	The System user interface must be suitable for users with special needs; that is, compatible with specialist software that may be used and with appropriate interface guidelines
7.	The System must provide End User and Administrator functions which are easy to use and intuitive throughout.
8.	The System must allow persistent defaults for data entry where desirable. These defaults should include: • user-definable values; • values same as previous item; • values derived from context, e.g. date, file reference, user identifier
9.	Frequently-executed System transactions must be designed so that they can be completed with a small number of interactions (e.g. mouse clicks).
10.	Where the System employs a graphical user interface, it must allow users to customize it. Customization should include, but need not be limited to the following changes: • menu contents & layout of screens; • use of function keys; • on-screen colours, fonts and font sizes;

2. Usability

S. No.	Functionality
1.	The user interfaces should be designed to make them user-intuitive.
2.	The user interfaces of the system should comply with Standard ISO 9241.
3.	ICT accessibility: ISO 9241-20 shall be the standard for guidance on ICT accessibility. Application user interfaces to meet its requirements and recommendations. Software accessibility ISO 9241-171 shall be the standard for guidance on software accessibility. User interfaces should meet its requirements and recommendations. Content accessibility WCAG 1.0 shall be the standard used for guidance on content accessibility. The application logo to be available on all pages as a link to the home page.
4.	Providing text equivalents for non-text media objects: All non-text media objects, such as graphical images or video, should be provided with alternative equivalent textual

S. No.	Functionality
	descriptions and/or with equivalent text-based functionality.
5.	Making navigation self-descriptive: Navigation should be designed to help users understand where they are, where they have been and where they can go next. General guidance on achieving self-descriptiveness is given in ISO 9241-110.
6.	Showing users where they are: Each presentation segment (page or window) should provide the user with a clear and sufficient indication of where he or she is in the navigation structure and of the current segment position with respect to the overall structure. Offering alternative access paths: Alternative access paths for navigating to a specific unit of content should be offered to support different navigation strategies.
7.	Minimizing navigation effort: The number of navigation steps needed to reach a certain piece of content should be minimized as long as different mental models, navigation strategies and tasks of the user are taken into account.
8.	Splash screens should be avoided unless they provide useful content or feedback about the application state to the user. If a splash screen is used, a navigation option to skip it should be offered.
9.	Avoiding opening unnecessary windows: Additional windows such as new browser windows or pop-up windows should only be opened if this supports the user's task. Opening new windows can distract, confuse or impede users for a variety of reasons. They can superimpose the primary window, hiding relevant information. They could make it cognitively more difficult to understand the navigation structure with negative effects on both usability and accessibility. They also require additional user actions for closing unwanted windows.
10.	Vertical scrolling should be minimized. This may be done by placing important information at the top and providing links to information that is further down the page. Horizontal scrolling should be avoided wherever possible.
11.	Designing for input device independence: User interfaces should be designed to allow activation of controls by a variety of input devices. The ability to choose between different input devices for activating controls such as links, fields and buttons is important both for users who prefer a certain input mode, mobile users and users with disabilities. In general, device independence can be achieved if the functionality is operable via a keyboard.
12.	Making user interfaces robust: User interfaces should be designed to be as robust as possible in the face of changing technology. This encompasses being able to present content containing newer technologies by older user agents as well as designing content to be usable with future technologies.
13.	Acceptable opening / download times: Application pages should be designed and implemented so that there are acceptable opening times and download times for the expected range of technical contexts of use (e.g. bandwidth between the application and the user). This is particularly important for frequently accessed pages or pages that are important for user navigation and exploration, such as the home page.

S. No.	Functionality
14.	Minimizing user errors: Potential user errors as well as the effort needed to recover from errors should be minimized.
15.	Providing clear error messages: The content of error messages shown on the pages or special error pages should clearly state the reason why the error occurred and, if possible, actions the user can take to resolve the error. Users expect error messages to be in the same language as the user interface.
16.	Using appropriate formats, units of measurement or currency: When designing user interfaces for use by diverse groups, input and output of information elements such as currency, units of measurement, temperatures, date and time, phone numbers, address or postal codes should be designed so that they are usable.
17.	Making text resizable by the user: Text should be able to be resized by the user, using functions provided by the user agent or other appropriate means i.e. see ISO 9241-171.
18.	Text quality: The quality of textual content with respect to spelling and grammar should be sufficient so as not to impede readability.
19.	Writing style: The reading and understanding of the textual content on the screen should be supported by suitable means, including the use of short sentences, the division of the text into shorter chunks or the presentation of content items in the form of bullet points.
20.	Supporting text skimming: Fast skimming of text should be supported by the provision of clear links, bulleted lists, highlighted keywords, logical headings, and short phrases and sentences.
21.	Readability of text: Text presented on the pages should be readable taking into account the expected display characteristics and spatial arrangement. ISO 9241-303 shall be consulted for screen text legibility requirements.
22.	Distinguishable within-page links: Within-page links should be clearly distinguishable from other links that lead to a different page. EX. Within-page links are shown with dashed rather than solid underlines
23.	Avoiding link overload: Text pages containing large proportions of links should be formatted so that the presence of links does not impede the readability of the text.
24.	Using familiar terminology for navigation links: Navigation links — particularly links representing the main navigation structure — should be labelled with terms that are familiar to the user, based on his/her general knowledge, prior experience in the application domain or experience of using other systems.
25.	Using descriptive link labels: The target or purpose of a link should be directly indicated by its label, avoiding generic labels such as “go” or “click here” except where the purpose of the link is clear from its context on the page or the labels have commonly understood semantics in the particular application domain. Using Appropriate terminology specific to the user’s tasks and information needs is important for making the content easy to understand.

S. No.	Functionality
26.	Marking links opening new windows: Links that open new browser windows or pop-up windows should be clearly marked.
27.	Distinguishing navigation links from controls: Navigation links should be clearly distinguishable from controls activating some action. Typical action types in user interfaces include manipulating application data, performing searches, communication actions, such as opening a new e-mail window or starting a chat function, and Hpresentation-related actions, such as sorting a list of search results.
28.	Providing printable document versions: If a document is either too long, dispersed over several pages or in a specific layout that is not suitable for online reading, a printer-friendly version of the document should be provided that prints the content in a form acceptable to the user (e.g. in the expected layout, paper format, or orientation).
29.	Use of “white space”: “White space” on a page i.e. space filled only with the background color should be used in such a way that it does not impair the visual skimming of the page. While white space is an important means of visually organizing the different content elements on a page, if the distance between the blocks of information displayed becomes too large, rapid skimming of the page can be impeded.
30.	Selecting appropriate page lengths The length of a page should be selected so as to support the primary purpose and use of the page. Short pages are generally more appropriate for homepages, navigation pages, or overview pages that need to be read quickly. Longer pages can be more appropriate when users want to read the content without interruptions or when the page needs to match a paper counterpart.
31.	Using colour: Colour should be used with care, taking into account human capabilities and restrictions in perceiving colour, and not as the only means of conveying information. Color should never be the only means of coding. Some users may have difficulties in perceiving certain colors or color combinations
32.	Providing alternatives to frame-based presentation: If frames are used, an alternative way of presenting relevant information without frames should be provided. Providing alternative text-only pages: When style sheets and/or frames are turned off it should be possible for the user to read and understand the page; alternatively, the user should be provided with an equivalent alternative text-only page.
33.	Consistent page layout: Pages should be designed using consistent layout schemes, supporting the user in finding similar information at the same position on different pages. Overall layout schemes apply to all pages and are preferable when all pages have a similar structure. Frequently, however, different pages have different purposes and types of content. In such cases, pages can usually be grouped in different categories, using one layout scheme for each category consistently.
34.	Placing title information consistently: Page titles should be placed in a consistent location on the different pages.
35.	Observing principles of human perception When designing application pages, the general principles of human perception should be taken into account. The International Standards mentioned below shall be consulted for guidance. Practical guidelines for presenting information to the user are to be found in ISO 9241-12. Guidance on selecting and using

S. No.	Functionality
	different forms of interaction techniques is to be found in ISO 9241-14 to ISO 9241-17. ISO 9241-14 gives guidance about menus, ISO 9241-15 about command dialogues, ISO 9241-16 about direct manipulation and ISO 9241-17 about forms. In addition, when designing multimedia information presentations, the design principles and recommendations described in ISO 14915-1 to ISO 14915-3 should be taken into account. Appropriate content presentation also plays a key role in accessibility.
36.	Linking back to the home page or landmark pages: Each page should contain a link leading to the home page of the application or to a landmark page that is easy to recognize for the user.
37.	Providing a site map: A separate navigation overview such as a site map should be provided for application showing the structure of the site in an overview form.
38.	Consistency between navigation components and content: If navigation components (or overviews) are shown in conjunction with associated content, consistency between the navigation component and the content shown should be maintained by indicating in the navigation component (e.g. highlighting) the topic currently visible in the content area.
39.	Placing navigation components consistently: Navigation components should be placed consistently on the pages or in the framesets in the pages of the application.
40.	Individualization and user adaptation : Adapting the content and the navigation of a user interface to individual users or user groups can be a useful mechanism for providing information that is of interest to the users and for making access to relevant information more efficient. User adaptation can also be important for making the user interface more accessible. Different approaches can be used for achieving these goals, like providing users with means for customizing the user interface to their personal needs i.e. individualization designing content and navigation differently for varying user groups or roles i.e. such as employees of different levels, citizens etc, monitoring the user's behavior and adapting to the user's goals that are inferred from the behavior observed, recommending information that is potentially more relevant or interesting to the specific user, based on the behavior of all users or a user group.
41.	Taking account of the users' tasks and information needs: When providing different access paths or navigation structures for different user groups, the tasks and information needs of these user groups should be taken into consideration.
42.	Making individualization and adaptation evident: It should be made evident to the user when individualization and/or adaptation are used.
43.	Making user profiles evident: If predefined user profiles or user-specified profiles are used for individualizing or adapting content, the profile currently used should be made evident. If profiles are used, it is important to provide users with information about this concept and its implications.
44.	Allowing users to see and change profiles: If user-specified profiles are used, users should be able to see, modify and delete that profile on demand.

S. No.	Functionality
45.	The user interfaces of the system should follow the guidelines specified under www.usability.gov

3. System Availability

S. No.	Functionality
1.	The System must be available to users: • 24X7 • On all days of week
2.	The planned downtime for the System must not exceed <06> hours per <rolling three month period>. The System is considered to be down if any user is unable to perform any normal System function and if this failure is attributed to any component of the System other than the workstation.
3.	In the event of any software or hardware failure, it must be possible to restore the System (with inline synchronization) within defined limits as per SLA

4. Performance and Scalability

S. No.	Functionality
1.	The System must provide adequate response times for commonly performed functions under both standard and peak conditions
2.	The System must be able to perform a simple search within 5-8 seconds and an advanced search (multiple search criteria) within 10-15 seconds regardless of the storage capacity or number of cases in the system. In this context, performing a search means returning a result list. It does not include retrieving the records themselves.
3.	The System must be able to retrieve and display within 5-8 seconds the case which has been accessed within the previous 2 months, regardless of storage capacity or number of cases in the system. This requirement is intended to allow for rapid retrieval of frequently-used cases, on the understanding that frequency of use is typically correlated with recent use.
4.	The System must be able to retrieve and display within 20 seconds the case which has not been accessed within the previous 2 months, regardless of storage capacity or number of cases in the system. This requirement is intended to allow for cases where cases used infrequently are stored on slower media than more active records.

S. No.	Functionality
5.	The System be scaleable and must not have any features which would preclude use in small or large police stations, with varying numbers of cases handled.

ANNEXURE VI: MEGHALAYA MAP

Meghalaya Police with a strong force of more than 11333 personnel (including Battalions) and with 39 Police Stations across the state plays an important role in maintaining the law and order situation in Meghalaya. State has been divided into 2 ranges covering 7 districts. The ranges cover various sub-division offices and PS coming under it as shown below:

S. No	Range	District	Subdivision	Circles	Police Station
1	Eastern Range	East Khasi Hills	Sohra	Sohra	Shillong Sadar
2				Mawsynram	Laitumkhrah
3					Lumdiengiri
4					Laban
5					Mawlai
6					Rynjah
7					Madanrting
8					Mawsynram
9					Pynursla
10					Sohra
11					Mawryngkneng
12					Shella
13					CID PS
14		West Khasi Hills	Nogstoin	Nogstoin	Nongstoin
15			Mawkyrwat	Mawkyrwat	Mawkyrwat
16			Mairang	Mairang	Mairang
17					Ranikot
18		Jaintia Hills	Khliehriat	Khliehriat	Jowai
19			Amlarem	Jowai	Dawki
20				Amlarem	Khliehriat
21					Amlarem
22					Saipung
23		Ri-Bhoi Hills		Khanapara	Nongpoh
24				Nongpoh	Umiam
25				Umiam	Khanapara
26	Western Range	East Garo Hills	Resulbelpara	Resulbelpara	Williamnagar
27				Williamnagar	Rongjeng
28					Mendipathar
29					Songsak
30		West Garo Hills	Dadengiri	Tura	Tura
31				Dalu	Phulbari
32				Mahendraganj	Mahendraganj
33				Phulbari	Dalu
34					Ampati
35					Tikrikilla
36					Dadengiri
37		South Garo Hills		Baghmara	Baghmara
38				Nongalbibra	Chokpot
39					Rongara

ANNEXURE VII: MEGHALAYA WAN AND SWAN POPS

As of now, there is no networking framework or structure that connects the offices and Police Stations of Meghalaya Police. The existing computers at the various sites and offices are standalone PCs, with no WAN connectivity. However, many of these have internet connectivity.

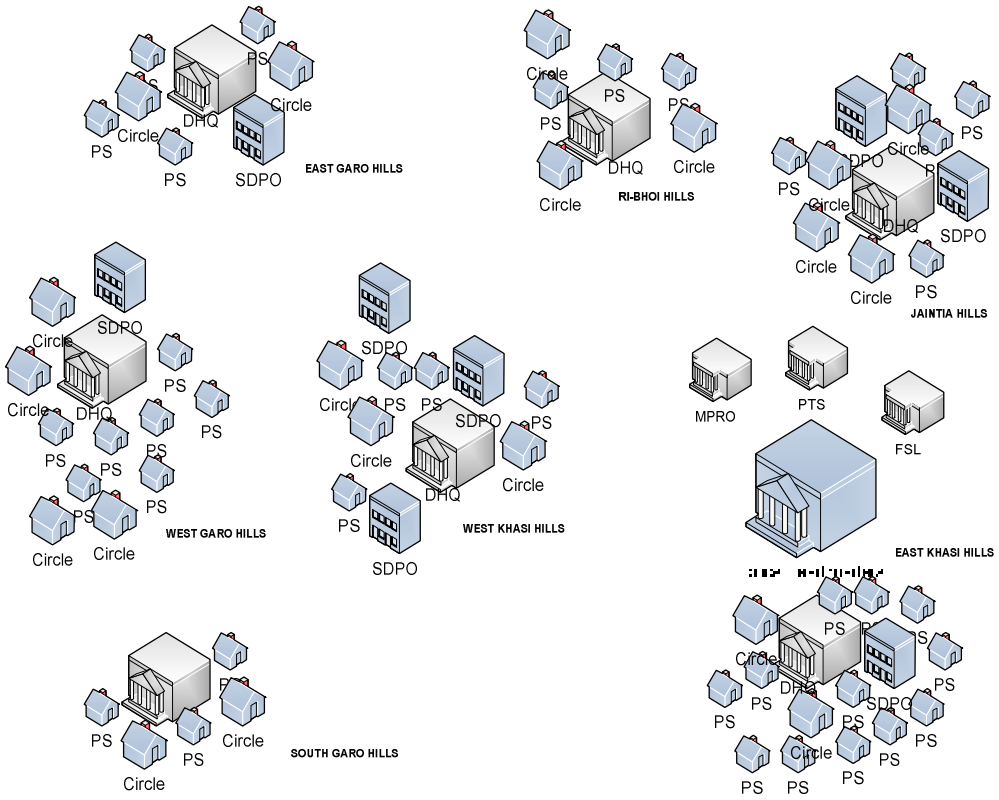


Figure: AS IS Snapshot of Network Connectivity showing No connectivity

The above table shows that none of the branches are connected by any WAN. However, some establishments do have an existing LAN structure for internal uses. Again, most of them have high speed internet connectivity.

- Most of the police wings are devoid of Computer network connectivity. Hence there is no internet connectivity among the various police units, although some police units have procured Internet Broadband Connection from BSNL.
- MPRO (Meghalaya police Radio Organization) and ISPW (Interstate police wireless) are responsible for radio communications
- PolNet was also set up but it is not in operation.

Network Detail					
Police Division	**Network Connectivity**	**Bandwidth**	**Internet Connectivity**	**Type**	**Internet Bandwidth**
SCRB & PHQ	LAN System/	LAN	OFC from NIC	Internet	Variable> 1 Mbps

SWAN POPs in MEGHALAYA

The SHQ, DHQ, SDHQ & BHQ PoP's will be located at the State Secretariat, District Commissioner / District Collector's Office, Sub Divisional Officer's (SDO) office & Block Development Officer's (BDO) office respectively. List of Districts, Subdivisions and Blocks is given below:

S. No.	District	SubDivision	Block
1	East Khasi Hills	Sohra	Shella*
			Mawsynram
			Khadar Shnong
			Mawphlang
			Mylliem
			Mawkynrew*
			Pynursla*
			Mawryngkneng
2	West Khasi Hills	Mairang	Mawshynrut
		Mawkyrwa	Nongstoin
			Ranikor*
			Mawkyrwat
			Mawthadraishan
			Mairang
3	Jaintia Hills	Amlarem	Thadlaskein
		Khliehriat	Laskein*
			Saipung*
			Khliehriat
			Amlarem
4	Ri Bhoi		Jirang
			Umling
			Umsning
5	East Garo Hills	Resubelpara	Resubelpara
			Kharkutta
			Rongjeng
			Samanda*
			Songsak
6	WestGaro Hills	Dadenggiri	Tikrikilla
		Ampati	Dadenggiri
			Selsella
			Rongram*
			Betasing*
			Dalu
			Gambegre*
			Zikzak*
7	South Garo Hills		Chokpot
			Gasupara*
			Baghmara*
			Rongra*

Some of the identified police offices where the SWAN connectivity would be provided in the initial phase are

Proposed and identified Horizontal Police / SP Offices under MSWAN				
S/N	**Name of DHQ**	**Name of PoP**	**Name of Office**	**Type**
1	South Garo Hills	Baghmara	**Office of Superintendent of Police**	DHQ
2	Jaintia Hills	Jowai	**Police SP - Jowai**	DHQ
3	Jaintia Hills	Jowai	**Police Station, Jowai**	DHQ
4	Jaintia Hills	**Khliehriat SDO**	**Police station, Khilerihat Meghalaya**	SDHQ
5	Ri Bhoi	Nongpoh	**Police Station - Nongpoh**	DHQ
6	West Khasi Hills	Nongstoin	**Police Station**	DHQ
7	West Khasi Hills	Nongstoin	**Police, SP Oofice - Nongstoin**	DHQ
8	East Khasi Hills	**Sohra SDO**	**Police Station(as requested by SDO) , Sohra SDO, Meghalaya**	SDHQ
9	East Khasi Hills	Shillong	**Police SP Office**	SHQ
10	West Garo Hills	**Dadenggre SDO**	**Police Station - Dadenggre SDO**	SDHQ
11	West Garo Hills	Tura	**Office of the Superintedent of Police**	DHQ
12	East Garo Hills	**Resubelpara**	**Police Station**	SDHQ
13	East Garo Hills	Williamnagar	**Office of the Superintendent of Police**	DHQ
14	East Garo Hills	Williamnagar	**Police Station**	DHQ

ANNEXURE VIII: EXISTING INFRASTRUCTURE DETAILS

CIPA Infrastructure details

Sl. No	District	Office	Desktop PC	Printer (Laser)	Multifunction Product	16 port unmanaged switch	Modem/Fax cards	Additional HDD 120 GB	DVD Writer i/o DVD Rom Drive	UPS 2KVA
1	East Khasi Hills	Shillong Sadar	3	1	1	1	2	2	2	1
2		Laitumkhrah	3	1	1	1	2	2	2	1
3		Lumdiengjri	3	1	1	1	2	2	2	1
4		Laban	3	1	1	1	2	2	2	1
5		Madanrting	3	1	1	1	2	2	2	1
6		Rynjah	3	1	1	1	2	2	2	1
7		CID(HQ)	3	1	1	1	2	2	2	1
8	West Khasi Hills	Nongstoiñ	4	1	1	1	2	2	2	1
9		Mairang	3	1	1	1	2	2	2	1
10	Jaintia Hills	Jowai	4	1	1	1	2	2	2	1
11		Khliehriat	3	1	1	1	2	2	2	1
12	Ri Bhoi	Nongpoh	4	1	1	1	2	2	2	1
13		Umiam	4	1	1	1	2	2	2	1
14	West Garo Hills	Tura	5	1	1	1	2	2	2	1
15		Phulbari	3	1	1	1	2	2	2	1
16	East Garo Hills	Williamnagar	3	1	1	1	2	2	2	1
17		Mendipathar	3	1	1	1	2	2	2	1
18	PTS	Shillong PHQ	9	-	-	-	-	-	-	9
		Total	**66**	**17**	**17**	**17**	**34**	**34**	**34**	**26**

Infrastructure details at various offices

Sl. No.	Office	Desktop PC	UPS	Printer (Dot Matrix)	Printer (Laser)	Scanner	Printer Combo
1	ADG (CID)	**1**	**1**	**0**	**0**	**0**	**1**
2	ADG (L&O)	**1**	**1**	**0**	**0**	**0**	**0**
3	ADG (R/PR/TS)	**1**	**1**	**0**	**0**	**0**	**0**
4	SB	**6**	**8**	**2**	**0**	**1**	**1**
5	IGP (TAP)	**2**	**2**	**1**	**0**	**0**	**0**
6	Dy IGP (ER)	**1**	**1**	**1**	**0**	**0**	**0**
7	Asst. IGP (E)	**1**	**1**	**1**	**0**	**0**	**0**
8	Asst. IGP	**1**	**1**	**1**	**1**	**0**	**0**
9	MPRO	**14**	**10**	**10**	**4**	**1**	**0**
10	F&ES	**3**	**3**	**2**	**1**	**0**	**0**
11	1st MLP Bn	**4**	**6**	**2**	**1**	**0**	**0**
12	2nd MLP Bn	**3**	**3**	**2**	**1**	**0**	**1**
13	3rd MLP Bn	**1**	**1**	**2**	**0**	**0**	**0**
14	4th MLP Bn	**2**	**3**	**2**	**1**	**0**	**1**

15	5th MLP Bn	**1**	**3**	**1**	**1**	**0**	**1**
16	Special Branch	**29**	**22**	**3**	**13**	**1**	**-**
17	Infiltration	**2**	**2**	**1**	**1**	**0**	**-**
18	CW&B	**8**	**11**	**2**	**1**	**1**	**0**

Infrastructure details at SP offices

Sl. No.	Office	Desktop PC	UPS	Printer (Dot Matrix)	Printer (Laser)	Scanner	Printer Combo
1	E.K.H	**1**	**2**	**2**	**1**	**1**	**1**
2	W.K.H	**1**	**2**	**2**	**1**	**0**	**1**
3	J.H	**1**	**2**	**2**	**1**	**0**	**1**
4	Ri-Bhoi	**1**	**4**	**2**	**1**	**0**	**1**
5	S.G.H	**1**	**2**	**2**	**0**	**0**	**1**
6	W.G.H	**1**	**3**	**2**	**1**	**1**	**1**
7	E.G.H	**1**	**2**	**2**	**1**	**0**	**1**

Capacity Building Infrastructure

Training Institues	Infrastructure Details								
	Servers	Desktop	LCD Projector	UPS	Printer	LCD Screen	Network Switches	Tables	Chairs
Computer Lab Training Centre, State PHQ	2	40	2	2	2	2	2	40	40
PTS	2	16	2	2	2	2	1	16	16
EKH DTC	1	10	1	1	1	1	1	10	10
WKH DTC	1	10	1	1	1	1	1	10	10
JH DTC	1	10	1	1	1	1	1	10	10
RiBhoi DTC	1	10	1	1	1	1	1	10	10
EGH DTC	1	10	1	1	1	1	1	10	10
WGH DTC	1	10	1	1	1	1	1	10	10
SGH DTC	1	6	1	1	1	1	1	6	6
Total	**11**	**122**	**11**	**11**	**11**	**11**	**10**	**122**	**122**

ANNEXURE IX: EXISTING SOFTWARE IN MEGHALAYA POLICE

This section lists the applications used by Meghalaya Police for their operational activities. Each application is detailed on the basis of its functionality, technology usage, issues and the recommendations.

a) Common Integrated Police Application	
Description	The application is a national level application & is used to – ▪ Record Case Registration Details ▪ Record Prosecution Details ▪ Record Other Crime & criminal related details ▪ Generate various Registers (Arrest register, Missing register etc) ▪ Generate various Reports (Crime Cases reports, Missing Persons reports, Unnatural death etc). ▪ Maintain daily station diary (Only at some of the police stations)
Technology Used	▪ Java as front end ▪ Postgres SQL as backend ▪ Linux as operating system
Installed At	▪ Police Stations
Issues	▪ Only FIR Registration module is used ▪ Operating System LINUX – not user friendly ▪ Standalone application (One police station application is not connected with that of other police station application) ▪ The system is not utilized at its maximum.
Recommendations	
Continue after CCTNS	NO
▪ All existing data on FIR Registration from CIPA should be migrated to CCTNS application. ▪ The data needs to be migrated to "Complaint and FIR Management Service" module of CCTNS.	

b) Crime Criminal Information System	
Objective	The Application is the previous version of CIPA & CIPA and has almost all the functionalities of CCIS.
Technology Used	NCRB latest version CCIS MLe SQL server
Installed At	Working in the entire state.
Issues	Non Submission of some forms
Recommendations	
Continue after CCTNS	NO
▪ All existing data from CCIS need to be migrated to CCTNS (Assumption is that that even though CIPA is newer version of CCIS – data migration has not been done from CCIS to CIPA) ▪ The data needs to be migrated to "Complaint and FIR Management Service" module of CCTNS.	

c) Talash System	
Objective	Investigation

Description	Contains database of arrested, kidnapped etc
Technology Used	SQL Server
Installed At	Shillong , PHQ, SCRB
Recommendations	
Continue after CCTNS	NO
▪ "Talaash" module of CAS (Centre) CCTNS would be provided by NCRB.	

d) Motor Vehicle Coordination System (MVCS)	
Objective	Public Service
Description	▪ Record information regarding lost/stolen and recovered vehicles. ▪ Generate certificates for the vehicle (whether involved in crime or not) and various other reports like monthly/yearly reports etc
Technology Used	SQL server
Installed At	SCRB, Shillong
Issues	Not Integrated with other systems
Recommendations	
Continue after CCTNS	NO
▪ CCTNS CAS application would come with the module of Vehicle Registration	

e) Monthly Crime Statistics System	
Objective	Crime Statistical Report
Description	All crimes under different heads starting from IPC crimes, Local and Special Laws, crime against women, crime against children, etc.
Technology Used	DOS Application
Installed At	SCRB,Shillong
Issues	Not Integrated with other system
Recommendations	
Continue after CCTNS	NO
▪ Data from the system should be migrated to the "Periodic Crime and Law and Order Reports and Review Dashboard Service" module of CCTNS.	

f) Crime in Indian Application System (CIA)	
Objective	Crime Statistical Report
Description	This is a 53 page yearly statistics which is being compiled at SCRB it contains information on cognizable crimes, arrested persons, juvenile cases, police housing, police strength, pay, budget etc
Technology Used	DOS Application
Installed At	SCRB, Shillong
Issues	Not Integrated with other system
Recommendations	
Continue after CCTNS	NO

Data from the system should be migrated to the "Periodic Crime and Law and Order Reports and Review Dashboard Service" module of CCTNS.

g) Accidental Deaths & Suicide Information System	
Objective	Recording of accidents and suicides statistics.
Description	This is another yearly report which contains information of unnatural deaths by various causes.
Technology Used	DOS Application
Installed At	SCRB, Shillong
Issues	Not integrated with other systems
Recommendations	
Continue after CCTNS	No
▪ Data from the system should be migrated to the "Periodic Crime and Law and Order Reports and Review Dashboard Service" module of CCTNS.	

h) Fingerprint Analysis & Criminal tracing System	
Description	The application is used for capturing, encoding, storing and matching fingerprints using the image processing and pattern recognition technique.
Technology Used	FACTS application
Installed At	PHQ,Shillong
Issues	System is not installed at all places. Installed only at PHQ. The system is not utilized at its maximum.
Recommendations	
Continue after CCTNS	NO, as newer version AFIS has been proposed to be integrated with the CCTNS

i) Meghalaya Police Department Website	
Description	http://meghpol.nic.in/ is a Web based system designed by NIC Meghalaya Some of the features of the website are like ▪ Crime Statistics ▪ Lookout Notice of Missing Person ▪ Wanted Persons ▪ Alerts and Precautions ▪ Guidelines on Disaster Management ▪ Citizens Charter And others.
Technology Used	Web Based Application
Installed At	Internet base, available wherever internet is available
Issues	▪ Since all police stations does not have internet, there is high probability that not all information on missing objects is available in the system. ▪ No data analysis & data mining on the data has been done as of now. ▪ Not integrated with any other system resulting in duplicate data entry.
Recommendations	
Continue after CCTNS	NO
▪ A new web portal would be developed by System Integrator which would be integrated with the	

CCTNS CAS State Citizen Interface/ Portal.

- The Website would serve as online interface for Citizens with Meghalaya Police department
- The website would have an interface with the "Citizen Portal Service" module under CCTNS.
- No data digitization & migration would be required for this, this would be developed afresh

Note: *Exact details would emerge out of the Detailed System Study by the SI as part of the scope of work under this RFP*

ANNEXURE X: INDICATIVE HARDWARE REQUIREMENTS & SPECIFICATIONS

Enterprise Management and Monitoring Solution (EMS)
Meghalaya State has an Enterprise Management Solution for its SDC, which addresses the following areas:

- Network management comprising of Fault manager
- Performance monitoring for network and Servers
- Application Performance & Traffic Monitoring
- Host level security for servers

Bidders to do a detailed assessment of the existing EMS at state data centre and as part of implementing the monitoring tool for this project, SI is required to procure full use CAL licenses of the existing EMS/ additional modules (if any) with Meghalaya State for this project from the OEM. SI shall be responsible for configuring and integrating the Meghalaya Police sites on the existing EMS. SI shall also be required to provide all the necessary hardware/ software to meet the below mentioned indicative requirements from EMS.

Specification-cum-Compliance Sheet for EMS

Sl No	Specification	Complied (Y/N)	Value Add (If any)/ Remarks
Basic Requirements			
1	Solution should be inclusive with hardware, OS, patches, etc.		
2	Solution should provide for future scalability of the whole system without major architectural changes.		
3	Should be SNMP v1, v2, v3 and MIB-II compliant.		
4	Filtering of events should be possible, with advance sort option based on components, type of message, time etc.		
5	Should support Web / Administration Interface.		
6	Should provide compatibility to standard RDBMS.		
7	Solution should be open, distributed, and scalable and open to third party integration.		
8	Should provide fault and performance management for multi-vendor TCP/IP networks.		
Security			
9	Should be able to provide secured windows based consoles / secured web-based consoles for accessibility to EMS.		
10	Should have web browser interface with user name and Password Authentication.		
11	Administrator/ Manager should have privilege to create/modify/delete user.		
Polling Cycle			
12	Support discriminated polling		
13	Should be able to update device configuration changes such as re-indexing of ports		
Fault Management			
14	Should be able to get fault information in real time and present the same in alarm window with description, affected component, time stamp etc.		
15	Should be able to get fault information from heterogeneous devices — routers, switches, servers etc.		
16	Event related to servers should go to a common enterprise event console where a set of automated tasks can be defined based on the policy.		
17	Should have ability to correlate events across the entire		

Sl No	Specification	Complied (Y/N)	Value Add (If any)/ Remarks
	infrastructure components of DC/DR.		
18	Should support automatic event correlation in order to reduce events occurring in DC/DR.		
19	Should support advanced filtering to eliminate extraneous data / alarms in Web browser and GUI.		
20	Should be configurable to suppress events for key systems/devices that are down for routine maintenance or planned outage.		
21	Should be able to monitor on user-defined thresholds for warning/ critical states and escalate events to event console of enterprise management system.		
22	Should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis.		
23	Should have self-certification capabilities so that it can easily add support for new traps and automatically generate alarms.		
24	Should provide sufficient reports pertaining to asset and change management, alarms and availability of critical network resources as well as network response times for critical links.		
25	The tool shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network and system components. The current performance state of the entire network and system infrastructure shall be visible in an integrated console.		
26	Should provide an integrated performance view for all the managed systems and networks along with the various threshold violations alarms in them. It should be possible to drill-down into the performance view to execute context specific reports		
27	Should provide the following reports for troubleshooting, diagnosis, analysis and resolution purposes: Trend Reports, At-A-Glance Reports, & capacity prediction reports		
28	Should be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits		
Discovery			
29	Should provide accurate discovery of layer 3 and heterogeneous layer 2 switched networks for Ethernet, LAN and Servers etc.		
30	Manual discovery can be done for identified network segment, single or multiple devices.		
Presentation			
31	Should be able to discover links with proper colour status propagation for complete network visualization.		
32	Should support dynamic object collections and auto discovery. The topology of the entire Network should be available in a single map.		
33	Should give user option to create his /or her map based on certain group of devices or region.		
34	Should provide custom visual mapping of L2 and L3 devices connectivity and relationships.		
Agents			
35	Should monitor various operating system parameters such as processors, memory, files, processes, file systems etc. where applicable using agents on the servers to be monitored.		
36	Provide performance threshold configuration for all the agents to be done from a central GUI based console that provide a common look and feel across various platforms in the enterprise. These agents could then dynamically reconfigure them to use these		

Sl No	Specification	Complied (Y/N)	Value Add (If any)/ Remarks
	threshold profiles they receive.		
System Monitoring			
37	Should be able to monitor/manage large heterogeneous systems environment continuously.		
38	Windows OS - Should monitor / manage following: • Event log monitoring • Virtual and physical memory statistics • Paging and swap statistics • Operating system • Memory • Logical disk • Physical disk • Process • Processor • Paging file • IP statistics • ICMP statistics • Network interface traffic • Cache • Active Directory Services • Should be capable of view/start/stop the services on windows servers		
39	Unix OS - Should monitor / manage following: • CPU Utilization, CPU Load Averages • System virtual memory (includes swapping and paging) • Disk Usage • No. of Inodes in each file system • Network interface traffic • Critical System log integration		
Infrastructure Service			
40	IIS / Tomcat / Apache / Web server statistics		
41	HTTP service		
42	HTTPS service		
43	FTP server statistics		
44	POP/ SMTP Services		
45	ICMP services		
46	Database Services – Monitor various critical relational database management system (RDBMS) parameters such as database tables / table spaces, logs etc.		
Application Performance Management			
47	End to end Management of applications (J2EE/.NET based)		
48	Determination of the root cause of performance issues whether inside the Java application in connected back-end systems or at the network layer.		
49	Automatic discovery and monitoring of the web application environment		
50	Ability to monitor applications with a dashboard.		
51	Ability to expose performance of individual SQL statements within problem transactions		
52	Monitoring of third-party applications without any source code change requirements.		
53	Proactive monitoring of all end user transactions; detecting failed transactions; gathering evidence necessary for problem diagnose.		
54	Storage of historical data is for problem diagnosis, trend analysis		

Sl No	Specification	Complied (Y/N)	Value Add (If any)/ Remarks
	etc.		
55	Monitoring of application performance based on transaction type		
56	Ability to identify the potential cause of memory leaks.		
Reporting			
57	Should able to generate reports on predefined / customized hours.		
58	Should be able to present the reports through web and also generate "pdf" / CSV / reports of the same.		
59	Should provide user flexibility to create his /or her custom reports on the basis of time duration, group of elements, custom elements etc.		
60	Should provide information regarding interface utilization and error statistics for physical and logical links.		
61	Should create historical performance and trend analysis for capacity planning.		
62	Should be capable to send the reports through e-mail to pre-defined user with pre-defined interval.		
63	Should have capability to exclude the planned-downtimes or downtime outside SLA.		
64	Should be able to generate all sorts of SLA Reports.		
65	Should be able to generate web-based reports, historical data for the systems and network devices and Near Real Time reports on the local management console.		
66	Should be able to generate the reports for Server, Application, infrastructure services and Network devices in DC/DR environment.		
Availability Reports			
67	Availability and Uptime – Daily, Weekly, Monthly and Yearly Basis		
68	Trend Report		
69	Custom report		
70	MTBF and MTTR reports		
Performance Reports			
71	Device Performance – CPU and Memory utilized		
72	Interface errors		
73	Server and Infrastructure service statistics		
74	Trend report based on Historical Information		
75	Custom report		
76	SLA Reporting		
77	Computation of SLA for entire DC/DR Infrastructure		
78	Automated Daily, Weekly, Monthly, Quarterly and Yearly SLA reports		
Data Collection			
79	For reporting, required RDBMS to be provided with all licenses.		
80	Should have sufficient Storage capacity should to support all reporting data for 5 Years of DC/DR operation.		
Integration			
81	Should be able to receive and process SNMP traps from infrastructure components such as router, switch, servers etc.		
82	Should be able integrate with Helpdesk system for incidents.		
83	Should be able to send e-mail or Mobile –SMS to pre-defined users for pre-defined faults.		
84	Should trigger automated actions based on incoming events / traps. These actions can be automated scripts/batch files.		
Network Management			
85	The Network Management function must monitor performance		

Sl No	Specification	Complied (Y/N)	Value Add (If any)/ Remarks
	across heterogeneous networks from one end of the enterprise to the other.		
86	It should proactively analyze problems to improve network performance.		
87	The Network Management function should create a graphical display of all discovered resources.		
88	The Network Management function should have extensive reporting facility, providing the ability to format and present data in a graphical and tabular display		
89	The Network Management function should collect and analyze the data. Once collected, it should automatically store data gathered by the NMS system in a database. This enterprise-wide data should be easily accessed from a central location and used to help with capacity planning, reporting and analysis.		
90	The Network Management function should also provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment, WAN links and routers.		
91	Alerts should be shown on the Event Management map when thresholds are exceeded and should subsequently be able to inform Network Operations Center (NOC) and notify concerned authority using different methods such as pagers, emails, etc.		
92	It should be able to automatically generate a notification in the event of a link failure to ensure proper handling of link related issues.		
93	The Systems and Distributed Monitoring (Operating Systems) of EMS should be able to monitor: • Processors: Each processor in the system should be monitored for CPU utilization. Current utilization should be compared against user-specified warning and critical thresholds. • File Systems: Each file system should be monitored for the amount of file system space used, which is compared to user-defined warning and critical thresholds. • Log Files: Logs should be monitored to detect faults in the operating system, the communication subsystem and in applications. The function should also analyze the files residing on the host for specified string patterns. • System Processes: The System Management function should provide real-time collection of data from all system processes. This should identify whether or not an important process has stopped unexpectedly. Critical processes should be automatically restarted using the System Management function. • Memory: The System Management function should monitor memory utilization and available swap space. • Event Log: User-defined events in the security, system, and application event logs must be monitored.		
SLA Monitoring			
94	The SLA Monitoring function of the EMS is by far the most important requirement of the DC/DR Project. The SLA Monitoring component of EMS will have to possess the following capabilities: • EMS should integrate with the application software component of portal software that measures performance of system against the following SLA parameters: ▪ Response times of Portal;		

Sl No	Specification	Complied (Y/N)	Value Add (If any)/ Remarks
	▪ Uptime of data centre; ▪ Meantime for restoration of Data Centre etc; • EMS should compile the performance statistics from all the IT systems involved and compute the average of the parameters over a quarter, and compare it with the SLA metrics laid down in the RFP. • The EMS should compute the weighted average score of the SLA metrics and arrive at the quarterly service charges payable to the Agency after applying the system of penalties and rewards. • The SLA monitoring component of the EMS should be under the control of the authority that is nominated to the mutual agreement of Director, the partner so as to ensure that it is in a trusted environment. • The SLA monitoring component of the EMS should be subject to random third party audit to vouchsafe its accuracy, reliability and integrity.		
Reporting			
95	The Reporting and Analysis tool should provide a ready-to-use view into the wealth of data gathered by Management system and service management tools. It should consolidate data from all the relevant modules and transform it into easily accessible business-relevant information. This information, should be presented in a variety of graphical formats can be viewed interactively		
96	The tool should allow customers to explore the real-time data in a variety of methods and patterns and then produce reports to analyze the associated business and service affecting issues.		
97	The presentation of reports should be in an easy to analyze graphical form enabling the administrator to put up easily summarized reports to the management for quick action (Customizable Reports). The software should be capable of supporting the needs to custom make some of the reports as per the needs of the organization.		
98	Provide Historical Data Analysis: The software should be able to provide a time snapshot of the required information as well as the period analysis of the same in order to help in projecting the demand for bandwidth in the future.		
ITIL Based Help Desk System			
99	Helpdesk system would automatically generate the incident tickets and log the call. Such calls are forwarded to the desired system support personnel deputed by the Implementation Agency. These personnel would look into the problem, diagnose and isolate such faults and resolve the issues timely. The helpdesk system would be having necessary workflow for transparent, smoother and cordial DC/DR support framework.		
100	The Helpdesk system should provide flexibility of logging incident manually via windows GUI and web interface.		
101	The web interface console of the incident tracking system would allow viewing, updating and closing of incident tickets.		
102	The trouble-ticket should be generated for each complaint and given to asset owner immediately as well as part of email.		
103	Helpdesk system should allow detailed multiple levels/tiers of categorization on the type of security incident being logged.		
104	It should provide classification to differentiate the criticality of the security incident via the priority levels, severity levels and impact levels.		

Sl No	Specification	Complied (Y/N)	Value Add (If any)/ Remarks
105	It should allow SLA to be associated with a ticket based on priority, severity, incident type, requestor, asset, location or group individually as well as collectively.		
106	It should maintain the SLA for each item/service. The system should be able to generate report on the SLA violation or regular SLA compliance levels.		
107	It should be possible to sort requests based on how close are the requests to violate their defined SLA's.		
108	It should support multiple time zones and work shifts for SLA & automatic ticket assignment.		
109	It should allow the helpdesk administrator to define escalation policy, with multiple levels & notification, through easy to use window GUI / console.		
110	System should provide a knowledge base to store history of useful incident resolution.		
111	It should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.		
112	The web-based knowledge tool would allow users to access his / her knowledge article for quick references.		
113	It should provide functionality to add / remove a knowledge base solution based on prior approval from the concerned authorities		
114	Provide seamless integration to generate events/incident automatically from NMS / EMS.		
115	Each incident could be able to associate multiple activity logs entries manually or automatically events / incidents from other security tools or EMS / NMS.		
116	Allow categorization on the type of incident being logged.		
117	Provide audit logs and reports to track the updating of each incident ticket.		
118	Proposed incident tracking system would be ITIL compliant.		
119	It should be possible to do any customizations or policy updates in flash with zero or very minimal coding or down time.		
120	It should integrate with Enterprise Management System event management and support automatic problem registration, based on predefined policies.		
121	It should be able to log and escalate user interactions and requests.		
122	It should support tracking of SLA (service level agreements) for call requests within the help desk through service types.		
123	It should be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and should support notification and escalation over email, web etc.		
124	It should provide status of registered calls to end-users over email and through web.		
125	The solution should provide web based administration so that the same can be performed from anywhere.		
126	It should have a customized Management Dashboard for senior executives with live reports from helpdesk database.		

NOTE: EMS tools deployed shall have the ability to manage the entire IT infrastructure proposed by the SI

Storage and Backup Solution

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
SAN Switch				
1	Switch should be configured with redundant power supply and fans			
2	Switch solution should be highly available with no single point of failure			
3	The SAN fabric should be configured in highly available solution with no single point of failure			
4	Should support 4 Gbps FC ports			
5	Selection of SAN switch should be done in such way that, after configuring integration, storage server and backup, there are minimum 40% ports free with switch and it should have capability to upgrade to 100%			
6	The switch shall support role based administration by allowing different administrators different access rights to switch. There should be head room of 100% for port expansion (on top of being proposed for the solution) at a future date by state government within the same chassis or different chassis			
7	The SAN switch should have capability to interface with HBA of different makes and model from multiple OEM, supporting multiple OS including, but not limited to HP-UX, IBM AIX, Linux, MS-Window, Sun Solaris etc. The SAN switch should support all leading SAN disk array and tape libraries including, but not limited to, EMC, Hitachi, HP, IBM Sun etc.			
SAN				
1	RAID Controller: It should support various levels of RAID (RAID 0, 1 etc.)			
2	The storage subsystem proposed should have no single point of failure with respect to controller, cache, disks, power supply and cooling			
3	It should disrupt non-disruptive component replacement of controllers, disk drives, cache, power supply, fan subsystem etc.			
4	The storage array or subsystem shall support ATA/SATA/FATA and FC disks etc.			
5	Storage subsystem shall support 300GB 15K RPM disks and 400GB or higher 10 K RPM Fiber channel drives & 750GB, 1TB SATA or higher SATA / equivalent drives in the same device array			
6	Storage subsystem shall support global hot spare or universal hot spare disks			
7	The storage array shall be configured with at least 8 GB cache scalable to min 16 GB useable and mirrored/protected across two storage controllers for disk I/O operations			
8	It shall support non disruptive online micro code upgrades			
9	It shall support de-staging of cache to disks on power down or shall support internal battery backup of cache for at least 48 hours. The data in cache shall not be lost in case of power failure			

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
10	System should be configured with necessary multi-pathing and load balancing components for high availability			
11	The design shall provide provision for LUN masking and SAN security			
12	The Storage shall support Point-in-time copy and full volume copy for heterogeneous storage arrays. The licenses configured should be one time for the entire storage device and no incremental license should be charged at the time of capacity upgrade. It should support these operations from storage of one OEM to storage from another OEM.			
13	The storage architecture shall have 1+1 active or active –passive storage controllers and mirrored cache, with no single point of failure			
14	Each storage controller shall support minimum 4 front-end FC port and 4 backend FC ports. Each fiber channel shall support minimum 4 Gbps rated BW			
15	The storage array should support latest Operating System Platforms & Clustering including: CISC/RISC/EPIC – based servers running Microsoft, HP, IBM, Sun, Linux etc.			
16	The storage shall support the following high availability cluster solution from HP, IBM, Symantec, EMC, SUN and Windows			
17	The storage shall support and configure with storage based point-in-time copy and full volume copy			
18	The storage system shall be configured with GUI based management software as below. - Monitor and manage the storage array - Configuring PITs - Remote storage base replication - Storage front end monitoring - Disk monitoring - LUN Management - Storage component replacement etc.			
19	Should provision for LUN masking, fibre zoning and SAN security.			
20	To meet interoperability requirements, the Storage arrays shall support data replication in both synchronous and asynchronous modes across heterogeneous storage arrays from different OEMs.			
21	The storage should be configured with 10 TB 146 GB 15 K RPM FC disks, 10 TB with 300 GB 15 K RPM FC disks and 10 TB with 500 GB or higher 15 K RPM SATA drives.			
22	SI should factor Storage Operating System disk and Global Hot spare disks as an addition to the RAW capacity mentioned			
23	Licenses for software (Storage Array Management, Point-in-Time copy, Volume copy, multipathing software for host) should be provided as part of the solution			
24	The storage sub system should replicate to DR site			

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
	using FCIP protocol			
25	Storage solution shall factor 1 hot spare disk for every 25 disk used in storage subsystem, unless required or otherwise specified in solution			
26	Load balancing must be controlled by system management software tools			
27	Multi-path & Load balancing software for all SAN connected servers shall be provided. The multi-path software should not only support the supplied storage and Operating systems but should also support heterogeneous storage and operating systems from different OEMs.			
28	Any other Specification			
Tape Library				
1	Tape drives: 4 x LTO 4/ LTO 5 FC drives scalable to minimum 15			
2	Interface: Fiber Channel Interface			
3	Should have sufficient speed backup to Tape Library in High Availability for backing up data from the SAN without any user intervention.			
4	Should be able to backup 100% of the entire production landscape in 8 hours window			
5	Should support LTO-4 or latest technology based library with at least 4 LTO-4 tape drives (>=4), rack mountable with redundant power supplies.			
6	Cartridges should have native capacity of 800 GB or more per cartridge.			
7	At least 50 LTO 4 Media Cartridges with 2 Cleaning Cartridges, Barcode labels shall also be provided			
Archival Software				
1	The software shall support defined policies that are based on a variety of standard file attributes such as age of file / last access time.			
2	The software shall set high and low watermark levels for purging data from high performance storage based upon a percentage of disk space in use.			
3	The software shall keep active data on host arrays while inactive or compliance data is automatically moved to disk or tape.			
4	The software shall support truncated stub files to point to migrated data, enabling seamless file access regardless of location of the data			
5	Shall enable back-ups at disk speed, while dramatically decreasing recovery times.			
6	Shall offer a single logical view of both active and inactive data regardless of where it is physically located			
7	Shall eliminate repeated backups of the same archived data			
8	OS support: Microsoft® Windows Server 2008, Enterprise Edition / Red Hat® Enterprise Linux 5 AS / SUSE® Linux Enterprise Server 9 / Unix			
9	Metadata / Archival servers shall be offered in cluster, Min 2 Node cluster shall be offered based on Industry Standard Servers with 2 x Dual Core			

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
	Intel CPU , Min 8 GB of RAM , 2 x DC HBA's (4 Gbps) , 4 x NIC Ports on each node.			
10	Any other Specification			
Back-up Software				
1	The proposed Backup Solution should be available on various OS platforms such as Windows, Linux and UNIX platforms and be capable of supporting SAN based backup / restore from various platforms including UNIX, Linux, and Windows.			
2	Proposed backup solution shall be offered with cluster client license to take the back up of clustered servers in the setup			
3	Proposed backup solution shall have same GUI across heterogeneous platform to ensure easy administration.			
4	The proposed backup solution should allow creating tape clone facility after the backup process.			
5	The proposed Backup Solution has in-built frequency and calendar based scheduling system and high availability			
6	The proposed backup Solution supports the capability to write multiple data streams to a single tape device or multiple tape devices in parallel from multiple clients to leverage the throughput of the Drives using Multiplexing technology.			
7	The proposed backup solution support de-multiplexing of data cartridge to another set of cartridge for selective set of data for faster restores operation to client/servers			
8	The proposed backup solution should be capable of taking back up of SAN environment as well as LAN based backup.			
9	The proposed back up solution shall be offered with 25 Client licenses for SAN based back up and 50 client licenses for LAN based backup.			
10	The proposed solution also supports advanced Disk staging.			
11	The proposed Backup Solution has in-built media management and supports cross platform Device & Media sharing in SAN environment. It provides a centralized scratched pool thus ensuring backups never fail for media.			
12	Backup Software is able to rebuild the Backup Database/Catalog from tapes in the event of catalog loss/corruption.			
13	The proposed Backup Software shall offer OPEN File Support for Windows, Linux based servers.			
14	The proposed Backup Solution has online backup solution for different type of Databases such as Oracle, MS SQL, Sybase, MYSQL, Post GRE SQL etc. on various OS.			
15	The Proposed backup solution shall provide granularity of single file restore.			
16	The Proposed backup solution shall be designed in such a fashion so that every client/server in a SAN can share the robotic tape library.			

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
17	Backup Solution shall be able to copy data across firewall.			
18	Backup solution should also provide report writer that allows designing of report templates which can be used to generate meaningful reports in CSV / HTML / XML / Text format / PDF.			
19	Any other			

Note: Backup Policy

- Full snapshot backup of database and application executables done per day onto the SAN that would be transferred to tape library
- The backup schedule would be as follows

Day	Type of backup
Sunday	Full backup
Monday and Tuesday	Differential backup
Wednesday	Full backup
Thursday, Friday and Saturday	Differential backup

- Apart from this, weekly backup, monthly backup, half-yearly backup and annual backup needs to be taken
- Two copies of tapes to be taken during backup
    - 1 copy in local fire-proof cabinet and another copy at a distance of 50 Km from the site
- SI would be responsible for transportation of tapes to the secure location and get receipt confirmation from Meghalaya Police that all tapes have been received at the remote location

Specification-cum-Compliance Sheet for Database & Application Servers

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
1	64 bit processors with 2.6GHz or above with a minimum of 4 processor or higher with 4 core or more per each processor			
2	Processor: Processor should be latest series/generation for the server model and Support should be available for a minimum period of 5 years (The SI should provide Certificate from the OEM in this regards)			
3	Operating System: Support for 64bit Windows/ Linux / UNIX Operating System as applicable (as per the proposed stack), with cluster support			
4	Memory: Minimum 24 GB ECC or equivalent RAM of highest frequency as applicable in the quoted model to be offered per processor. Memory should support RAID and memory mirroring. Memory scalable to 256 GB			
5	Cache: Total Cache to be min 8 MB per processor socket			
6	Min 2 x 300 GB (or higher) SAS / FC hot plug drives for operating system (10 K / 15 K rpm) for each partition in RAID 0,1 combinations with provision of mirroring OS and provision of maintaining data for certain specific applications			
7	Ethernet Ports of minimum 10/100/1000 Mbps. 4 Nos USB 2.0 compliant ports			

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
8	Fiber Channel Adapters 2 x minimum 4GBps			
9	SAN HBAs should be connected on separate slots for high throughput requirements			
10	All cards should be on 64 bit PCI-X/PCI-e slots.			
11	25% of total slots should be free for future expansion. Alternatively, vendors should not consume more than 75% of available slots in the server. (The SI should give duly signed (by the person who is authorized to sign the bid document)and sealed declaration)			
12	1 DVD (preferably RW-DL) Drive ;			
13	Power: Minimum Dual Redundant Power Supply Hot Pluggable			
14	The Server chassis should be fitted with HS fan modules fully loaded			
15	Logical or Physical Partitioning should be supported;			
16	Server should support virtualization.			
17	Capable of dynamic movement of resources (CPU/ memory/ adapters) across partitions;			
18	Should be provided with a GUI based management console to take care of the partition management & configuration;			
19	The server should be capable of generating pre-failure alerts for CPU, memory, harddisks. It should also provide HS Fans failure indications.			
20	The Server quoted must conform to all relevant international standards like FCC, UL etc			
21	Necessary software and scripts for automatic cluster failover and load balancing within cluster to be supplied for cluster based solutions.			
22	It should have seamless failover without manual intervention; Management of the OS and the partitions (if required) in the Servers; A console with color monitor, keyboard and Mouse			
23	System Management: Local System Management and Control. It must enable complete access, monitoring and control from console. Required hardware and software must be supplied.			
24	Form Factor: 19” rack mountable with rack mounting accessories			
25	The Volume Manager and File System on the server should support heterogeneous storage models from different OEMs			
26	Preloaded Software (Full and Perpetual use by Meghalaya Police) • Operating System • Office Suite • Anti Virus (if any) • Any other (As per SI Proposal)			
27	The system software must provide perpetual & full use licenses.			
28	For Database cluster, the clustering software should support heterogeneous Operating systems from different OEMs.			
29	The applicable system software for RDBMS must			

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
	provide all the administration tools, notification services, Enterprise reporting services, business intelligence, analysis services, and high availability and management tools at no additional cost			

Specification-cum-Compliance Sheet for Web Server, Management Server etc

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
1	Minimum 1x Quad core processor with 2.4GHz or above with 1066Mhz FSB / 2000 MT /s with min 2MB L2 cache per processor. Processor should be latest series/generation for the server model being quoted			
2	Operating System: Support for 64bit Windows/ Linux / UNIX Operating System (Latest Version) as applicable (as per the proposed stack), with cluster support			
3	Memory (RAM): Minimum 24 GB ECC or equivalent RAM of highest frequency as applicable in the quoted model to be offered per processor. Memory should support RAID and memory mirroring. Memory should be scalable to 256 GB			
4	RAID controller with RAID 0/1/5 with 512 MB cache			
5	HDD: 2 x 300 GB 2.5" 10 K RPM HDD or more			
6	Disk bays: Support for min 8 small form factor hot plug SAS / SCSI hard drives in disk drive carriers that slides out from front			
7	Atleast 2 x 10/100/1000 Mbps Ethernet ports or more			
8	2 x 4 Gbps Fiber Channel Ports			
9	Ports Rear: Two USB ports (Ver 2.0); RJ-45 Ethernet; keyboard and mouse; two RJ-45 Ethernet; / no parallel port Front: One USB (Ver 2.0)			
10	Graphics controller: SVGA / PCI bus / ATI® ES 1000 / min 16MB SDRAM std/max / 1280x1024 at 16M colors			
11	Optical / diskette: 8X / 24X slim-line DVD ROM drive			
12	Security: Power-on password / admin password / unattended boot / selectable boot / boot without keyboard			
13	Cooling fans: minimum Four fans / multispeed / hot-swap and redundant fan failure signals to management module / fan in each power supply / CPU / memory			
14	Power supplies: Hot plug redundant AC power supply			
15	Management feature to identify failed components even when server is switched off			
16	It should provide Secure Sockets Layer (SSL) 128 bit encryption and Secure Shell (SSH) Version 2 and support VPN for secure access over internet.			
17	Should be able to manage systems through a web-browser			

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
18	Should be provided with a GUI based management console to take care of the partition management & configuration;			
19	Form Factor: Rack mountable (with accessories as applicable)/ Blade*			
20	Preloaded Software (Full and Perpetual use by Meghalaya Police) • Operating System • Office Suite • Anti Virus (if any) • Any other (As per SI Proposal)			
21	It should have seamless failover without manual intervention; Management of the OS and the partitions (if required) in the Servers; A console with color monitor, keyboard and Mouse			
22	System Management: Local System Management and Control. It must enable complete access, monitoring and control from console. Required hardware and software must be supplied			

* In case the Bidder proposes the Blade Server, the Bidder must provide 1 quantity of Blade Chasis complying to the minimum specification as below at no additional cost to Meghalaya Police

Specification-cum-Compliance Sheet for Blade Chasis

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
1	Single blade chassis should accommodate minimum 6 (Quad core Processor) / 8 (Dual core Processor) or higher hot pluggable blades.			
3	6U to 12U Rack-mountable			
4	Dual network connectivity for each blade server for redundancy should be provided. Backplane should be completely passive device. If it is active, dual backplane should be provided for redundancy			
5	Should accommodate Intel, AMD, RISC / EPIC Processor based Blade Servers for future applications			
6	Should have the capability for installing industry standard flavours of Windows, Linux, Unix, Solaris for x86 Operating Environments			
7	Single console for all blades in the enclosure or KVM Module			
8	DVD ROM can be internal or external, which can be shared by all the blades allowing remote installation of S/W and OS			
9	Minimum 2 external USB connections functionality			
10	Two hot-plug, redundant 1Gbps Ethernet module with minimum 8 ports (cumulative), which enable connectivity to Ethernet via switch. Switch should be (Internal/external) having Layer 2/3 functionality			
11	Two hot-plugs/hot-swap redundant 4 Gbps Fiber Channel for connectivity to the external Fiber channel Switch and ultimately to the storage device			
12	Power Supplies • Hot Swap redundant power supplies to be			

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
	provided • Power supplies should have N+N. All Power Supplies modules should be populated in the chassis			
13	Hot Swappable and redundant Cooling Unit			
14	Management • Systems Management and deployment tools to aid in Blade Server configuration and OS deployment, • Remote management capabilities through internet browser • It should provide Secure Sockets Layer (SSL) 128 bit encryption and Secure Shell (SSH) Version 2 and support VPN for secure access over internet. • Ability to measure power historically for servers or group of servers for optimum power usage • Blade enclosure should have provision to connect to display console / central console for local management like trouble shooting, configuration, system status / health display			
15	Built in KVM switch or Virtual KVM feature over IP.			
16	Dedicated management network port should have separate path for management			
17	Support heterogeneous environment: AMD, Xeon and RISC/EPIC CPU blades must be in same chassis with scope to run Win2003/2008 Server, Red Hat Linux / 64 Bit UNIX, Suse Linux / 64 Bit UNIX / Solaris x86			

Software for Data Center & DR Center

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

The SI shall also provide services for software license management and control. SI shall maintain data regarding entitlement for software updates, enhancements, refreshes, replacements, and maintenance. SI should perform periodic audits to measure license compliance against the number of valid end user software licenses consistent with the terms and conditions of site license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions and report to Meghalaya Police.

All the software licenses should be in the name of DGP, Meghalaya.

All Operating system, database and other software licenses for DC and DR shall be genuine, perpetual, full use and should provide patches, bug fixes, security patches and updates directly from the respective developer / manufacturer for the contract period. The CAS application will be implemented at various police locations from where various departmental users will access the Core Application Software on approximately 500 desktop computers.

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

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

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

The bidder shall provide with a full use of database license during the project period for unrestricted users. Database should have received the security certification such as International common criteria for information technology security evaluation. Database should also support industry standard TCP benchmark. The database software should provide the following capabilities:

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

Specification-cum-Compliance Sheet for Desktop PCs

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
1	Processor: • Multicore, x86 CPU 2.6 GHz clock frequency or higher • Spec_CPU_rate_base 2006 min. 50 (Avg. of Spec_int_rate_base & Spec_fp_rate_base) • CPU should be available for next 5 years i.e. the OEM will guarantee against product obsolescence for next 5 years			
2	On Chip Cache: 2 MB or Higher			
3	Motherboard: OEM Motherboard			
4	Chip Set: Processor OEM Chipset with integrated SATA controller and audio controller			
5	HDD: 250 GB – Serial ATA - 7200 rpm (150 Mbps data transfer rate) HDD or higher			
6	Optical Drive: DVD R/W			
7	Key Board: PS/2 Type OEM Keyboard with 104 keys			
8	Monitor: 17" or higher TFT monitor should be of same make and color as the base PC			
9	LAN: 10/100 Ethernet with Wake on LAN feature			
10	Mouse: 2 button optical scroll mouse (USB or PS/2)			
11	Chasis: ATX cabinet with Minimum 300 watts ATX vers 2.2 Power supply (compatible version to the motherboard PCB) with fan			
12	I/O Port: Minimum 6 USB 2.0 (at least 2 ports should be mounted in the front), PS/2 ports, 1 RJ-45 port, Video, Audio			
13	OS: Windows/ Linux/ Unix (as per the proposed solution stack of the SI). OS Certification: The SI must provide the latest Certification of the OS proposed			
14	Accessories: Necessary accessories like Power cord etc. Operating documentation / Manuals			
15	Certifications: • Relevant FCC & UL certification mandatory, Energystar, • TCO and • other necessary certifications OEM must possess ISO 9001:2000 & ISO 14001 (for product range offered) [If called for bidder have to produce valid FCC part 15 & UL certificate for the particular model/configuration of PC offered]			
16	Preloaded Software (Full and Perpetual use by Meghalaya Police) • Operating System • Office Suite • Anti Virus (if any) • Any other (As per SI Proposal)			
17	Security: 1. Removable media boot control, 2. Serial, Parallel & USB Interface Control 3. Power-On Password, 4. Setup Password,			

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
18	Warranty: 3 years onsite comprehensive warranty support.			

Specification-cum-Compliance Sheet for Anti Virus Solution

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
1	Unified protection - from viruses, spyware, and other current integrated through one client agent			
2	Simplified administration - through central management to protect the infrastructure with greater efficiency			
3	Visibility and control - through insightful, prioritized security reports and a summary dashboard view, which enable administrator for visibility and control over malware threats			
4	Infrastructure Integration Capabilities • All Data must be stored Centrally in proposed Database Server and Reporting should be provided			
5	Malware Filtering Capabilities • Should support Integrated anti-virus/anti-spyware agent delivering real-time protection • Should support Static analysis and code emulation for addressing threats • Should support Event Flood Protection • Should support Integrated and Single foot printed State Assessment Scans to detect Vulnerabilities • Should support In-depth scanning of unknown malware by Dynamic Translation			

6	Manageability
	• The Solution Should support Centralized Monitoring of the integrated anti-malware engine, security state assessment technologies and policies alerts, and reports
	• Should support in-built Reporting for Below Items :
	  • Deployment Status: Number of machines up to date or not up to date with the latest signatures
	  • Top issues and issue history: Information about the top issues in their environment categorized by type along with the history of issues over time
	  • Top Threats and threat history: List of top threats, their severity and number of machines impacted. Should provide info on current status and trends
	  • Top vulnerabilities and vulnerability history: Through security state assessment checks, admin should be able to see the top vulnerabilities as well as history of vulnerabilities over time. The admin should also be alert to measure the security risk			

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
	profile based on security best practices • Top alerts and alert history: Should support Information about the key alerts impacting their environment (with the ability to drill down into more information), along with the history of alerts over time • It should be capable of providing customized alerts based on incidents and assets			

Specification-cum-Compliance Sheet for Line Interactive UPS - 2 KVA with 120 min back up

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
1	Type : Line-interactive			
2	Capacity: 2 KVA/10 KVA as per the Bill of Material			
3	Back up: 120 minutes as per the Bill of Material			
4	Input Voltage Range: 140 – 280 V AC			
5	Input Frequency: 50 Hz +/-10%			
6	Output Voltage: 220 V +/- 10%			
7	Output Frequency: 50 Hz +/- 0.5 Hz (under battery mode)			
8	Noise: < 40 db at 1 m			
9	Protection: Low Battery, Overcharge			
10	AVR: Built in Automatic Voltage Regulator (AVR)			
11	Indicators: LED indicators for AC Mains, DC, Load on Mains/Battery			
12	Battery Type & back-up time: Batteries shall be inbuilt Sealed Maintenance Free (SMF) type. The system must be capable of providing 30 minutes battery back-up time as per VAH rating below : (Minimum VAH for 30 minutes back-up = 504 VAH) Total number of batteries, Voltage of each battery, Ampere-Hour rating of each battery offered to be specified.			
13	Ambient Conditions: Temperature: 0 to 40 deg Celsius **Humidity**: upto 95%			
14	Quality Certification: UPS OEM should be ISO 9001:2008 certified			

Specification-cum-Compliance Sheet for Duplex laser printer

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
1	**Print technology:** Monochrome Laser			
2	**Print speed:** > 15 ppm			
3	**Processor speed:** 266 MHz			
4	**Print Resolution:** Up to 1200 x 1200 dpi			
5	**Duty cycle (monthly, A4):** > 5000 copies			
6	**Media types supported:** Plain paper, envelopes, transparencies, cardstock, postcards, labels			

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
7	**Duplex print options:** Manual (driver support provided)			
8	**Usable Media weights:** Main tray: 60 to 160 g/m			
9	**Memory**: 8 MB or higher			
10	**System Interface:** Hi-Speed USB 2.0 port (compatible with USB 2.0 specifications)			
11	**Compatible operating systems:** Microsoft® Windows® VISTA/Linux			
12	**Operating temperature range:** 10 to 30º C			
13	**Energy Star certified:** Yes			

Specification-cum-Compliance Sheet for Multi-Function Laser

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
Printer				
1	High-speed printing, up to 15ppm			
2	Black-and-white: up to 35ppm (draft);			
3	Duty Cycle: Up to 15,000 pages per month			
4	Automatic two-sided printing			
5	250-sheet input tray			
6	Print, scan and copy unattended with the Automatic Document feeder, enhanced print permanence.			
7	Capable of installation, configuring, monitoring and troubleshooting in the network, from anywhere on the network			
Scanner				
1	Flatbed with automatic document feed			
2	Upto 4800 dpi; Enhanced upto 19200 dpi			
3	Scan size maximum (flatbed): 216 x 356 mm (8.5 x 14 inches),			
4	Front panel scan (scan to application)			
Copier				
1	Black-white colour-Upto 1200x600 dpi			
2	Copy speed (black, draft quality, A4):Up to 35 cpm			
3	Copy resolution (black graphics): Up to 1200 x 600 dpi,			
4	Copier resize: 25 to 400%			
5	Maximum number of copies: Up to 99			
6	Copier smart software features: Up to 99 multiple copies			
7	Reduce/enlarge from 25 to 400%			
8	2-up or 4-up allowing 2 or 4 pages to be copied onto 1 page			

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
9	Contrast (lighter/darker), resolution (copy quality), tray select, collate, margin, shift			

Specification-cum-Compliance Sheet for Generator Set: 2 KVA Generator Set

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
General Features				
1	The proposed DG set should be able to support the Police Unit equipments along with AC, in absence of primary power source.			
2	Engine shall be vertical multi cylinder 4 stroke type in accordance with IS 10002-1981 with latest amendments.			
3	Type: Multi cylinder			
4	Method of starting: Electric start 12 V DC			
5	Type of cooling: Water cooled /Air cooled			
6	Type of governor: Mechanical/Electronic			
7	Type of fuel: High speed diesel			
8	Rating: Continuous			
9	Output: Suitable HP rated to match the alternator			
10	Rated speed: 1500 RPM			
11	Over load capacity: 10% overload – minimum 1 hour, 50% overload – minimum 1 minute			
12	DG set shall be compliant with the latest CPCB emission & noise norms (less than 75db at 1 meter distance).			
Accessories				
1	Flywheel to suitable diameter and fuel injection equipment			
2	Air cleaner			
3	Lubricating oil cooler			
4	Electric motor starting equipment like motor, battery, charging generator with voltage regulator etc.			
5	Heavy duty radiator with fan			
6	Residential type silencer with exhaust piping with vibration isolator			
7	Fuel tank suitable for 8 Hrs of continuous running with necessary piping and fuel gauge, drain valve, inlet and outlet connections.			
8	Anti vibration mounting pads (Dunlop)			
9	Speed controlling governor			
10	Suitable coupling system to the Alternator			
11	Tachometer			
12	Lubricating oil pressure gauge			

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
13	Hour meter to indicate number of Hrs of operation			
14	Auto trip on low oil pressure			
15	Over speed alarm with trip			
16	Thermal insulation for exhaust line with glass wool, Aluminium sheet, chicken mesh, Diesel line 12 mm dia including beads flanger etc			
17	Battery 12 V with lead and terminal			
18	Battery charger.			
19	Protection: Protection against low lubricating oil pressure, high water temperature and over speed shall be provided for engine with alarm and fuel shut off.			

Specification-cum-Compliance Sheet for Finger Print Reader

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
Standards				
1	The Finger Print Reader should be Forensic grade and should be PIV (Personal Identification and Verification) standards compliant			
Fingerprint Sensor				
1	▪ Scanner: Optical sensor			
2	▪ Resolution: 500 dpi at 256-bit (416 X 416 pixels)			
3	▪ Platen Area: 0.83 in x 0.83 in (21 mm x 21 mm)			
4	▪ Distortion: <1%			
Biometric Matching				
1	▪ Authentication: <1 second (including detection, encoding and matching)			
2	▪ Identification: <2 seconds in 1:3000 mode (including detection, encoding and matching)			
3	▪ False Acceptance Ratio (FAR): 1 in 10,000 or better, configurable based on security specifications			
Interfaces				
1	▪ Standard USB			
Environment				
1	▪ Temperature: 0° C to 50° C			
2	▪ ESD Protection: 15 KV			
Format Supported				
1	▪ AANSI/ INCITS 378,			
2	▪ ISO 19794-2			

Specification-cum-Compliance Sheet for Electornic Pen

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
1	Average battery life: Min. 2.5 hours continuous writing use			
2	Average usage life:150,000 hours			
3	Approximate battery recharge time: 2 hours			
4	Battery type: Lithium-ion polymer rechargeable battery			
5	Standard connectivity: USB 1.1 (also called High Speed USB 2.0)			
6	Humidity non-operating: 0 to 95% RH (excluding rain, non-operating)			
7	Humidity range: 0 to 95% RH (excluding rain)			
8	Humiditiy recommended operating range: 0 to 90% RH (non-condensing, operating)			
9	Operating temperature maximum**:** 104°F			
10	Operating temperature recommended range: 32 to 104°F			
11	Storage temperature range: -4 to 104°F			
12	Storage life: Up to 5 years			
13	Image compression: Pattern images to X, Y coordinate samples with relative time of capture			
14	Image processing rate**:** 75 Hz			
15	Image resolution**:** Atleast 500 dpi			
16	Image scaling: Perspective, rotation, tilt, and error correction			
17	Languages supported: English and Hindi			
18	Internal fixed memory: Atleast 10 MB (1.3 MB available for user strokes)			

Specification-cum-Compliance Sheet for Digital Camera

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
Basic Features				
1	Atleast 14 Mega Pixels			
2	Sensor Type 1/2.3 Super HAD CCD			
3	Optical Zoom: 4x			
4	Precision Digital Zoom: 8x			
5	Lens: Carl Zeiss Vario-Tessar or equivalent			
6	F Number 2.7 - 5.7			
7	Auto Focus Range (W: Approx. 4cm to Infinity, T: Approx. 60cm to Infinity)			
8	Compatible Recording Media Memory Stick Duo / Memory Stick PRO Duo / Memory Stick PRO Duo (High Speed) / Memory Stick PRO-HG Duo / SD Memory Card / SDHC Memory Card			
9	LCD: 2.7 (6.9 cm) (230K pixels), Clear Photo LCD			

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
10	Battery Life: 240 shots or 120mins			
11	Battery System: Lithium ION Battery			
12	USB 2.0 Hi-Speed			
Main Features				
1	Photo Mode Intelligent Auto, Easy Shooting, Program Auto, Steady Shot			
2	Scene Selection Twilight / Twilight Portrait / Landscape / Soft Snap / Snow / Beach / High Sensitivity / Underwater / Gourmet / Pet			
3	Still Image Size 14M 4,320 x 3,240			
4	Still Image Size 16:9 Mode 11M(4,320 x 2,432) / 2M(1,920 x 1,080)			
5	Movie Recording Mode (QVGA) 320 x 240, 29.97fps			
6	Movie Recording Mode (VGA) 640 x 480, 29.97fps			
7	Movie Recording Time Up to 2GB per shoot			
8	Recording Format Motion JPEG / AVI			
9	Still Image Recording Mode Normal (JPEG) / Burst (JPEG)			
10	ISO Sensitivity Setting Auto / 80 / 100 / 200 / 400 / 800 / 1600 / 3200			
11	Image Stabilizer Steady Shot			
12	Focus Mode Multi-point AF (9 points) / Center-weighted AF / Spot AF			
13	Auto Focus Mode Intelligent			
14	Exposure Compensation Plus / Minus 2.0EV, 1 / 3EV step			
15	White Balance Auto / Daylight / Cloudy / Fluorescent / Incandescent / Flash			
16	Underwater White Balance Auto / Underwater 1-2			
17	Light Metering Multi-Pattern / Center Weighted / Spot			
18	Flash Mode Auto, Flash On, Flash Off, Slow Synchro			
19	Flash Range ISO Auto: Approx. 0.3 - 3.5m (W) / 0.6 - 1.8m (T), ISO3200: up to Approx. 7.1m (W) / 3.7m (T)			
20	Pre-flash			
21	Auto Daylight Syncro			
22	Dynamic Range Optimiser Standard / Off / Plus			
23	Face Detection			
24	Red-eye Reduction			
25	Clear RAW NR (Noise Reduction)			
User Interface				
1	Self-Timer (10sec / 2sec / off)			
2	Auto Review			

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
3	Index Playback			
4	Playback Moving Image Mode (QVGA / VGA)			
5	Slide Show Playback (SD)			
6	Image Rotation / Divide (MPEG) / Cue & Review			
7	Hand Shake Alert			
8	LCD Brightness Setting			
9	Speaker Volume Control			
10	Internal Memory Full Data Copy (to Memory Stick)			
11	Multi-use Terminal			
12	USB Connecting Auto / Mass Storage			

Specification-cum-Compliance Sheet for 16-Port/24-Port Managed switch

Sl No	Specification	Complied (Y/N)	Reference to Data Sheet	Value Add (If any)/ Remarks
General Features				
1	No of Switch Ports: 16/24			
2	MAC Address Table Size: 8K			
3	Switch Fabric: 3.2Gbps Forwarding Capacity			
4	Transmission Method:Store-and-Forward			
5	**Diagnostic LEDs** ▪ Per Device: Power ▪ Per Port: Link/Activity ▪ Duplex/ Collision Speed			
6	**Packet Buffer Memory:** 160KBytes Buffer Memory per Device			
7	**QoS:** 802.1p			
Interface Options				
1	**RJ-45:** RJ-45, 10BASE-T, 100BASE-TX Universal UTP Cable Recognition for Straight-through or Crossover cables			
Network Protocols and Standards				
1	**IEEE:** 802.3 10BASE-T Ethernet, 802.3u 100BASE-TX Fast Ethernet, 802.3x Flow Control, 802.3 Nway Auto-negotiation, 802.1p QoS			

* Please Note: Only Number of Ports per Switch will change. Please Note: Only Number of Ports per Switch will change

UTP & Structured Cabling:

The cabling material shall be supplied, laid tested and commissioned in accordance with specifications and site requirements. -
All the cabling shall run through PVC conduit / Casing Capping of suitable size of ISI standard. -
Separate PVC conduits or Casing Capping shall be used for electrical and data cabling. -
Laying of Cables- Cables shall be laid by skilled and experienced workmen using adequate equipments to minimize stretching of the cable. -

All terminations should be carried out according to the manufacturer's instructions and guidelines and standards of generic cabling systems. When terminating outlets, care must be taken to avoid damaging the copper cores when stripping back the outer sheathing.
Testing and Documentation: Testing of each node should be done as per manufacturer standards and the final report should be submitted.

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

Specification-cum-Compliance Sheet:

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

Cat-6 Patch Cord (1-Meter)

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

Specification-cum-Compliance Sheet:

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

Cat - 6 Patch Cord (2 Meters Length)

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

Specification-cum-Compliance Sheet:

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

Specification-cum-Compliance Sheet for Furniture required

Sl No	Specification	Complied (Y/N)	Value Add (If any)/ Remarks
Computer Table (Size: L 910 x W 610 x H 728 mm)			
1	Top: Size 910 x 610 mm made of 18 mm thick pre laminated medium density fiber (MDF) board ISI Marked (IS: 14587-1998). The top shall be firmly screwed on 25x25x1 mm square tube frame as shown in figure.		
2	Upper side of laminated board shall be in natural teak shade while the bottom side shall be white/cream shade.		
3	Sliding key Board tray: A Sliding key Board tray shall be made of 18mm pre laminated medium density fiber board of size 725x450 mm. The gap between top and tray shall be 100mm. Key board tray shall slide smoothly on sliding channel duly powder coated having nylon roller arrangement.		
4	The storage shelve for CVT : A storage shelve made of 18 mm particle board shall be provided along with the length of the table at bottom about 100 mm above from the ground level. Shelves shall be screwed on frame work of 25x25x1 mm square tube. The shelve shall be covered from back side with 18mm pre laminated medium density fiber board as shown in drawing.		
5	Steel Structure: The rigid steel structure shall consist of two nos. rectangular base tubes of size 50x25x1.25 mm about 520 mm length placed along the width on vertical tubes of size 25x25x1 mm shall be welded for fixing up of side panels. A supporting frame of 25x25x1 mm square tube shall be welded on the top of the tubes for the side panels as shown for supporting the top of the table.		
6	The base tube shall be provided with adjustable shoes 2 nos. on each side.		

Sl No	Specification	Complied (Y/N)	Value Add (If any)/ Remarks
7	Painting: Complete frame of tubes shall be powder coated.		
Printer Table (Size: L 610 x W 610 x H 660 mm)			
1	Shelves : 3 no. made of 18mm thick pre laminated Medium Density Fiber Board(MDF) ISI marked (IS 14587 – 1998)		
2	Top shelve size 610x610 mm for placing printing unit.		
3	Middle Shelve size 460x330 mm for placing feet on stationary.		
4	Bottom shelve size 460x380 mm for collecting print out.		
5	The top faces of the shelve shall be natural teak wood shade.		
6	The bottom faces shall be in plain white/cream shades.		
7	Structure: The structure shall be made from square and rectangular steel tubes duly welded finished and powder coated.		
8	The horizontal tube 25x25x1 mm thick 330 m long shall be welded over vertical tubes 25 mm off the center width /depth wise.		
9	Panels made of 18 mm pre laminated particle board shall be screwed rigidly between vertical tubes on both sides.		
10	Two nos. bottom support tubes 50x25x1.25mm thick shall also be provided with two nos. of adjustment shoes.		
11	A rectangular slot of size 455x25 mm shall be provided on top shelve along with length for feeding stationary as shown in figure. A slot shall be covered with PVC insertion for safely of paper.		
12	The ends of bottom and top shall be plugged with PVC/ plastic caps.		
13	Painting: Complete steel structure shall be pretreated and powder coated with minimum thickness of 60 microns coating.		
Computer Chair with Handle			
1	Seat size shall be 430x430 mm on 10 mm. thick molded comm. ply with 60 mm thick 40 density molded PU foam		
2	Back rest size shall be 400x300 mm on 10 mm thick molded comm. ply with 40 mm thick 32 density molded PU foam covered with tapestry.		
3	The height of back rest shall be 900x500 mm for top and bottom edges respectively. The black rest shall be provided with lifting arrangement on flat iron & helical spring.		

Sl No	Specification	Complied (Y/N)	Value Add (If any)/ Remarks
4	Two nos. suitable PU handles shall be provided.		
5	The base stand should be made up of 5 prongs duly pressed welded together centrally with a pedestal bush with good quality twin wheel castors. The stand and other metal parts excluding central spindle shall be powder coated. Complete steel structure shall be pretreated and powder coated with minimum thickness of 60 microns coating.		
6	A central spindle of 25mm dia rod without threads shall be provided with revolving arrangements. The adjustable height of chair shall be from 530 to 570 mm.		
7	A good quality tapestry cloth shall be provided on seat & back in attractive color/ shade.		