E-GOVERNANCE MISSION MODE PROJECT (MMP)

CRIME & CRIMINAL TRACKING NETWORK AND SYSTEM (CCTNS)

REQUEST FOR PROPOSAL

FOR

SELECTION OF SYSTEM INTEGRATOR FOR

IMPLEMENTATION OF CCTNS

IN ODISHA

VOLUME – I: FUNCTIONAL AND TECHNICAL SPECIFICATIONS

DEPARTMENT OF HOME, GOVERNMENT OF ODISHA

Table of Contents

List of Tables

List of Figures

Abbreviations

Table 1 Abbreviation

Sr. No.	Abbreviation	Description
1.	ASI	Assistant Sub Inspector
2.	ASP	Assistant Superintendent of Police
3.	CAS	Core Application Software
4.	CCIS	Crime and Criminals Information System
5.	CCTNS	Crime and Criminal Tracking Networking and Systems
6.	CIPA	Common Integrated Police Application
7.	CPMU	Central Project Management Unit
8.	DC	District Collector
9.	DCRB	District Crime Record Bureau
10.	DGP	Director General of Police
11.	DIG	Deputy Inspector General
12.	DPO	District Police Office
13.	DSR	Daily Status Report
14.	FCR	Fortnightly Crime Report
15.	FIR	First Information Report
16.	FSL	Forensic Science Laboratory
17.	GoO	Government of Odisha
18.	HC	Head Constable
19.	IG	Inspector General
20.	IIC	Inspector In charge
21.	IO	Investigating Officer
22.	IOC	Officer In charge
23.	IPC	Indian Penal Code
24.	IT	Information Technology
25.	MMP	Mission Mode Project
26.	NCRB	National Crime Record Bureau
27.	NIC	Nation Informatics Centre
28.	NOC	No Objection Certificate
29.	OIC	Officer In charge
30.	PCR	Police Control Room
31.	POC	Place of Occurrence
32.	PS	Police Station
33.	RPF	Request for Proposal
34.	RPO	Regional Passport Office
35.	SAP	Special Armed Police
36.	SC/ST	Scheduled Caste/Scheduled Tribe
37.	SCRB	State Crime Record Bureau
38.	SDPO	Sub Divisional Police Officer

Sr. No.	Abbreviation	Description
39.	SI	System Integrator
40.	SP	Superintendent of Police
41.	SPA	State Police Academy
42.	SPMC	State Project Management Consultants
43.	SR	Special Report
44.	SWAN	State Wide Area Network
45.	U/S	Under Section

1. PROJECT INTRODUCTION

1.1 CCTNS 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.*

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).

1.1.1 Crime and Criminal Information System (CCIS)

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

CCIS is primarily an initiative to create crime- and criminals-related database that can be used for crime monitoring by monitoring agencies such as National Crime Records Bureau (NCRB), State Crime Records Bureaus (SCRB) and District Crime Records Bureaus (DCRBs) 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 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).

However, CCIS focuses exclusively in Crime and Criminals information and does not address the other aspects of Police functioning. CCIS software was more an application designed for supervisory officers at the office of the Superintendent of Police and above and, was not meant for the usage at Police Stations level. This was not designed to capture the SHD (Station House Diary) routine, which is a mandatory requirement at the police station and other tasks. Even after improvements in the software of CCIS made during 2001-02 which enabled Multi-lingual support with web-based interface, it still did not cater to the requirements of the Police Station applications.

1.1.2 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.

Common Integrated Police Application (CIPA) started in the year 2004 after a detailed study thereof by a Subgroup of domain and technical experts. The pilot project was launched in Delhi in 2005. Computer hardware, software and technical assistance were provided to police stations. 20% police stations have been covered under CIPA wherein, at present, FIRs are being registered digitally and some events relating to investigations are also being captured. 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. 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.

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

Over a period of time, at one level, it was felt that, at this pace, it would take many years before all police stations could be covered and, at another level, that a stand-alone system of this nature would have very limited utility.

1.1.3 Need for CCTNS

Keeping these aspects in mind, it was decided that there is a need for expanding the functional applications, widening the territorial spread, and building in networking capabilities in the system, both from the angle of Management Information Systems (MIS) requirements and storage, collation, analysis and transmission/sharing of crime and criminals related information at the police station, District, State and Central levels. In this background, the Crime and Criminal Tracking Network and Systems (CCTNS) Scheme was conceived and incorporated in the Eleventh Five Year Plan.

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. 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. **CCTNS has been conceptualized in response to the need for establishing a comprehensive e-Governance system in police stations across the country.**

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 enhancing outcomes in the areas of Crime Investigation and detection of Criminals; in information gathering and its dissemination among various police organizations and units across the country and in enhancing Citizen Services.

1.2 Overview of CCTNS

CCTNS aims at creating a comprehensive and integrated system for enhancing the efficiency and effectiveness of policing through adoption of principles of e-Governance and creation of a nationwide networking infrastructure for evolution of IT-enabled-state-of-the-art tracking system around 'investigation of crime and detection of criminals.' It aims to create infrastructure and mechanism to provide the basis for evolution of an IT enabled state-of-the art workflow (Processes) automation system in a planned manner from Police Station level upwards and also provide public service delivery systems. It will not only automate police functions at police station and higher levels but will also create facilities and mechanism to provide public services like registration of online complaints, ascertaining the status of case registered at the police station, verification of persons etc.

CCTNS will cover all the Police Stations in the States/UTs, and also the Circle offices, Sub-Divisions, District headquarters, Range headquarters, Zonal IG offices and State/UT headquarters. Necessary Hardware will be provided at all these locations including data centers at State/UT and National headquarters. All these locations will be networked by providing appropriate high-speed connectivity for data transfer and sharing of information amongst various stakeholders.

1.3 Vision and Objectives of CCTNS

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

The broad objectives of the project are as follows:

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

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

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

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

1.4 Desired Outcomes of CCTNS

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

a) **Benefits to Citizens**

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

b) **Benefits to Police Department**

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

vii. Enhanced tools to optimize resource allocation for patrols, emergency response, petition enquiries, and other general duties
viii. A collaborative knowledge-oriented environment where knowledge is shared across the different regions and units
ix. Better coordination and communication with external stakeholders through implementation of electronic information exchange systems

c) Benefits to Ministry of Home Affairs (NCRB)

i. Standardized means of capturing the crime and criminal data across the police stations in the country
ii. Faster and easier access to crime and criminal information across the country in a manner amenable for trend and pattern analysis
iii. Enhanced ability to detect crime patterns and modus operandi across the states and communicate to the state police departments for aiding in crime prevention
iv. The ability to respond faster and with greater accuracy to inquiries from the parliament, citizens and citizens groups; and to RTI queries.

1.5 Background of Police Systems in Odisha

Several initiatives have been introduced in the past in Odisha State Police 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). This section explores the details of the initiatives in Odisha.

1.5.1 Crime and Criminals Information System (CCIS)

CCIS was launched in Odisha in the year 1994 in Odisha. CCIS is a Headquarter based application. Currently, it is being used in DCRBs. The data collected in different DCRB offices are shared with SCRB using CDs and pen drives. It is like many of the applications implemented in the state which are stand-alone. The data from this will need to be migrated to CCTNS.

1.5.2 Common Integrated Police Application (CIPA)

Odisha witnessed Phase I CIPA implementation in the year 2007. It was implemented in a total of 45 police stations in the State. A dedicated CIPA operator had been assigned at each of the Police Stations where the application was commissioned. The CIPA Operator was trained on CIPA Software. The data from this will need to be migrated to CCTNS.

1.6 Goals of this Request for Proposal (RFP)

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

a) To seek proposals from potential bidders for providing the “bundle of services” in implementing and managing the CCTNS solution in the State.
b) To understand from the bidders how they propose to meet the technical and operational requirements of CCTNS.

c) To ascertain how potential bidders propose to deliver the services and sustain the demand and growth in the requirements.
d) To ascertain from bidders on how they will ensure scalability and upgradeability of the infrastructure and solution proposed to be deployed.
e) To understand from the bidders as to how they intend to innovate further on this service delivery model.

Odisha Police shall be the final authority with respect to qualifying a bidder through this RFP. The decision with regard to the choice of the System Integrator (SI) who qualifies through this RFP shall be final and the department reserves the right to reject any or all the bids without assigning any reason. The department 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.

1.7 RFP Issuing Authority

This Request for Proposal (RFP) is issued by the Odisha Police.

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

Table 2 Details of RFP issuing authority

Sr. No.	Item	Descriptions
1.	**Project Title**	E-Governance Mission Mode Project on Crime & Criminal Tracking Network and Systems for Odisha Police
2.	**Project Initiator Details**	Director, State Crime Records Bureau, Government of Odisha
3.	**Department**	State Crime Records Bureau
4.	**Contact Person**	Director (State Crime Records Bureau), IG of Police (Computer, Odisha) & Nodal Officer (CCTNS Project, Bhubaneswar).
5.	**Contact Details**	State Crime Records Bureau, Rasulgarh, Bhubaneswar - 751010 **Phone**: 0674-2580110 **Mobile**: +91-9437015487 **Fax**: 0674-2587234 **Email**: scrborissa@gmail.com

1.8 Governance Structure

For Details of Governance structure refer to Annexure 1

1.9 Structure of the RFP

The Request for Proposal or RFP (this document) for selection of State System Integrator (SI) is segregated into the following three volumes:

Volume I – Functional & Technical Specifications

'Volume I' provides Introduction to the Project, and the Scope of Services required from the State System Integrator.

Volume II – Commercial & Bidding Terms

'Volume II' details the General Terms & Conditions with respect to the bid process management including bid submission forms to be adopted for the proposed project.

Volume III – Contractual & Legal Specifications

'Volume III', Contractual and Legal Requirements for the proposed engagement, outlines the contractual, legal terms & conditions applicable for the proposed engagement.

This is the Volume I of the RFP.

2. IMPLEMENTATION FRAMEWORK FOR CCTNS PROJECT

CCTNS would be implemented in a way where the State will 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. However, the State would drive the planning and implementation of the project at the State level.

The role of the Centre (MHA and NCRB) focuses primarily around planning, providing the Core Application Software (CAS) which is to be configured, customized, enhanced and deployed in States, managing and monitoring the program at a higher level. 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.

In line with "bundling of services" concept, Odisha will select one System Integrator (SI) who would be the single point of contact for the Odisha Police for all the components of CCTNS. These components include the customization of Application (the changes made to the core application provided by MHA), hardware and associated services such as operation and maintenance, Capacity Building and Handholding, etc. Following broad level services are to be provided by the System Integrator:-

- Program Planning and Management
- Configuration, Customization and Extension of CAS State and integration with CAS Center and External Agencies
- Site preparation at Police Station and Higher offices
- Infrastructure ate Client locations
- IT infrastructure at the Data Center and Disaster Recovery Center
- Data migration and data digitization
- Migration of CIPA and CCIS Police Stations / Higher offices to CCTNS
- Design, execution and management of Change Management Plan for project
- Capacity Building
- Handholding support
- Adherence to standards

3. CORE APPLICATION SOFTWARE (CAS)

The CCTNS application software will contain a "core" for the States that is common across all 35. States and UTs. The CCTNS Core Application Software (henceforth referred to as CAS) will be developed at NCRB premises and provided to States and UTs for deployment. Each State 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.

The Core application Software (CAS) is expected to be ready by July 2011 (tentative).

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

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

CAS (Center)

CAS (Centre) would cater to the functionality that is required at the GoI level (by MHA and NCRB). CAS (Centre) would enable NCRB to receive crime and criminals' related data from States 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 is needed 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.

Table 3 Overview of CAS(Centre)

Overview of Services for CAS (Center)
i) State-SCRB-NCRB Data Transfer and Management
The service shall enable the NCRB to receive, transform, and collate the crime, criminal, and related data from States/UTs, to organize it suitably to serve NCRB requirements.
ii) Crime and Criminal Reports
The service shall enable authorized personnel to generate the reports and perform analysis on the central crime, criminals, and related data repository of the nation.
iii) Crime and Criminal Records and Query Management
The service shall enable the authorized personnel to view various registers and perform basic and advanced queries on the central crime, criminals, and related data repository of the nation.
iv) *Talaash* Service
The service will enable the user to search for missing persons across a central/ national database.
v) Person of Interest
The service will enable the user to search for persons of interest such as persons wanted on outstanding warrants, accused, charged habitual offenders, convicts, etc. across the national database.

Overview of Services for CAS (Center)
vi) Registered Vehicle and Vehicle of Interest Service
The service will enable the user to search for registered vehicles and vehicles of interest such as, missing / stolen vehicles, abandoned / unclaimed vehicles, and vehicles involved in traffic incidents across the national database.
vii) Publication Service
This functionality will help the NCRB to publish the periodic crime reviews to the NCRB portal.
viii) NCRB Citizen Interface
The service shall enable the citizens to access/ search the NCRB National Database on the data (ex, Stolen Vehicles / Property, Missing Persons, etc.) that is approved to be made accessible to public.
ix) NCRB Interface for RTI
Due to the sensitivity of the information that pertains to national security and harmony, this service shall enable a limited and restricted access to the authorized external stakeholders to search the NCRB National Database, upon submission of any RTI requests.

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 State 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, that helps police personnel (playing different roles) in more effectively performing their core functions and that relieves police personnel from repetitive tasks that claim much of their time while returning low or no value.

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

- It will lay special emphasis on the functions at police stations with focus on usability and ease of use of the application.
- It will be designed to provide clear and tangible value to key roles at the Police Station: specifically the SHO (Station House Officer), the IO (Investigation Officer) and the Station Writer.
- It will be event and role-driven.
- It will be content/forms-based, with customized forms based on requirements.
- It will be a flexible application 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 , thus 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.
- It will provide the ability to view and exchange information amongst Police Stations, between Police Stations and other Police formations and with external entities including citizens.
- It will ensure that relevant 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.
- It will ensure central facilitation and coordination; however CAS (State) will be primarily driven and owned by States where States can configure and customize the CAS for their unique requirements without the intervention of the central entity

Table 4 Overview of CAS(State)

Overview of Services in CAS (STATE)
i. Citizens Portal Service
This service shall enable Citizens to request services from Police through online petitions and track status of registered petitions and requests online. Citizens requests/services include passport verification services, general service petitions such as No Objection Certificate (NOC) for job, NOC for vehicle theft, NOC for lost cell phone/passport, Licenses for arms, processions etc.
ii. Petition Management Service
The service shall enable the police personnel to register and process the different kinds of general service petitions and complaints.
iii. Unclaimed / Abandon Property Register Service
The service shall enable the police personnel to record and maintain unclaimed/abandoned property registers and match unclaimed/ abandoned property with property in lost/stolen registers.
iv. Complaint and FIR Management Service
The service shall enable the police personnel to register and process the complaints (FIR for cognizable complaints, Non-Cognizable Report for non-cognizable, Complaint Report for genera complaints, etc.) reported by the public.
v. PCR Call Interface and Management Service
The service shall enable the police personnel to register and process the complaints as received through the Police Control Room through the Dial 100 emergency contact number.
vi. Investigation Management Service
The service shall enable the police personnel to process the complaints through capturing the details collected during the investigation process that are required for the investigation officer to prepare a final report.
vii. Court and Jail Interface and Prosecution Management Service
The service shall enable the police personnel to interface with the courts and jails during the investigation process (for producing evidence, producing arrested, remand etc.) and during the trial process.
viii. Crime and Criminal Records and Query Management Service
The service shall enable the police personnel to view various registers and perform basic and advanced queries on the crime and criminal information.
ix. Police Email and Messaging Service
The service shall enable the police personnel to send / receive official as well as personal correspondence.
x. Periodic Crime, Law and 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.

Overview of Services in CAS (STATE)
xi. Notification of Alerts, Important Events, Reminders and Activity Calendar or Task Services
The service shall capture / generate the required alerts, important events, reminders, activity calendar and tasks.
xii. State-SCRB-NCRB Data Transfer and Management Service
The service shall enable the States to collate, transform and transfer the crime, criminal, and other related data from state to NCRB.
xiii. State CAS Administration and Configuration Management Service
The service shall enable the individual State to configure/ customize the application to suit to their unique requirements.
xiv. User Help and Assistance Service
The service shall enable the end user to view the help manuals of the application and in guiding the end user in using the application.
xv. User Feedback Tracking and Resolution Service
The service shall enable the police personnel in logging the issues/defects occurred while using the system.
xvi. Activity Log Tracking and Audit Service
The service shall capture the audit trail resulting from execution of a business process or system function.
xvii. User Access and Authorization Management Service
The service shall enable the administrative user in setting the access privileges and will provide authentication and authorization functionality

DEVELOPMENT OF CCTNS CORE APPLICATION SOFTWARE (CAS)

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

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

In order to achieve the above stated goals of simultaneously ensuring consistency and standardization across States (where necessary and possible), and enabling States 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 and deployed in all States.

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.

TECHNOLOGY STACK FOR CAS (STATE) AND CAS (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 an Annexure 2 to this RFP. The SI is expected to bid with one of the technology stacks in response to this RFP. SI shall procure all necessary underlying solution components required to deploy CAS (State) solution for the State Annexure 2.

ROLE OF SOFTWARE DEVELOPING 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:

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

Each of these activities is detailed out below:

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

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

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

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

- Appropriate communication on change required has taken place.
- Proper approvals have been received from CAS Core Group/CTT/CPMU.
- 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 hand over the certified CAS (State) to States through NCRB. While NCRB will facilitate the transfer, the successful transfer of CAS to States on time is SDA's responsibility. During the period of CAS Solution Design and Development and the Operations and Maintenance phase following that, the SDA shall provide technical program management services in implementing CAS in States. Through the Technical Program Management, the SDA shall extend all the necessary support to the State SI and ensure that the SI successfully configures, customizes and deploys CAS (State) in States. 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; 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 tuning, 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/artifact (including configuration utilities / tools, deployment scripts to SIs to deploy CAS (State) in States)
  - 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 Points of Contact:** Members of the SDA's team shall act as points of contacts for the State level SIs. The number of States 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' needs).
- **Helpdesk Support:** SDA shall provide Helpdesk support to the State SIs during customization, deployment and stabilization phases with 8 contact hours (during normal business hours of 10 AM to 6 PM), 6 days (Monday through Saturday, both included). The SDA shall deploy a team of at least 5 qualified and certified resources in NCRB to address the questions from the SIs.
- **Deployment Scripts:** The SDA shall develop the necessary deployment scripts to deploy CAS (State) in States and provide the same to State SIs.
- **Data Migration Utility:** The SDA shall develop a Data Migration Utility/application with all the formats and tools to load the data into the State databases. This will be provided to States and will enable the SIs to migrate data from legacy/paper based systems to the CAS databases.
- **Language Localization Support:** Proving interface in local languages is a key requirement of CAS (State). The SDA shall build CAS (State) with interfaces in English and Hindi; and also build CAS (State) in such a way that it can be configured for interfaces in other local languages at the State

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

- **Supporting the SI** to ensure that the CAS (State) that is configured and customized by the SI in the State successfully passes the User Acceptance Testing (UAT) milestone.
  - Configuration of CAS (State)
  - Customization of CAS (State)
  - Data Migration of CAS (State) related data from the legacy systems and / or manual records to CAS (State)
  - Infrastructure Sizing related to CAS (State)
  - Commissioning and Deployment of CAS (State)
  - Infrastructure Environment Performance Tuning 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.

4. GEOGRAPHICAL SCOPE OF THE PROJECT

Odisha Police is the law enforcement agency of the government of Odisha in India. Odisha Police was formed on April 1st, 1936. Odisha Police has 9 ranges. Each range is constituted by 3-5 Districts. There are total 36 Police District in the State. In each district the head of the Police is the Superintendent of Police. In discharge of his duties he is assisted by Additional Superintendents of Police (Addl. S.P.), Deputy Superintendents of Police (Dy. S.P.). . The number of Addl. S.Ps and Dy. SPs varies with the size, population, police work or nature of police work in different districts

4.1 Offices to be Covered Under CCTNS Implementation

CCTNS will cover 780 locations in Odisha State including State Police Head Quarters, Range headquarters, and District headquarters, District Police Stations, Sub Divisional Police Offices, Assistant Commissioner of Police offices & Deputy Commissioner of Police Offices, State Crime Records Bureau, Training Centres and all Police Station, Crime Branch, Human Right Protection Cell, State Forensic Science Laboratories, District Control Room, State Control Room and Finger Print Bureau

Refer Annexure 4:

a) Organisation Structure of Police Department
b) Functional Units/ Wings within Police Department at State Police Head Quarters, and typical Commissionerate along with a brief description of Functional wing
c) List of SDPO and Police Stations across the State
d) District wise list of Police Stations located in Remote/inaccessible areas with no power/ difficult in terms of availability of power

Offices to be covered under CCTNS implementation

Table 5 Offices to be covered

Sr. No.	Districts in Phase I	No. of Offices
1.	STATE POLICE HEAD QUARTER	1
2.	Commissioners Office	1
3.	RANGE Offices	9
4.	District HQs	36
5.	Sub Divisional Police Offices (SDPO)	96
6.	Assistant Commissioner of Police offices & Deputy Commissioner of Police Offices	16
7.	State Crime Records Bureau (SCRB)	1
8.	Crime Branch	1
9.	Human Rights Protection Cell (HRPC)	1
10.	State Forensic Science Laboratories (SFSL)	1
11.	Police Stations	579

Sr. No.	Districts in Phase I	No. of Offices
12.	District Control Room	36
13.	State Control Room	1
14.	Finger Print Bureau (FPB)	1

District Wise list of Police Stations

Table 6 District wise list of Police Stations

Sr. No.	Districts	No. of PS
1.	Cuttack District	18
2.	Jagatsinghpur	13
3.	Jajpur	19
4.	Kendrapara	13
5.	Puri	23
6.	Natagarh	13
7.	Khurda	9
8.	Balasore	23
9.	Bhadrak	15
10.	Mayurbhanj	32
11.	Ganjam	24
12.	Gajapati	11
13.	Boudh	7
14.	Berhampur Police District	12
15.	Kandhmal	18
16.	Kalahandi	15
17.	Nuapada	7
18.	Rayagada	17
19.	Malkangiri	12
20.	Nabarangpur	13
21.	Koraput	24
22.	Bargarh	16
23.	Jharsuguda	11
24.	Sambalpur	23
25.	Bolangir	14
26.	Sonepur	9
27.	Deogarh	5
28.	Dhenkanal	15
29.	Angul	23

Sr. No.	Districts	No. of PS
30.	Sundergarh	15
31.	Keonjhar	25
32.	Rourkela	26
33.	RAILWAY POLICE, CUTTACK	6
34.	RAILWAY POLICE, ROURKELA	8
35.	COMMISSIONERATE, BHUBANESWAR	23
36.	COMMISSIONERATE, CUTTACK	22

5. SCOPE OF SERVICES DURING IMPLEMENTATION PHASE

The scope of the "bundled services" to be offered by the SI to rollout CCTNS across the State of Odisha includes the following:

a) Project planning and management
b) Configuration, Enhancements and Extension to CAS (State)
   i. Systems Study and assessment
   ii. Design and Implementation of enhancements and extensions of CAS (State) including Citizen Portal and integration with CAS (Center)
   iii. Design and Implementation of advanced/ additional Functionality I(Human Resource Management Services, Extremist Management System, Coastal Security Requirement and Traffic management and e-challaning) Enhancements to CAS (State) Software such as SMS Gateway
   iv. Continuous Improvement of CAS (State) Application
c) Data Migration/ Digitization of historical Data
d) Site preparation, commissioning, operationalization of IT infrastructure of District Training Center and Regional Training Centre
e) Site Preparation and Procurement, Delivery, Commissioning of IT Infrastructure at Police Stations and Higher Offices
f) Capacity building and Change Management
g) Co-ordination and management of network connectivity
h) Setup and management of IT infrastructure at the Data Center and Disaster Recovery Center
i) Handholding Support
j) Support to 3rd party acceptance testing, audit, and certification
k) Post Implementation (Operational and Maintenance) Services covering the following:
   i. Software maintenance and support services (including Maintenance of Current CAS (State) Software and Release Management of subsequent versions) for CAS (State) application to meet the desired Service Levels
   ii. Application functional support services
   iii. Warranty support for all the new hardware procured as part of this RFP
   iv. AMC support for Hardware
   v. Annual Technical Support (ATS) for all the licensed software
   vi. Operations and maintenance services for the server and related infrastructure supplied and commissioned by the SI for the application at the Data Center and Disaster Recovery Center
   vii. Central Helpdesk from the STATE designated premises
l) Exit Management and Transition at the end of Contract Period

The project will be managed out of State Nodal Officer's Office. At all points in the execution of the project, key senior resources including the Project Manager must be based out of State Nodal Officer's office. In implementing the above, the SI shall strictly adhere to the guidelines set by the MHA, NCRB, and State.

5.1 Project planning and management

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

Project Management Office

The SI shall setup a Project Management Office (PMO) to manage the implementation and rollout of the CCTNS project in Odisha. The requirements of the PMO are provided below:

a. The PMO will be an operational PMO which shall provide oversight and management of the all activities, take implementation decisions, research best practices and provide guidance & co-ordination to all stakeholders.
b. The PMO shall be the primary vehicle for communication between Odisha Police and SI and partners or sub-contractors if any.
c. The PMO shall follow an industry standard of Project Management e.g. PMBOK or PRINCE2
d. One of the objectives of the PMO would be to train the staff of Odisha Police in project management methodologies through short courses and hands-on experience.
e. The PMO shall be effectively transition to Odisha Police upon completion of various contracts for continued growth, management and operation of CCTNS project and other projects.
f. The PMO be staffed by members of the State Project Management Unit (SPMU), members from Odisha Police and members of the SI team.
g. Senior level personnel of the SI shall operate as part of the PMO.

Scope of Project Management Activities

As part of the Project Management, SI shall be responsible for the following:

a. Create an organized set of activities for the project with activities, timelines and resource plans.
b. Coordinate and collaborate with all stakeholders including the PMO, Odisha Police, SPMU, CPMU and the SDA at Center
c. Establish and measure resource assignments and responsibilities
d. Construct a project plan schedule including milestones
e. Measure project baseline, deviations, deadlines, budget figures, and performance objectives.
f. Communicate the project plan to stakeholders with meaningful reports
g. Detect problems and inconsistencies in the plan and take corrective actions
h. During the project implementation, the SI shall report to the PMO and the State Nodal Officer, on following items:
    i. Results accomplished during the period;
    ii. Cumulative deviations to date from schedule of progress on milestones as specified in this RFP, the agreement and 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 PMO, Project Director, Governing Body and / or actions to be taken by the Project Director before the next reporting period
i. Progress reports on a fortnightly basis.
j. Project quality assurance reports.
k. Change control mechanism.
l. Issue Management to identify and track the issues that need attention and resolution from the State.

m. Scope Management to manage the scope and changes through a formal management and approval process.

n. Risk Management to identify and manage the risks that can hinder the project progress.

The Project plan prepared by the SI would be reviewed by the PMO, Project Director, and CCTNS Governance Committees in Odisha and approved by the Apex / Empowered Committee on the advice of the State Mission Team and State Project Management Unit.

The SI would update and maintain the Project Plan throughout the duration of the engagement. All changes are to be reviewed and approved by the Odisha Police/ SCRB and may require approval of MHA/ NCRB.

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/ PMO in the State.

a. State Mission Team/ PMO would also approve any changes required to these documents during the course of the project.

b. State will finally sign-off on the documents on the recommendation of State Mission Team / SPMU / Empowered Committee.

c. Where necessary, the SI shall update the documentation based on changes and submit a new version of the document to SCRB.

d. All project documents are to be submitted in bound hardcopy and in a softcopy/ CD format for archival by SCRB.

e. All project documents shall have a version number and major changes from the last submission shall be highlighted in the beginning of the revised documents.

f. Documents and all artefacts generated by the project shall be kept in revision/ version controlled system with released documents accessible to Odisha Police and working documents (read-only) accessible to PMO / SCRB.

g. Project documents include but are not limited to the following:
   i. Detailed Project Plan
   ii. Updated/vetted FRS
   iii. SRS document
   iv. CAS Configuration Plan
   v. HLD documents (including but not limited to)
      - Application architecture documents
      - Use Cases
      - 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.
   vi. LLD documents (including but not limited to)
      - Application flows and logic including pseudo code

- GUI design (screen design, navigation, etc.)
- CAS Customization design document

vii. All Test Plans
viii. Requirements Traceability Matrix
ix. Change Request Management and Capacity Building Plans
x. SLA and Performance Monitoring Plan
xi. Training and Knowledge Transfer Plans
xii. Issue Logs

h. 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 the State prior to its use for deliverables.

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

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

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

Procurement, Commissioning and Maintenance of Project Management, Configuration Management and Issue Tracker Tools at SCRB, Bhubaneswar

Project Management Tool: 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:

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

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

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

The SI shall procure and commission the required infrastructure (software, servers) for *Project Management Tool, Configuration Management Tool* and *Issue Tracker* tool and maintain the same through the duration of the project. These tools along with the servers on which they are deployed will become property of the Odisha Police and will be used by the State even beyond the contract period.

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

Compliance with Industry Standards

Wherever feasible, any enhancement/ feature addition shall 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 minimize/ avoid any technology or technology provider lock-in.

In addition to above, the proposed solution has to be based on and be 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.

Table 7 Specifications

Sr. No.	Items	Specifications
1.	Portal development	W3C specifications
2.	Information access/transfer protocols	SOAP, HTTP/HTTPS
3.	Interoperability	Web Services, Open standards;
4.	Photograph	JPEG (minimum resolution of 640 x 480 pixels)
5.	Scanned documents	TIFF (Resolution of 600 X 600 dpi)
6.	Biometric framework	BioAPI 2.0 (ISO/IEC 19784-1:2005) specificatio
7.	Finger print image and Minutiae Standard	ISO/IEC 19794-4:2005(E) & ISO 19794-2:2005(E
8.	Digital signature	DSS Standards (RSA, DSA)
9.	Document encryption	PKCS specifications
10.	Information Security	CCTNS system to be ISO 27001 certified
11.	IT Infrastructure management	ITIL / EITM specifications
12.	Service Managements	ISO 20000 specifications
13.	Project Documentation	IEEE/ISO specifications for documentation

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

5.2 Configuration, customization, and extension (new modules) of CAS (State) and integration with CAS (Center)

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/UTs. This includes core functions in the areas of Complaints/ Case Management, Police Station Efficiency and Analysis & Reporting. 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 States/UTs and deployed in all States/UTs. SI would be responsible for adding the functionality over and above the CAS (State) as provided in the Annexure 5

CAS (State) contains functionality that is common across all States/UTs. 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/UTs and facilitate the exchange of crime and criminals related information between States/UTs and the Centre and between States/UTs, NCRB would develop, own and maintain the CAS. The services that will be provided by the Software Development Agency (SDA) for the CAS (State) are articulated in Annexure 5

The details of the CCTNS Core Application Software, CAS (State) and CAS (Center) including the overview of the functionality and architecture are provided as Annexure 5 to this RFP. The Functional Requirements and System Requirement Specification of CAS (State) and CAS (Center) are provided as Annexure 5 to this RFP.

Scope of Enhancements and Extensions to CAS (State)

a) Configuration of CAS (State). The collection and validation of the data required for the configuration of the CAS (State) shall be the responsibility of the SI. The SI shall configure CAS (State) to the requirements of the State that include but not limited to:
   i. Developing Local Language Interfaces and Support
   ii. Configuring users
   iii. Configuring Police Stations / Higher Offices
   iv. Configuration of the UI as required by the State
   v. Configuration of the workflows as required by the State
   vi. Configuration of additional State and Local Laws as per Odisha State Requirements
b) Detailed Configuration and customization requirements as provided in the Annexure 5
c) Design and Implementation of enhancements and extensions of CAS (State) including State Specific Registers, State Specific Reports, Citizen Portal and integration with CAS (Center) as provided in Annexure 5 to this RFP
d) Design and Implementation of Additional Functionality Enhancements to CAS (State) Software such as Knowledge Repository and SMS Gateway as provided in the Annexure 5 to this RFP.
e) Continuous Improvement of CAS (State) Application

The SI shall conduct a detailed Systems Study before the design of the enhancements and extensions and design as per the guidelines to system study give below.

Guidelines to System Study/ Design/Release Management

The SI shall carry out a detailed systems study to refine the Functional Requirements Specifications for the enhancements / extensions provided in this RFP and formulate the System Requirements Specifications (SRS). The SI shall also study CAS-State and CAS-Center being developed at NCRB. The SRS preparation shall take into account the BPR recommendations suggested by the NCRB. The study would also include different integration points of CAS (State) with external agencies and stakeholders within Odisha. The SI should also prepare a detailed document on the implementation of Enhancement/Extension to CAS (State), Portal, and other components as detailed in this RFP. 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 artefacts /documents provided by NCRB.

a) The System Study needs to be comprehensive. The SIs understanding of the department and associated offices, their infrastructure, processes, needs and challenges have to be complete and thorough so as to provide a solution that is relevant, error-free, up to date, meets all the needs of the state, is easy to use, maintain, and update/upgrade, comprehensive, and has a high probability of adoption and success.

   The System Study needs to cover locations based on but not limited to the following criteria. The following plan is indicative and would be finalized in consultation with the SI when they are on board:

   i. Geographic
      - Commissionerate
      - Urban Centers
      - Rural Locations
      - Covering all 36 Police Districts but not limited to the District Headquarters.
   ii. Functional
      - SCRB
      - Selected Police Stations and Higher Offices
      - CB-CID Office
      - Selected FSLs/FPBs/Traffic/STF
      - Integrating departments HQs / main offices
   iii. Special Needs:
      - Extremist Management
      - Coastal Security
      - Remote Locations:
        - Police Stations having problems of land/sea connectivity
        - Police Stations covering jurisdiction of remote areas
      - Power: Police Stations having problems of lack of availability of electricity

b) Preparation of System Requirements Specifications (SRS) for additional functionalities and different integration points with CAS (Center) and External agencies.
c) Preparation of the final CAS (State) enhancement implementation document with respect to extension, configuration, customization as per the requirement of Odisha Police.
d) Preparation of the Solution Design including solution architecture, use cases identifying the additional solution components/ modifications to CAS (State) application.
e) Solution Development and Customization and/or Configuration and Extension as required
f) Development of MIS and other reports

g) Formulation of test plans and test cases for additional functionalities and different integrations with external agencies including CAS (Center)
h) Change/Reference document include all the changes or deviations from the base version of the CAS (State) Application provided to the SI.
i) Testing of the configured solution (CAS) and additional functionalities.

Requirements Traceability Matrix

The SI would ensure that developed solution is fully compliant with the requirements and specifications provided in this RFP such as functional, non-functional and technical requirements.

a) 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 Odisha Police (updated, expanded and fine-tuned by the SI as necessary) and the System Requirements Specifications (SRS) prepared by the SI.
b) 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.
c) 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.
d) The Requirement Traceability Matrix would provide both forward and backward traceability.
e) The traceability matrix should be used to determine gaps and complexity and shall be reviewed by PMO and Odisha Police as a decision making tool.

Through the duration of the project, the PMO and 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.

Creation of Test Plans

Once the SRS is approved and design is started, the SI should prepare all necessary Test Plans (including test cases), i.e., functional and non-functional testing. Test cases for UAT would be developed in collaboration with domain experts identified at state headquarters. The Test Plans should 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 PMO & SPMU. Odisha Police will sign off on the test plans on the advice of PMO/ SPMU.

High Level Design (HLD)

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

Application Development and Unit Testing

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

The SI would also implement the changes proposed in the Change/Reference document to CAS (State) and carry out a thorough regression testing includes running some of the previously executed scripts for the functionality from the traceability matrix created.

Setup of Technical Environment at State Headquarters

The SI shall procure, setup and maintain the required software and the infrastructure for systems testing, functional testing and User Acceptance Testing where not available or not adequate; and training activities within State Headquarter premises; and for any other activities that may be carried out of State Headquarter premises such as issue management (Issue Tracker), document repository (configuration management tool), etc.

Regression, Integration, System and Functional Testing

After successful unit testing of all components, the SI would conduct full-fledged integration testing, system testing and functional testing in accordance with the approved Test Plans for the enhanced CAS (State) application, 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.

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

The SI along with PMO/ SPMU should take the responsibility in coordinating with NCRB and other external agencies for a smooth integration with CAS (Center).

The SI shall also prepare and execute automated test scripts covering majority of the application functionality (current and new) for subsequent regression tests.

Test Reports

The SI shall create test reports from testing activities and submit to Odisha Police/SPMU for validation

Test Data Preparation

The SI shall prepare the required test data and get it vetted by PMO/ Odisha Police/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.

End-to-End Performance and Security Testing

End-to-End Performance and Security testing of the Application to ensure that the application scales to the required number of users as per the service levels defined in this RFP.

User Acceptance Testing (UAT)

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

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

SI shall implement robust development / quality / release management / change management / incident management processes as per the industry standards.

Intensive Field Testing (Pilot Testing)

Intensive Field Testing should be carried out for all the major releases with new functionality. After successful UAT, the new version (only for major release) must be rolled out in at least 10 Police Stations / Higher Offices for intensive field-testing for a period of eight (8) weeks before being released across the State. Before the Intensive Field Testing of the new release, the SI shall train representative users from each of the police units on the new functionality. This will be an intense and brief training session of not more than a week. The new release must run without problems for a maximum period of four months in each of these police stations and SI shall incorporate the required changes (bug fixes, enhancements, feedback from end users after proper analysis) in the application before rolling out the new release across the State.

Objectives of Intensive Field Testing

a) To ensure that the new release / functionality provides the envisaged value to the end-users and is well accepted by the end-user.
b) To test on the field and ensure that new functionality is built to meet the functional requirements.
c) To ensure intense interaction of with users to fine-tune critical aspects such as look and feel, navigation, usability and ease of use and data fields of the new functionality.

Continuous Improvement of the CAS (State) Application Enhancements / Extensions

Focus on continuous improvement of CAS (State) Application is an important part of Application Management. The SI is expected to be the prime driver of continuous improvement during the application management phase. Based on their own domain expertise, research and user feedback, the SI shall propose ideas that significantly enhance SI and improve its effectiveness in meeting user needs and project goals.

The improvements proposed as part of this Continuous Improvement initiative will not be the usual run-of-the-mill enhancements, but will be significant changes that result in a quantum leap in meeting user needs and improving the outcomes in policing. Whether a proposed change forms part of Continuous

Improvement or is a minor change that will have to be incorporated into the application as part of the Application Management Services will be determined by the Empowered Committee.

5.3 Data Migration

Objectives of Data Migration and Digitization

In order to achieve the intended objectives of CCTNS such as Providing Enhanced Tools for Law & Order Maintenance, Investigation, Crime Prevention, and Traffic Management, Increase Operational Efficiency, and Creating a Platform for Sharing Crime and Criminal Data Across the Country, it is critical that the data that is currently available in various case files and registers maintained in the Police Station be migrated and captured as structured / parameterized data within the application.

The structured legacy data in the application in a format amenable for easier search and analysis will provide value to the end users for conducting efficient searches, statistical analysis and generating comparative statements and other mandatory / ad-hoc returns and reports. Eventually, the crime/criminal related physical registers at the Police Stations and Higher Offices will be phased out and the legacy data available in the system will serve as the one-stop repository of crime and criminal information across the State. This will also enable the required returns reports (regular and ad-hoc), one of the most time consuming activities at the Police Stations, to be generated at the higher office where the report is required thereby eliminating the need for collection and collation of data at multiple offices.

Scope of Data Migration and Digitization

The scope of data migration and digitization shall include:

a) The case data of the approximately 7, 95,715 cases from 2001-2010. The case data is spread across the electronic data captured in CIPA systems in the Police Stations and physical case files and registers within the Police Station.
   i. CIPA: CIPA implemented in 45 Police Stations have the FIR data from the last 5 years.
   ii. Case Files and Related Registers: The remaining data of the case has to be digitized (manual entry of the attributes) from the case files and physical registers at the Police Stations. The data attributes are in Hindi.
      - These registers are available at the various offices as physical copies.
      - FIRs of the cases that are not migrated from CIPA have to be digitized (manual entry of the attributes) into CAS (State).
      - The remaining attributes of the case should be migrated from the physical registers in the Police Stations and Higher Offices.
      - The list of the registers to be migrated into CAS (State) are as below:

Table 8 Source of registers

Sr. No	Source of Register	Register/Forms Name	Format of the register that depicts all the attributes along with type of the attribute
1.	Police Station	FIR	Ref to the Annexure 8
2.	Police Station	Case Diary	Ref to the Annexure 8
3.	Police Station	Final Form	Ref to the Annexure 8

i. Other case related information for cases created between 2001-2010 (both years including) needs to be digitized into CAS Application
   - Photographs of the Accused / Arrested (in color)
   - Fingerprints of the Accused / Arrested
   - Expert Opinion from Domain Specialists

b) In addition to the above, all the currently open cases (on-going investigation / trial) have to be migrated into CAS (State) even if the case is not registered between 2001-2010 (both years included).

c) Other Registers
   i. These registers are available at the various offices as physical copies.
   ii. The list of the registers to be migrated into CAS(State) Application are as below:

Table 9 registers to be migrated

Sr. No	Source of Register	Register/Forms Name	Format of the register that depicts all the attributes along with type of the attribute
1.	Police Station	Modus Operandi Register	Ref to the Annexure-8
2.	Police Station	Alphabetical Register	Ref to the Annexure 8
3.	Police Station	Crime Index	Ref to the Annexure-8
4.	Police Station	History sheet	Ref to the Annexure-8

*While the conviction details of the cases registered between 2001-2010 will be digitized as per the earlier clause, the conviction details of the cases for which trial has concluded in the last ten years will be registered as part of this scope.

Digitization

Data digitization of 10 years records with Odisha Police is mentioned in the table below.

Table 10 Volume of Digitization

Sr. No	Register/Forms Name	Number of Records* (in lakhs)
1.	FIR	7.95715
2.	Case Diary	7.95715
3.	Final Form	7.95715
4.	Modus Operandi Register	0.6369
5.	Alphabetical Register	0.6369
6.	Crime Index	0.8685
7.	History sheet	0.2895

*These figures are indicative only

The SI has to digitize of the relevant data/records till the CAS is operational. Migration of CIPA and CCIS Police Stations / Higher Offices to CCTNS-The Details of existing CIPA data is provided in the Annexure 8. CCIS Data also needs to be migrated. CCIS & CIPA data would be validated by the State Police Department before Data is migrated into CAS by the SI. The SI is also responsible for migrating data of Police Stations and Higher Offices currently operational on CIPA and CCIS to CCTNS as part of the CCTNS implementation in the State.

Details regarding list of Police Stations / Higher Offices running CIPA / CCIS along with the data to be

migrated is given in Annexure 8

The recommended methodology for Data Digitization and Data Migration is provided below:

Recommended Methodology of Data Migration

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

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

a) 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:

i. 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
ii. Write a specification to create, transfer and migrate the data set
iii. Document all exceptions, complex scenarios of the data
iv. This phase will generate the specification for Data Take-On routines

b) Transformation

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

i. Identify the fields, columns to be added/deleted from the existing system
ii. Identify the default values to be populated for all 'not null' columns
iii. 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
iv. Develop test programs to check the migrated data from old database to the new database
v. Test the migration programs using the snapshot of the production data
vi. Tune the migration programs & iterate the Test cycle
vii. Validate migrated data using the application by running all the test cases

viii. Test the success of the data take-on by doing system test

c) Data Take-On

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

i. Schedule data transfer of the computerized data that has been newly created by the data entry operators based on the hard copy records.
ii. Schedule data transfer of the existing digital data in the proposed new format
iii. Migrate the data from an old system (legacy) to the envisaged database
iv. Test on the staging servers after the data take-on with testing routines
v. Migrate from staging servers to production servers
vi. Deploy and rollout the system as per the project plan

Additional Guidelines for Data Migration

a) SI shall migrate/convert/digitize the data at the implementation sites of STATE.
b) SI shall formulate the "Data Migration Strategy document" which will also include internal quality assurance mechanism. This will be reviewed and signed-off by STATE prior to commencement of data migration.
c) SI shall incorporate all comments and suggestions of STATE in the Data Migration Strategy and process documents before obtaining sign-off from STATE.
d) SI shall perform mock data migration tests to validate the conversion programs.
e) Since there could be structural differences in the data as stored currently from the new system there should be a mapping done between the source and target data models that should be approved by Project Director
f) SI shall ensure complete data cleaning and validation for all data migrated from the legacy systems to the new application.
g) SI shall provide checklists from the migrated data to State Nodal Officer for verification, including number of records, validations (where possible), other controls / hash totals and highlight errors, abnormalities and deviations. SI shall incorporate corrections as proposed.
h) SI shall validate the data before uploading the same to the production environment.
i) SI shall generate appropriate control reports before and after migration to ensure accuracy and completeness of the data.
j) SI shall convey to STATE in advance all the mandatory data fields required for functioning of the proposed solution and which are not available in the legacy systems and are required to be obtained by STATE.
k) In the event STATE is unable to obtain all the mandatory fields as conveyed by SI, SI shall suggest the most suitable workaround to STATE. SI shall document the suggested workaround and sign-off will be obtained from STATE for the suggested workaround.
l) SI shall develop data entry programs / applications that may be required for the purpose of data migration in order to capture data available with / obtained by STATE in non – electronic format.
m) SI shall conduct the acceptance testing and verify the completeness and accuracy of the data migrated from the legacy systems to the proposed solution.
n) STATE may, at its will, verify the test results provided by SI.

SI shall get final sign off from State Nodal Officer for migrated / digitized data

5.4 Site Preparation, Commissioning, and Operationalization of the Infrastructure at the District Training Centers (DTC) / Regional Training Centers (RTC)

a) Locations of DTC / RTC

Table 11 Location of RTC

Sr. No.	Recruit training Centre	Estimated sitting capacity
1.	APTC Jharsuguda	20
2.	Third Bn. Koraput	20
3.	4th Bn Roukela	20
4.	5th Bn. Baripada	20
5.	6th Bn. Cuttack	20
6.	8th Bn Chahatrapur	20
7.	1st IR. Bn Upper Kolab	20
8.	3rd IR Bn Kalinga Nagar	20
9.	4th IR bn. Deogarh	20
10.	PTS Nayagarh	20
11.	SOG training centre Chandaka	20
12.	Angul Police Training College	20

b) Existing Infrastructure at Training Centre

Table 12 Existing Infrastructure at Training Centres

Sr. No.	Hardware procured for Training Centres
1.	Desktop Computers
2.	Printer (Inkjet Printer, Dot Matrix Printer, Laser Printer)
3.	Scanner (Document Scanner, Code Scanner)
4.	Laptop
5.	Server
6.	UPS
7.	LCD Projector

Odisha Police has carried out procurement of hardware infrastructure for Training Centres. Hardware procurement for Training Centre does not form part of scope of work for SI.

c) Infrastructure provided to SI from SCRB

d) Scope of work

i. Site Preparation

ii. Installation / Commissioning
iii. Operationalization
iv. AMC of the infrastructure provided by SCRB is covered for three years from the date of Delivery

5.5 Site preparation at Police Stations and Higher Offices

Site Preparation

The Odisha Police shall provide the necessary office space to the SI. Site Preparation shall cover all the activities necessary to enable the Police Station to setup the client side infrastructure and operate on CCTNS. The Site survey report should essentially mention all the civil works required at the Police Station/Higher office which is essential for SI to carry out his work.

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 and submit to the Nodal agency. The report will reflect the status of readiness of the office space for the proposed work. SI would be responsible to prepare the client sites for setting up the necessary client site infrastructure. Civil work at Police Stations and Higher Offices is out of scope for SI.

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

a. Setting up of Local area network (LAN cables, LAN ports, etc.)
   i. 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, provision of cords, connectors along with all the necessary accessories.
   ii. 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. SI shall create LAN at each location such that the Service Levels as per the requirements are met.
b. Ensure adequate power points in adequate numbers with proper electric-earthling
c. Earthing and electric cabling as required at the site
d. In addition to the above, fixing and maintenance 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

In the offices (Police Stations and Higher Offices), where LAN is already setup and functional, SI shall upgrade the LAN to enable the commissioning of additional computers and peripherals procured as part of this RFP and provide the operations and maintenance support for continued functioning of the LAN.

The components to be procured, delivered and commissioned as part of Site Preparation include:

Table 13 LAN Cabling

Items	Total Quantity	Specifications
LAN Cabling	**As Required**	**N/A**

Procurement, Delivery and Commissioning of IT Infrastructure at Police Stations and Higher Offices

SI shall procure the CCTNS infrastructure required at the locations statewide. At each such location the following shall be carried out.

a. Supply of the hardware, software, UPS, DG set to the location as per the requirements
b. Installation, Testing and Commissioning of UPS, DG-Set
c. Physical Installation of Desktops, Printer, Scanner, /MFD, Switch- Connecting peripherals, devices, Plugging in
d. Operating System Installation and Configuration
e. Configuring the security at the desktops, switch
f. Network within the Police Station and Higher Offices and liBrowser Configuration
g. Test accessibility and functionality of CAS (State) application from the desktops
h. Ensuring all the systems required are supplied, installed, configured, tested and commissioned and declaring the site to be operational. SI should submit a Site Operational Report which will mention that Site is ready for operation.

It shall be the responsibility of the Selected SI to bring all the installation equipment and tools required for the aforementioned all activities.

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

a. 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, Odisha 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.
b. The selected SI would be responsible for delivering the equipment to all the respective locations.
c. 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.
d. 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 Odisha Police during acceptance testing shall be replaced by new accepted equipment(s) at no additional cost to Odisha Police
e. 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 signoff would be provided by the Odisha Police / Project Nodal Officer assisted by SPMU/ State Mission Team.

The components to be procured, delivered and commissioned as part of Infrastructure at Police Stations and Higher Offices include:

Table 14 BOM

Sr. No.	ITEMS	Quantity (Indicative only)	Specifications provided in Annexure
1.	Client Systems	3216	Annexure -7
2.	Licenses for Office MS Offices	869	Annexure -7
3.	Licenses for Open Offices	2347	Annexure -7
4.	HDD 160 GB	579	Annexure -7
5.	Duplex Laser Printer	579	Annexure -7
6.	Multi-Function Laser	742	Annexure -7
7.	UPS for 120min backup	1177	Annexure -7
8.	2KVA Generator	579	Annexure -7
9.	16-Port Switch	742	Annexure -7
10.	Fingerprint Reader	579	Annexure -7
11.	Digital Camera	579	Annexure -7
12.	Electronic Pen	579	Annexure -7

Hardware at Police Stations

Table 15 Hardware requirement at Police Station

Sr. No.	ITEMS	Total police Stations(Figures are indicative)
1.	Client Systems	4
2.	HDD 160 GB	1
3.	Duplex Laser Printer	1
4.	Multi-Function Laser	1
5.	UPS for 120min backup	1
6.	2KVA Generator/Changed to Solar Power	1
7.	16-Port Switch	1
8.	Fingerprint Reader	1
9.	Digital Camera	1
10.	Electronic Pen	1

Hardware Requirement at Higher Offices

Table 16 Hardware requirements at Higher Offices

ITEMS	State Police Head quarters	Commissioners Office	RANGE Offices	District HQs	SDPO	ACP & DCP	SCRB	Crime Branch	HRPC	SFSL	State Police Control Room	District Police Control Room	Finger Print Bureau
Client Systems	50	25	4	10	3	3	4	4	4	4	4	2	1
UPS	-		1	-	1	1	1	1	1	1	1	1	1
MFP	50	25	1	10	1	1	1	1	1	1	1	1	1
Switch	-		1	-	1	1	1	1	1	1	1	1	1

5.6 Capacity Building and Change Management, Communication & Awareness

Odisha Police has made significant progress towards change management training in over 28221 personnel in Basic IT and other IT applications in use Odisha . The SI is required to design, build and execute and comprehensive Capacity Building and Change Management, Communication and Awareness plan for Odisha Police and execute the same as per the scope of work in this RFP. Details on Capacity Building and Change Management are in Annexure-6

5.7 Co-ordination and Management of Network Connectivity

The Networking solution of CCTNS project shall be based on a Hybrid Model which will consist of Odisha State Wide Area Network (OSWAN) operated by BSNL (through its vendor M/s. Spanco Ltd.) under SWAN scheme of Government of India and Data network operated by Bharat Sanchar Nigam Limited (BSNL) which consists of point-to-point leased lines, VPNoBB, Wi-Max, VSAT and MPLS technologies. BSNL shall be providing the Networking & Connectivity services along with Operations & Maintenance for all the locations implemented by BSNL in Odisha. BSNL shall also provide connectivity on MPLS VPN network for aggregated bandwidth at SDC (State Data Center) for the locations connected on VPNoBB, Wi-Max and VSAT network and also provide connectivity from SDC to State Head quarters (SHQs) to the National Data Centre (NDC) of NCRB. Further BSNL shall provide MPLS VPN network for connecting SDC and State Disaster Recovery Centre (SDRC) of Odisha.

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

a. Provisioning of 2Mbps Point to Point Lease Line (P2PLL) for locations to be connected with the nearest OSWAN POP.
b. Provisioning of WAN connectivity on VPNoBB/Wi-Max/VSAT for locations which are not feasible to be connected directly with the OSWAN on P2PLL.
c. Provisioning of the Routers (at CCTNS site) and Modems for locations to be connected directly with OSWAN and all other hardware and network infrastructure provided for VPNoBB/Wi-Max/VSAT connectivity.
d. Provisioning of Aggregated bandwidth on MPLS network at SDC for the locations connected on VPNoBB, Wi-Max and VSAT network.
e. Provisioning of MPLS connectivity between SDC and SDRC.
f. Provisioning of MPLS connectivity between NDC and state SDCs.
g. Maintaining the network including hardware supplied for minimum period of 3 years.

Role of System Integrator: The SI shall coordinate with BSNL and the Odisha Police Department and the Department of Information Technology (DIT), Government of Odisha, for implementation of the Network and Connectivity solution of CCTNS project. The following are the key responsibilities of the SI with respect to Networking and Connectivity.

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

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

d. The SI will also be coordinating with BSNL and OCAC/ SCRB for SLA Monitoring, Fault Reporting & Troubleshooting of the links for meeting the Service levels and Master Service Agreement.

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

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

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/UTs.
(The bidder may note that the above scope of work has been taken from the Addendum #2 of the SI RFP as detailed by NCRB; any further changes shall be communicated to the bidder during or after the conclusion of the bid process).

5.8 IT Infrastructure at the Data Center And Disaster Recovery Center

The SI shall provide system integration services to procure and commission the required software and infrastructure at the State Data Centre (SDC) and Disaster Recovery Centre, deploy the configured and customized CAS (State) and integrate with CAS (Centre) 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. 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/UT.

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. 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 is responsible for sizing the hardware to support the scalability and performance requirements of the solution.

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 also provide descriptive Deployment Model, Diagrams and other relevant design details.

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

Broad Overview of the User and Service Requirements

The below table provides the user and service requirements. The detailed service levels to be met by the SI are provided as Annexure 3 to this RFP.

Table 17 User and Service requir6ement

Sr .No	User and Service Requirements	
		Expected / Envisaged
1.	Average Concurrent Users	1500
2.	Peak Concurrent Users	4500
3.	Average Transactions per second	5
4.	Storage Requirement per case (including FIR/attachments/arrest card/charge sheet)	Refer to table below on Indicative Storage Requirement

Table 18 General Requirements

Sr. No.	General Requirements
1.	It is proposed to have the CAS application in high availability and clustering mode. The load on the application would be shared by redundant application and database servers via a load balancer. SI has to configure the servers with load balancing in active – active mode.
2.	The disaster recovery site shall only have the Storage and other related infrastructure. In the current phase, it is not envisaged to have CAS (State) application running at the Disaster Recovery Site.
3.	At the DR site the storage should have 100% of the capacity of the Data centre site.
4.	The Application servers would be accessing the database from the backend in order to process the user / citizens queries/requests.
5.	The Database servers (RDBMS) would be hosted in higher security layer, comprising of components such as Firewall and Intrusion Prevention system
6.	The frequency of Data backup etc. would be finalized at a later stage
7.	The SI should also install, configure and commission the monitoring software for the CAS

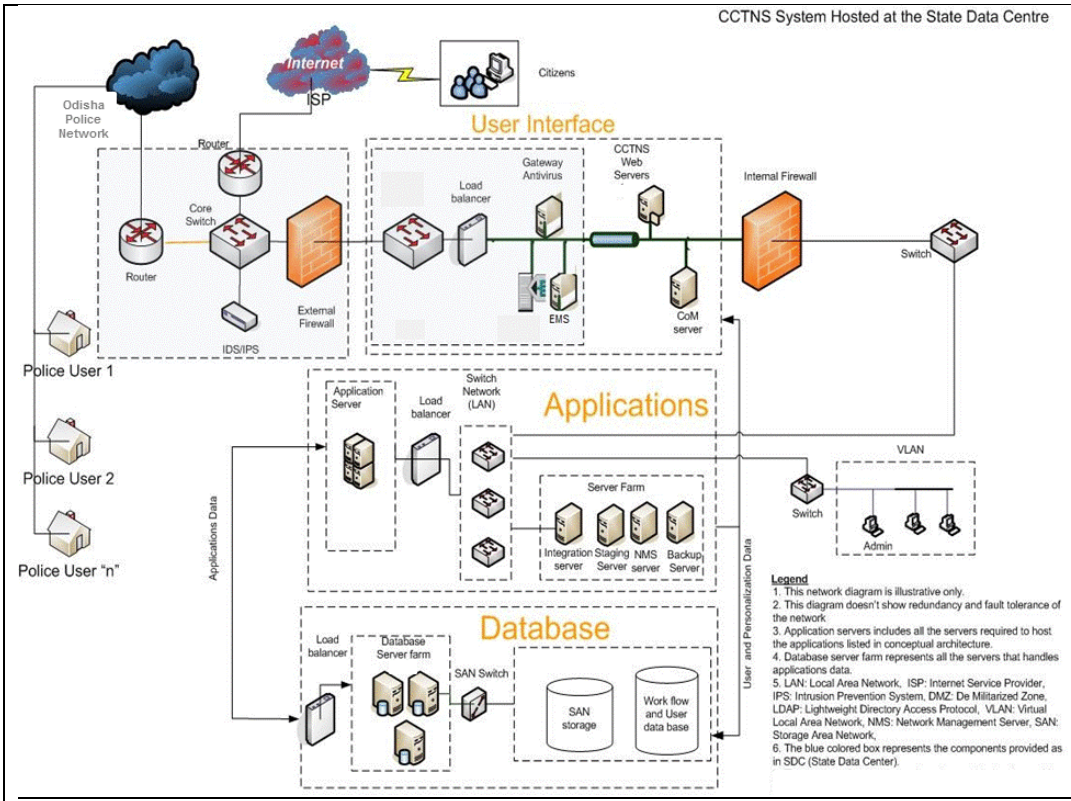
Sr. No.	General Requirements
	application and should be able to demonstrate the various performance parameters with respect to application availability, uptime & downtime of the server, Server utilization and other performance parameters. The SI should also configure the monitoring software covering all the features as mentioned in the technical specifications of the monitoring software. The SI shall install all the required clients on the application server, database servers and web server so as to integrate the monitoring software for obtaining the desired output
8.	No Products supplied under the RFP should be end of life. No IT equipment model should have been introduced in the market not later than 2 years back as on date of the bid submission
9.	All technical specifications, documentation generated during design, installation and commissioning phase shall be provided to the State.
10.	SI should design the storage solution keeping in mind the relevant requirement and its usage. The storage system should be scalable enough to handle future requirements. The SI should also adopt detailed system and data back-up processes and methodologies, using industry standard tools

Table 19 Storage requirement

Sr .No.	This is an indicative size only and the SI is expected to estimate the size and provide the required storage
1.	Indicative size of one case file (which may include several images and text) that makes up the 7-IIF data and additional data in the registers = 1 MB
2.	Estimated Total Number of Cases in Odisha in the 15 years (Past Data for 10 years and future Data for 5 years) = 15,00,000
3.	Approximate Storage Requirement at Odisha for digitized case file data =~ 2 TB usable
4.	Storage requirement for Mail and Messaging solution for approximate 25,000 employees considering 100 MB/employee =~ 3 TB usable
5.	Storage requirement for HRMS and other applications =~ 5 TB
6.	Total estimated usable storage requirement (Cases + Mail) for Odisha =~ 10 TB.

CAS (State) Deployment Architecture at the SDC

Figure 1 Deployment Architecture at the SDC



Indicative Data Centre architecture

The SI is responsible for the below at the Data Centre:
Procurement, installation, administration, operation and maintenance of:

a. Servers (Web, Application (CAS-State, Portal, SMS-Gateway), Reporting, Database, Training, Staging / Testing, Backup, Antivirus, EMS, etc.)
b. Enterprise Management System (EMS)
c. Antivirus Software
d. SAN Storage
e. SAN Switches
f. Tape Library
g. All necessary software components including but not limited to Operating System, Backup Software, and SAN Storage Management Software

The SI is responsible for the below at the Disaster Recovery Centre. (The list provided below is indicative. At the time of deployment, Government may choose to source some of these components from the shared infrastructure available at the SDC / DR. However, bidders shall mandatorily include these items in their IT Infrastructure sizing and provide price quotes for the same)

Procurement, installation, administration, operation and maintenance of:

a. Servers (Web, Application, Database, Backup, Antivirus, EMS, etc.)
b. Enterprise Management System (EMS)
c. Antivirus Software
d. SAN Storage
e. SAN Switches
f. Tape Library
g. Server Load Balancer
h. Firewalls & IPS
i. KVM over IP
j. All necessary software components including but not limited to Operating System, Backup Software, and SAN Storage Management Software

Table 20 BOM at DC and DR

Sr. No.	Items	QTY at Data Center	QTY at Disaster Recovery
1.	Application Server	2	1
2.	Database Server	2	1
3.	Web Server	2	1
4.	Management Server	2	2
5.	Firewalls & IPS	2	
6.	Mail/Messaging Server	2	
7.	Servers for Staging / Testing / Training Environment/Back up/Others.	3	
8.	SAN Storage	1	1
9.	SAN Switch	2	2
10.	Tape Library along with the tapes	1	1
11.	Server Load Balancer	2	1
12.	KVM over IP	2	1
13.	Back UP Software for Data Centre and DR	1	1
14.	Enterprise Management System (EMS)	1	1
15.	OS and Application – as per the Stack	-	-

At the time of deployment, Government may choose to source some of these components e.g. EMS from the shared infrastructure available at the SDC / DR. In this case, SI shall procure the additional licenses of the current EMS tool in the Data Center and Disaster Recovery Center and configure the EMS tool to monitor / manage the entire enterprise wide application, infrastructure and network related components commissioned by the SI. The SI shall also deploy a backup software to periodically backup all data and software.

The indicative specifications for the above components are provided in Annexure 9 of Volume I of the RFP.

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. CAS (State) shall be hosted in a collocation model in the State Data Centres (SDC). The connectivity between the Data Centres in the States and the CAS (Centre) Data Centre & CAS (Centre) Disaster Recovery Centre at NCRB and the connectivity between the CAS (Centre) Data Centre and CAS (Centre) Disaster Recovery Centre at NCRB is not in the scope of the SI.

The SDC is located in Bhubaneswar, Odisha. The corresponding DRC may be located at the SDC of another state, which would be decided subsequently by the Government.

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

a. RACK
b. Power and Cooling
c. UPS, DG set power backup
d. Bandwidth and Connectivity
e. LAN
f. VPN
g. Firewall
h. Intrusion Protection System
i. Fire prevention
j. Physical security surveillance
k. Network Operation Centre
l. Common Data Centre facility Maintenance and Support

Indicative Responsibility Matrix:

- **Odisha Police** / Ministry of Home Affairs / NCRB
- **DCO:** Data Centre Operator / Data Centre Service Provider
- **SI:** System Integrator

Table 21 Indicative Responsibility Matrix

Sr. No	Activity	Odisha Police/MHA/NCRB	DCO	SI
1.	Identification of Site for Data Centre and Disaster Recovery Centre	Y		
2.	Provision of Data Centre and Disaster Recovery Building Space		Y	
3.	Connectivity between the Data centre site and disaster recovery site	Y		
4.	Connectivity between States and Centre	Y		

Sr. No	Activity	Odisha Police/MHA/NCRB	DCO	SI
5.	Provisioning of UPS Power at DC and DR site		Y	
6.	Availability of power and cooling and other facility		Y	
7.	Physical Security at DC and DR site		Y	
8.	Network Security Management		Y	
9.	Requirement analysis, sizing and capacity planning for CAS at DC and DR site			Y
10.	Procurement, Installation, and maintenance of Infrastructure and application for CAS (Centre) & providing related documentation to Odisha Police			Y
11.	Setting (installation, configuration, commissioning) of Disaster recovery with respect to supplied hardware			Y
12.	Preparation of Backup policies, business continuity plan and other Policy documents			Y
13.	Administration and management services of the infrastructure and application deployed by SI at SDC and DRC			Y

5.9 Handholding Support

The System Integrator will provide one qualified and trained person per police stations for a period of 6 months to handhold the staff in the police station and ensure that the staff is able to use CAS (State) on their own by the end of the handholding period. Handholding support would be required only after the successful commissioning of CAS (State) application and the necessary infrastructure and completion of capacity building and change management initiatives in respective police stations / Higher Offices for each phase as detailed in the implementation plan.

The scope of the handholding personnel shall include but is not limited to:

a. Ensure that computers and other peripherals are in working condition
b. Trouble shoot any local issues related to applications, computers, peripherals, LAN, and connectivity
c. Provide assistance to Police Staff on basic computer usage and office productivity software
d. Provide assistance to Police Staff on any CAS (State) Application functional and usage issues
e. Escalate any issues to Help desk or Point of contacts given if issue is not resolved within a stipulated time

The Personnel will be deployed across state of Odisha. However OCAC/ SCRB reserves the right to change the location as per the needs of project.

General Guidelines for Handholding Personnel

a. The SI shall provide proper initiation and training to the Handholding personnel including necessary training on Basic IT, CAS (State) Application and L0 support.
b. The strength of service personals with their qualifications, experience and background shall be furnished. Background verification may be carried out by Odisha Police if necessary.
c. The Handholding Personnel shall not be changed frequently and in case of such change, this shall be done only in consultation with the Odisha Police.
d. In Event of Handholding Personnel leaving the project during any time of the project, an equally qualified replacement should be provided before the earlier person leaves the project and the SI should ensure that the activities at police stations are carried out without any delay.
e. The SI shall be solely responsible for the Salaries / Minimum wages, Bonus, Provident Fund, Gratuity, Family pension and contribution of E.S.I, service tax or any other statutory obligations towards the personnel including their welfare. The Proof of the same shall be submitted on request from Odisha Police.
f. The work and holiday Schedule of the personnel will comply Odisha Government Holiday Rules and Regulations
g. The SI should completely manage the handholding personnel, their deployment and Human Resource issues.
h. The SI shall be liable for any damage to premises or equipment due to the handholding personnel.
i. SI shall replace any handholding personnel, upon request from Odisha Police within 15 days.
j. SI shall ensure proper attendance and reporting from the Handholding personnel and shall maintain a daily activity log for all personnel.
k. One in five handholding personnel in adjacent location shall be designated as a team leader for advanced level support.
l. The minimum qualifications and work experience required for personnel to be deployed by SI is given below:
m. Graduate in any discipline
n. Three years of experience in Technical Support/Training/Handholding
o. Good knowledge of computer (MS Office, Word, Excel and Power Point) and Networking/LAN/Hardware functions
p. Good Communication skill (oral as well as in written)

5.10 SUPPORT TO ACCEPTANCE TESTING, AUDIT AND CERTIFICATION

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

a. Functional requirements
b. Test cases, Requirements Mapping and traceability matrix
c. Infrastructure Compliance Review
d. Availability of Services in the defined locations
e. Performance and Scalability
f. Security / Digital Signatures

g. Manageability and Interoperability
h. SLA Reporting System
i. Project Documentation
j. Data Quality Review

As part of Acceptance testing, audit and certification, performed through a third party agency, Odisha Police 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 Odisha Police Technical Services, one for audit & certification of security and control aspect of the system and the other for audit & certification of overall application s/w.

Odisha Police 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 Odisha Police Technical Services, will not, however, absolve the SI 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:

a. Functional Requirements Review

The system developed/customized by SI shall be reviewed and verified by the agency against the Functional Requirements signed-off between Odisha Police Technical Services 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 for 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).

b. 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.

c. 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:

i. Audit of Network, Server and Application security mechanisms

ii. Assessment of authentication mechanism provided in the application /components/ modules
iii. Assessment of data encryption mechanisms implemented for the solution
iv. Assessment of data access privileges, retention periods and archival mechanisms
v. Server and Application security features incorporated etc.

d. 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 Odisha Police Technical Services and SI. Such parameters include request-response time, work-flow processing time, concurrent sessions supported by the system, Time for recovery from failure, Disaster Recovery drill etc. The performance review also includes verification of scalability provisioned in the system for catering to the requirements of application volume growth in future.

e. 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.

f. 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.

g. SLA Reporting System

SI shall design, implement/customize the Enterprise Management System (EMS) and shall develop any additional tools required to monitor the performance indicators listed under SLA prescribed in this RFP. The Acceptance Testing & Certification agency shall verify the accuracy and completeness of the information captured by the SLA monitoring system implemented by the SI and shall certify the same. The EMS deployed for system, based on SLAs, shall be configured to calculate the monthly payout by Government of Odisha to SI.

h. 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 Odisha Police Technical Services.

i. 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.

6. SCOPE OF SERVICES DURING POST-IMPLEMENTATION (OPERATION & MANAGEMENT) PHASE

As part of the operations and maintenance services, the SI shall provide support for the software, hardware, and other infrastructure that are in the scope of this RFP. The details of O&M phase is provided in the section on implementation plan. SI shall provide comprehensive support from the date of Go Live of Phase I, which includes:

a. Software maintenance and support services
b. Application functional support services
c. Warranty support for all the new hardware procured as part of this RFP
d. AMC support for Hardware
    i. Hardware augmented as part of this RFP
    ii. Specific hardware required as per the RFP once the current AMC by the original vendor expires
e. Annual Technical Support (ATS) for all the licensed software
f. Operations and maintenance services for the server and related infrastructure supplied and commissioned by the SI for the application at the Data Center and Disaster Recovery Center
g. Central Helpdesk from the State designated premises
h. Handholding Support for the end users at each of the locations, as per the requirements of this RFP, to handhold the Police Station and Higher Office personnel after the CAS (State) application and the necessary infrastructure are successfully commissioned in the police stations and Higher Offices

The services shall be rendered onsite from the State designated premises. To provide the support for the police stations, circle offices, sub-divisional offices, district headquarters / , ranges, zones, state police headquarters and other locations across the State where the software, hardware, and other infrastructure will be rolled out, SI is expected to provide experienced and skilled personnel at each location. The SI shall develop a work plan for the knowledge sharing as per scope defined in this RFP for use in future phases of the project.

Software Maintenance and Support Services

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

a. The Software Maintenance and Support Services shall be provided for all current modules of CAS (State)application and the enhancements carried out by the SI as part of the scope of this RFP
b. The SI shall render both on-site and off-site maintenance and support services to the State at all the designated locations
c. Tuning of application, databases, third party software's and any other components provided as part of the solution to optimize the performance
d. SI shall perform minor changes, bug fixes, error resolutions and minor enhancements that are incidental to proper and complete working of the application.
e. Minor enhancements (the usual run-of-the-mill enhancements)
f. Release Management for the interim releases of the application
g. Centralized version control of the application
h. Routine functional changes

i. Any changes to the application code that may be required because of patches to licensed software being used (if any). 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.

j. Any changes to application code that may be required because of upgrades / patches to CAS (Center) if any

k. Updating and maintenance of all project documents

l. Change request management based on feedback from the users or the initiative of the SI. All planned changes to the application, especially major enhancements and changes in functionality that are deviations from the signed-off FRS/SRS, shall be coordinated within established Change control processes.

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

Application Functional Support Services

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

a. The Application Functional Support Services shall be provided for all current modules of CAS (State) application and the enhancements carried out by the SI as part of the scope of this RFP. The SI shall render both on-site maintenance and support services to the State from the SCRB premises in Odisha.

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

c. 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.

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

e. The SI shall maintain access controls to protect and limit access to the authorized End Users of the State.

f. 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.

g. SI shall carry out the configuration of new police stations, new acts/sections, and any other configurable data entities in the system as required by the State

Warranty support for all the new hardware procured as part of this RFP

As part of the warranty services SI shall provide:

a. SI shall provide a comprehensive warranty and on-site free service warranty for all the new hardware procured as part of this RFP

b. SI shall obtain the five year product warranty and five year onsite free service warranty on all licensed software, computer hardware and peripherals, networking equipment and other equipment from the OEMs.

c. 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.

d. 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.

e. 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.

f. 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 equipment for inspection, delivery of equipment or for commissioning of the systems or for acceptance tests / checks on per site basis, State reserves the right to charge a penalty. SI shall track and report observed Mean Time Between Failures (MTBF) for Hardware.

g. 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.

h. The SI shall as far as possible repair the equipment at site.

i. In case any hard disk drive of any server, SAN, or client machine is replaced during warranty / AMC the unserviceable HDD will be property of State and will not be returned to SI.

j. 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.

k. 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. PM envisages all activities require to be undertaken for good upkeep of hardware. It also includes the end user equipment or client side infrastructure.

l. SI shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.

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

n. 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.

o. 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).

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

AMC support for hardware augmented as part of this RFP and specific hardware required as per the RFP once the AMC by the original vendor expires

As part of the AMC services SI shall provide:

a. SI shall provide a comprehensive for 5 years from the date of Go Live for

i. hardware augmented as part of this RFP
ii. specific hardware required as per the RFP once the AMC by the original vendor expires

b. SI is responsible for sizing and augmenting the existing hardware and software licenses as per the performance requirements provided in the RFP. During the AMC period SI shall replace or augment or additional licenses at no additional cost to the State in case the augmented hardware or software is not adequate to meet the service levels

c. During the AMC 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.

d. SI shall as far as possible repair the equipment at site.

e. In case any hard disk drive of any server, SAN, or client machine is replaced during AMC the unserviceable HDD will be property of State and will not be returned to SI

f. AMC 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 AMC will not apply to such supplemental hardware items installed.

g. 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 AMC and the AMC period will be extended by the period of delay in PM.

h. SI shall monitor AMC to check adherence to preventive and repair maintenance terms and conditions.

i. SI shall ensure that the AMC complies with the agreed Technical Standards, Security Requirements, Operating Procedures, and Recovery Procedures.

j. 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.

k. 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).

l. SI shall develop and maintain an inventory database to include the registered hardware AMCs.

Annual Technical Support (ATS) for all the licensed software

As part of the ATS services for all the licensed software SI shall provide:

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

n. 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.

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

p. 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. 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

q. SI shall provide and apply regular patches to the licensed software including the software, operating system, databases and other applications.

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

s. 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.

t. 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.

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

v. The ATS Services will cover, all product upgrades, modifications, and enhancements

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

Operations and maintenance services for the server and related infrastructure supplied and commissioned by the SI for the application at the Data Center and Disaster Recovery Center

As part of the 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

System Administration, Maintenance & Management Services

The objective of this service is to support and maintain all the Systems and Servers provided as a part of this Contract, and shall include:-

a. 365x24x7 monitoring and management of the servers in the DC and DRC.

b. Regular monitoring of all the applications hosted.

c. Operating System administration, including but not limited to management of users, processes, preventive maintenance and management of servers including updates, upgrades and patches to ensure that the system is properly updated.

d. Installation and Re-installation of the server and other hardware in the event of system crash/failures.

e. Regular analysis of events and logs generated in all the sub-systems including but not limited to servers, operating systems, security devices etc. to identify vulnerabilities. Necessary Action shall be taken by the SI in accordance with the results of the log analysis. Suitable mechanism has to be maintained for security and forensic related logs or as per requirement of other government regulations issued from time to time.

f. Adoption of policies and procedure, compliances, guideline or international standard as defined

g. by the State.

h. Provide integration and user support on all supported servers, data storage systems, etc.

i. Troubleshoot problems with web services, mail services, applications software, desktop/server

j. relationship issues and overall aspects of a server environment.

k. Problems shall be logged in at the Help Desk and resolved as per the SLAs defined.

l. Manage and monitor server configuration, performance and activity of all servers. Performance optimization and reporting - Process and Memory Management, Monitoring CPU performance, Monitoring Memory performance, Monitoring Input/output performance, Monitoring Ethernet Traffic, etc.

m. Prepare and keep up to date document containing configurations of all server, IT infrastructure etc.

n. Hardening servers in line with security policies.

o. Carry out the DC and DRC failure testing and half yearly BCP real drills.

p. Perform Database Administration activities for Database. The SI agrees that all databases of the State will be administered as per standards and requirements. The service covers all the databases run on servers / SAN at DC and DRC including but not limited to:-
   i. Start-up and shutdown of databases.
   ii. Daily / Weekly / Monthly backup of databases.
   iii. Database recovery when required.
   iv. Weekly database recovery checks.
   v. Required logs maintenance as per policies of the State.
   vi. Disaster recovery as per polices of the State.
   vii. Documentation upkeep and records maintenance.
   viii. User account management.
   ix. Database problem resolution.
   x. Performance tuning.
   xi. Replication of Database from DC to DRC.

Application Monitoring Services

The services to be provided by the SI for Application Monitoring shall include:-

a. Web services.
b. Application server.
c. Database server.
d. Middleware.
e. Other components.

Network Management Services

SI shall ensure continuous operation and upkeep of the LAN & WAN infrastructure at the DC, DRC, and all the Police Stations and Higher Offices including all active and passive components. For overall functioning of the network connectivity, the SI shall be responsible to coordinate with Network Connectivity Provider's team for WAN link related issues. The services to be provided for Network Management shall include:

a. Ensuring that the network is available 365x24x7 as per the prescribed SLAs.
b. Attending to and resolving network failures and snags.
c. Support and maintain the overall network infrastructure including but not limited to LAN passive components, routers, switches, and SAN switches etc.
d. Configuration and backup of network devices including documentation of all configurations.
e. 365x24x7 monitoring of the network to spot the problems immediately.
f. Provide information on performance, including capacity utilization and error statistics for the network components.
g. Test new Network applications and tools installations prior to general use to check compatibility with the existing LAN and WAN configuration.
h. Establish, in conjunction with the State, a test and implementation plan prior to each application and tool installation.
i. Identify and communicate to the State, any prerequisites (eg, disk space, operating system, data backup) prior to licensed software and tools implementation and any post-install requirements (eg, security, software support), or any updates to the configuration database.
j. Provide a single-point-of-contact to WAN support personnel from State. The Network specialist representing the SI will respond to the initial request from State within standard service level objectives.
k. Provide one copy of appropriate software operational documentation to State.

Backend Services (Mail, messaging, etc)

a. SI shall maintain and support all the backend services (mail, messaging, etc) implemented that include Directory Services such as domain management, group management, user management, Database Services. The SI shall implement and effectively run the mailing service for the users of State.

Storage Administration and Management Services

The services to be provided by the SI shall include:-

a. Identify key resources in the Storage solution.
b. Identify interconnects between key resources in the Storage solution.
c. Receive asynchronous notification that the configuration of the Storage solution has changed.
d. Identify the health of key resources in the Storage solution.
e. Identify the available performance of interconnects in the Storage solution.

f. Receive asynchronous notification that the performance of the Storage interconnect solution has changed.

g. Identify the zones being enforced in the Storage solution.

h. Create/delete and enable/disable zones in the Storage solution.

i. Identify the storage volumes in the Storage solution.

j. Create/delete/modify storage volumes in the Storage solution.

k. Identify the connectivity and access rights to Storage Volumes in the Storage solution.

l. Create/delete and enable/disable connectivity and access rights to Storage Volumes in the Storage solution.

m. Storage administration - facilitates the states in connecting to the Storage later and gives them access rights as required.

IT Security Administration Services and Services for ISO 27001 and ISO 20000 compliance

SI shall be responsible for operating, monitoring, reviewing, maintaining, and improving the Information Security Management System (ISMS) at the DC and DRC. SI shall implement and maintain the ISO 27001 standard. SI shall be responsible for implementation and maintenance of ISO 20000 standard to promote the adoption of an integrated process approach to effectively deliver the services. The services to be provided by the SI shall include:-

a. Addressing the on-going needs of security management including, but not limited to, monitoring of various devices / tools such as firewall, intrusion detection, content filtering and blocking, virus protection, and vulnerability protection through implementation of proper patches and rules.

b. Maintaining an updated knowledge base of all the published security vulnerabilities and virus threats for related software.

c. Ensuring that patches/workarounds for identified vulnerabilities are patched/ blocked immediately.

d. Respond to security breaches or other security incidents and coordinate with respective OEM in case a new threat is observed to ensure that workaround / patch is made available for the same.

e. Provide a well-designed identity management system, security of physical and digital assets, data and network security, backup and recovery etc.

f. Maintenance and management of security devices, including, but not limited to maintaining firewall services to restrict network protocols and traffic, detecting intrusions or unauthorized access to networks, systems, services, applications or data, protecting email gateways, firewalls, servers, from viruses.

g. Ensuring that the security policy maintained and draft various relevant , procedures , guidelines and other ISMS documents as per ISO 27001 standard and implement these procedure accordingly , these documents shall be maintained and updated as per the ISMS ISO 27001 requirement.

h. A process must ensure the continuous improvement of all elements of the information and security management system. The ISO/IEC 27001 standard adopts the Plan-Do-Check-Act [PDCA] model as its basis and expects the model to be followed in an ISMS implementation.

i. Suitable mechanism has to be adopted for maintaining the ISMS, forensic logs or other as required for compliance by the SI time to time.

Backup and Restore Services

The services to be provided by SI shall include:-

a. Backup of storage as per the defined policies.

b. Monitoring and enhancing the performance of scheduled backups, schedule regular testing of backups and ensuring adherence to related retention policies as defined by State.

c. Prompt execution of on-demand backups of volumes and files whenever required or in case of upgrades and configuration changes to the system.

d. Real-time monitoring, log maintenance and reporting of backup status on a regular basis.

e. Media management tasks, including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets (onsite and offsite).

f. 365x24x7 support for file and volume restoration requests at the DC and DRC.

Central Helpdesk from the State designated premises

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

a. The service will be provided in the local language of the State.

b. 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.

c. 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, zonal offices, state police headquarters and other locations across the State where the software, hardware, and other infrastructure will be rolled out. This is further elaborated as handholding support services in the Scope of RFP.

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

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

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

g. 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.

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

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

6.1 Exit Management and Transition at the end of Contract Period

SI shall start the exit management and transition at least three month before the expiry of the Contract. SI shall provide the State with a recommended exit management plan detailing the transfer process that can be used by the State to ensure continuing provision of services throughout the transfer process and beyond.

SI shall ensure successful knowledge transfer to ensure that the knowledge about the entire Information Technology System including but not limited to the applications, the design and operational characteristics of these systems are transferred to the State's Project Team.

SI shall design or propose any additions to the State's Project team to manage the system. SI shall also undertake an analysis of the skill set requirement for the State's Project team to manage system and carry out the required training & knowledge transfer. SI shall handover all the project artefacts and assets after updating all the necessary project documentation. SI shall design Standard Operating Procedures to manage system (including application and IT systems), document the same and train State's Project team on the same

7. IMPLEMENTATION AND ROLL-OUT PLAN

REQUIREMENTS FOR ROLLOUT

a. The solution should be piloted in a few police stations in one or two districts/Commissionerate as a part of extensive field testing and the feedback incorporated before rolling out across Odisha
b. The rollout plan shall be defined date-wise, location-wise, module-wise and training completion and change management completion wise.
c. A detailed rollout checklist should be maintained for migrating application to production as well as for location readiness.
d. SI shall prepare a detailed roll-out plan for each of the Districts in the Phase and get the same approved by the State. SI is also responsible for conducting workshops for the key officers (State Mission Team, District Mission Team, and District Core Team) of the Districts 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.
e. 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 during the design and implementation of CCTNS in the State/UT.
f. One of the important factors that would determine the success of the Police IT implementation in the State is the continuous availability of domain experts to the implementation team. SI shall put together a team of at least five (5) domain experts with a minimum of 10 years of experience in the State Police Department who will work on this project on a full time basis during the entire duration of the project.

INDICATIVE PLAN

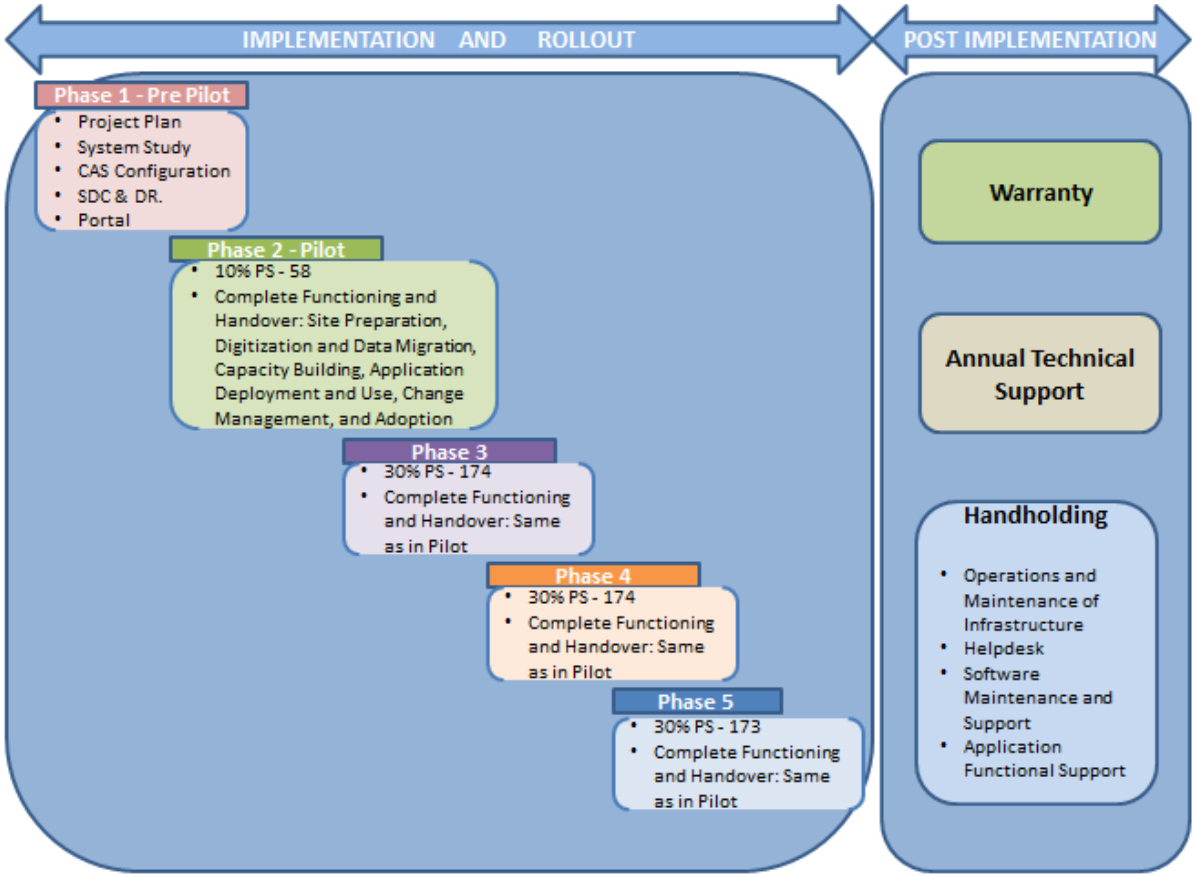
The Implementation and Rollout Plan will follow the following template:

a. Pre Pilot (Phase 1):
   i. Project Plan (Work Plan, Resource Plan, Risk Plan)
   ii. System Study
   iii. CAS Configuration/Customization/Extension
   iv. CCTNS Setup at State Data Center and Disaster Recovery Site

b. Pilot (Phase 2)
   i. To cover 58 (10%) of the Police Stations as detailed below:
      - Bhubaneswar-Cuttack Commissionerate, Bhubaneswar: 23 Police Stations
      - Bhubaneswar-Cuttack Commissionerate, Cuttack: 22 Police Stations
      - Puri District: 3 Police Stations
      - Khurda District: 3 Police Stations
      - Cuttack District: 7 Police Stations

ii. For this phase the Payment Milestone includes complete functioning and handover of the requisite number of Police Stations including but not limited to Site Preparation of these Police Stations, Digitization and Data Migration of the data at these Police Stations, Capacity Building of the personnel at these Police Stations, Application Deployment at these Police Stations and Use of the application by the personnel at these Police Stations, Change Management at these Police Stations, and Adoption and of the system at these Police Stations.

Figure 2 implementation plan



iii. Phase 3 – 30% of the Police Stations

For this phase the Work and Payment Milestone includes complete functioning and handover of the requisite number of Police Stations including but not limited to Site Preparation of these Police Stations, Digitization and Data Migration of the data at these Police Stations, Capacity Building of the personnel at these Police Stations, Application Deployment at these Police Stations and Use of the application by the personnel at these Police Stations, Change Management at these Police Stations, and Adoption and of the system at these Police Stations.

iv. Phase 4 – 30% of the Police Stations

For this phase the Work and Payment Milestone includes complete functioning and handover of the requisite number of Police Stations including but not limited to Site Preparation of these Police Stations, Digitization and Data Migration of the data at these Police Stations, Capacity Building of the personnel at these Police Stations, Application Deployment at these Police Stations and Use of the application by the personnel at these Police Stations, Change Management at these Police Stations, and Adoption and of the system at these Police Stations.

v. Phase 5 – 30% of the Police Stations

For this phase the Work and Payment Milestone includes complete functioning and handover of the requisite number of Police Stations including but not limited to Site Preparation of these Police Stations, Digitization and Data Migration of the data at these Police Stations, Capacity Building of the personnel at these Police Stations, Application Deployment at these Police Stations and Use of the application by the personnel at these Police Stations, Change Management at these Police Stations, and Adoption and of the system at these Police Stations.

TIMELINES FOR DELIVERABLES

These are indicative Timelines

Table 22 Timelines of deliverables

1.	**Preparation of detailed Project plan**	T
1.1.	Work Plan	T+2 Weeks
1.2.	Resource Plan	T+4 Weeks
1.3.	Risk Plan	T+5 Week
2.	**Capacity Building in State**	
2.1.	Preparation of the Training and knowledge transfer Plan	T+3 Weeks
2.2.	Preparation of training material	T+9 Weeks
2.3.	Conducting training for Police personnel	T+62 Weeks
3.	**Phase One: Implementation in Pilot District**	T
3.1.	Customisation of CAS(State)	
3.1.	Refinement of Functional Requirements Specifications (FRS)	T+2 Weeks
3.1.	Preparation of Software Requirement Specification of customisation of CAS(State)(SRS)	T+3.5 Weeks
3.1.	Design Document for Customisation of CAS(State) (HLD, LLD)	T+6.5 Weeks
3.1.	Parametric Customisation of Odisha CAS	
3.1.	Preparation of Test plan	T+7.5 Week
3.1.	Preparation of Test cases	T+9.5 Weeks
3.1.	Preparation of Test report	T+10.5 Week
3.1.	Integration testing of CAS(State)	T+13.5 Weeks
3.1.	User Acceptance testing	T+14.5 Week
3.1.	Acceptance testing, Audit and certification	T+16.5 Weeks
3.1.	Release of CAS(State)	T+17 Weeks
3.2.	Setting of Data Centre	T
3.2.	Site preparation for setting up of Data Centre	T+2 Weeks
3.2.	Setting up of Hardware & Networking infrastructure for data Centre	T+6 Weeks
3.2.	Installation of Database server, Application server etc	T_2+8 Weeks
3.2.	Testing of functioning of DC	T+10 Weeks
3.3.	Setting up of Disaster Recovery	T
3.3.	Setting up of Hardware & Networking infrastructure for DR	T+2 Weeks
3.3.	Installation of Database server, Application server etc	T+5 Weeks
3.3.	Testing of functioning of DR	T+7 Weeks
3.4.	Supply & Commissioning of Hardware at Pilot District	T

3.4.	Preparation of Distribution list for Hardware to the PS	T+1.5 Weeks
3.4.	Identification of Site Preparation need at remote & dilapidated PS	T+2.5 Week
3.4.	Site Preparation at PS	T+6.5 Weeks
3.4.	Setting up of LAN and connectivity at PS	T+8 Weeks
3.4.	Distribution of hardware to PS	T+10 Weeks
3.4.	Testing of functioning of PC & its connectivity	T+10.5 Weeks
3.5.	Rollout of CAS(State) in district (Roll out plan)	T+ 20 Weeks
3.6.	Testing of connectivity & resolution of performance issues	3 Weeks
3.7.	Data Digitization at Pilot Districts	2 Weeks
4.	**State Project Management Unit(SPMU)**	
4.1.	Terms & Condition of SPMU	3 Weeks
4.2.	Preparation of the RFP for selection of SPMU	4 Weeks
4.3.	Selection of the State Project Management Unit & Contract Signing	4 Weeks
5.	**Phase Two: Implementation across the state**	T
5.1.	Supply & Commissioning of Hardware at Police Station	T+20 Weeks
5.1.	Preparation of Distribution list for Hardware to the PS	T+21.5 Weeks
5.1.	Distribution of hardware to PS	T+30.5 Weeks
5.1.	Site Preparation at PS	T+34.5 Weeks
5.1.	Setting up of LAN and connectivity at PS	T+37.5 Weeks
5.1.	Testing of functioning of PC & its connectivity	T+40.5 Weeks
5.2.	Rollout of CAS(State) in district	1.5 Weeks
5.3.	Testing of connectivity & resolution of performance issues	1 Week
5.4.	Data Digitization at Pilot Districts	9 Weeks
5.5.	Maintenance of hardware	