

**E – GOVERNANCE
MISSION MODE PROJECT
(MMP)**

**CRIME & CRIMINAL TRACKING
NETWORK AND SYSTEMS
(CCTNS)**



RFP FOR SELECTION OF SYSTEM INTEGRATOR

CORRIGENDUM - II

Released By:

JK Police

Government of Jammu & Kashmir



TABLE OF CONTENTS

1. REQUEST FOR PROPOSAL DATASHEET..... 3

2. RFP Volume 1 4

A. 6. Scope of Services - System Study, Design, Application Development and Integration 4

6.2.3 Preparation of Solution Design 4

6.4 Site Preparation at Police Stations and Higher Offices 4

3. ANNEXURE 6

A. ANNEXURE X – SERVICE LEVELS 6

B. ANNEXURE XII – INDICATIVE TECHNICAL SPECIFICATIONS 6

C. ANNEXURE XIII – INDICATIVE HARDWARE BILL OF MATERIAL 43

4. RFP Volume 2 49

A. 3. BIDDING PROCESS DETAILS – General Instruction to Bidders..... 49

3.2.9 Earnest Money Deposit..... 49

B. 3. BIDDING PROCESS DETAILS – Bid Opening and Evaluation Process 50

3.4.4 Pre-Qualification Criteria 50



1. REQUEST FOR PROPOSAL DATASHEET

S. No	Information	Details
1	RFP Reference number and date	CHQ/CCTNS/11/2572-76
2	Non Refundable Tender Cost	10,000/-
3	Issuance of RFP Document	18 th Mar, 2011
4	Earnest Money Deposit (EMD/ Bid Security)	2 Crore
5	Last date and Time for submission of written queries for clarifications	7 th April, 2011; 05:00 PM
6	Date, Time and Venue of pre-proposal conference	08 th April, 2011; 10:00 AM; Crime HQ, Jammu
7	Release of response to clarifications on	19 th Apr, 2011
8	Last date, Time (deadline) and Venue for submission of proposals in response to RFP notice	25 th April, 2011; 10:00 AM; Crime HQ, Jammu
9	Date, Time and Venue of opening of Technical proposals received in response to the RFP notice	To be Intimated later
10	Place, Time and Date of Technical Presentations by the bidders	To be Intimated later
11	Place, Time and Date of opening of Financial proposals received in response to the RFP notice	To be Intimated later
12	Contact Person for queries	Deputy Inspector General of Police, Crime
13	Addressee and Address at which proposal in response to RFP notice is to be submitted:	DIG Crime, Crime HQ, Old PHQ Complex, Panjtirthi - Jammu

Deputy Inspector General of Police, J&K (Crime)

Old PHQ Complex, CPO Chowk

Panjtirthi, Jammu

Jammu and Kashmir- 180001

Phone Number: 0191-2561694

Email Address: cctns_jk@ncrb.nic.in, scrbjmu-jk@nic.in



2. RFP Volume 1

A. 6. Scope of Services - System Study, Design, Application Development and Integration

6.2.3 Preparation of Solution Design

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

Following Details added to this Clause:

To ensure integrity and confidentiality, the data collected (both online and offline) at the police location should be digitally signed and encrypted before it is sent from one location to other/ central data center. Hardware Security module should be integrated with the applications in Data Centre in high availability mode and should be able to endure the security and integrity of the signing key, key management and multifactor authentication to access the key and most significantly it should be able to enhance the performance of the complete system by offloading the complete cryptography process to a dedicated appliance. All data interchanged among various police offices and between the users of an application interface, Core application, Police agencies and CCTNS databases should be digitally signed and encrypted using the PKI infrastructure.

6.4 Site Preparation at Police Stations and Higher Offices

The Jammu and Kashmir Police shall provide the necessary minimum constructed rooms/ space permanent construction to the SI. The SI would be responsible for conducting a site survey to identify the exact situation of the sites for CCTNS infrastructure and commissioning. The SI would prepare a site survey report detailing the current status of each site and the enhancements to be made at each site (s) based on the State's requirement and the guidelines of MHA. SI would be responsible to prepare the client sites for setting up the necessary client site infrastructure (The space cannot be used for any purpose other than for delivering the said CCTNS services). State



Government shall arrange for necessary clearances which shall enable the SI to undertake civil, electrical, and mechanical works including but not limiting to installation of electrical equipments, cable laying etc. at the respective sites.

Site preparation at Police Stations & Higher Offices will include but not limited to:

- Provision of Local area network (LAN cables, LAN ports, port Switch)
- Provision of computer furniture for Police Stations
- Ensure adequate power points in adequate numbers with proper electric-earthing
- Earthing and electric cabling as required at the site
- Supply and fixing of furniture like computer tables, chairs and other item shall be carried out to ensure successful site preparation and installation of CCTNS at every Police Station for the smooth functioning of the CCTNS project.

The System Integrator shall cover all the activities necessary to enable the Police Station to setup the client side infrastructure and operate on CCTNS.

Following Details added to this Clause:

The system integrator has to carry out an extensive site study of all Police Stations and higher offices to indentify the exact room for the CCTNS project. The tentative layout of the room is 10x15 sq feet and should accommodate at least 4 persons all the time.

The department of Jammu and Kashmir Police will hand over the rooms to the selected SI for site preparation. The following are the activities that are required to be carried out by the SI for site preparation but are not limited to.

- Providing adequate furniture like 4 computer tables and 4 no of moving chairs.
- Proper flooring and ceiling need to be done at all Police Stations (approx height of room is 10 ft)
- Painting and illumination to be carried out at all Police Stations
- Separate desk for printers, Scanners, fingerprint reader and digital camera, the space needs to be indentified within the room for these items.
- The Firefighting equipment of any higher quality need to be deployed at all Police Stations.
- Power supply fluctuates between 150 – 200 volts at all Police Stations.
- Provision of Local area network (8 No of LAN Ports), Laying UTP cables, Structured Cabling, Installation of Patch Panels, Installation of Wall Mountable Network Rack, Information Outlet CAT 6, Cable Crimping, Installing RJ-45.)



3. ANNEXURE

A. ANNEXURE X – SERVICE LEVELS

Post Implementation Phase SLAs

Service Level Description	Measurement
Infrastructure Availability	RPO (zero data loss in case of failure of Primary DC) should be zero minutes Severity of Violation: High Each instance of non-meeting this service level will be treated as two (2) violations.
<u>Stands Amended as</u>	
Infrastructure Availability	RPO (zero data loss in case of failure of Primary DC) should not be more than sixty minutes. Severity of Violation: High Each instance of non-meeting this service level will be treated as two (2) violations.

B. ANNEXURE XII – INDICATIVE TECHNICAL SPECIFICATIONS

Minimum Technical Specifications for Data Center and Recovery Center:

Stands Amended as:

1. Enterprise Management System

SI hall procure and install EMS in the Data Center for the monitoring of the network.

- The EMS solution should monitor fault, availability and performance of network devices across Management.
- Performance monitoring of network and server.
- Trouble ticketing systems
- EMS components should be from same OEM for out of the box seamless integration capabilities
- EMS should be from ISO 27001 certified OEM. Bidder should provide necessary OEM certificate.

Network Fault Management

The Network Fault Management consoles must provide web based topology map view from a single central console. The system should provide discovery & inventory of heterogeneous



physical SNMP enabled network devices like Hubs (Layer 1), wireless (WAP) devices, Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level.

- Network Fault Management GUI should be Web-based providing views for Navigation, Contents & Components Detail. Navigation view should provide views for Users, Locator and Explorer search. Contents view should provide views for Alarm, Topology, List, events. Components detail should provide Impact, Root cause, Host Configuration, Interfaces & Alarms history information.
- The discovery should be able to identify and model router redundancy using vendor-specific protocols (like VRRP and HSRP support for Cisco devices) so that alarms generated from these virtual addresses are automatically excluded.
- The fault management should be able to discover MPLS links between MPLS routers for isolating problems of link failure due to provider backbone failure or CE MPLS router failure.
- The system must support multiple types of discovery like IP range discovery - including built-in support for IPv6 ,Import data - from pre-formatted files (IPs, ranges, strings or ports),Seed router based discovery - Using route tables and SNMP MIBs, Trap-Based Discovery - whenever new devices are added with capability to exclude specific devices based on IP addresses/ IP Address range
- The solution must use advanced root-cause analysis techniques. The system must deduces the root cause of the problem and in topology it should visually pinpoint single impacting device (in red color), as well as other impacted devices (in green color).
- The tool should provide sufficient reports pertaining to EMS. The tool should generate necessary set of reports pertaining to Network Device Asset Inventory , alarms & availability reports as well as a detailed network asset reports
- The fault management web based console must provide tabs like topology, alarm, interfaces, root cause tab in single GUI. It should provide explorer & search tabs as well as configuration management as integral part of fault manager.
- The Fault management must provide Spotlight views for Router Redundancy, VLAN list and VPN list. When clicked on a particular VLAN from VLAN List, participating devices only for that particular VLAN gets highlighted in the topology map.



- The fault management should display connecting link between two devices and port labels in same web GUI once clicked on a particular link. If there are multiple links between two devices all the multiple links between two devices and their connected port labels must be visible in same web GUI.
- Synchronized Discovery is required in order to reduce effort to discover devices again in performance management engine. Devices once discovered in groups in Fault Management should be imported directly into groups inside performance management engine without a need to run separate discovery in performance management engine.
- The proposed NMS should provide unified workflow between the fault and performance management systems including bi-directional and context-sensitive navigation, such as
 - Navigate from the Topology View to At-a-Glance or Trend Reports for any asset
 - Navigate from the Alarm View to At-a-Glance, Trend or Alarm Detail
- The system should provide capability to measure & report on response time for common TCP/ IP applications using test on routers:
 - HTTP, HTTPS, DNS, FTP, SMTP, SNMP, POP3, ICMP, Jitter
- The system should support secure device configuration capture and upload and thereby detect inconsistent “running” and “startup” configurations.
- The proposed system should be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements like Capture running & startup configuration, Upload configuration , Upload firmware , Write startup configuration.
- The proposed tool should display configuration changes differences in GUI showing modified, remove, masked lined from last captured network configurations for routers and switches. Also this should be able to identify which user has made changes or modifications to device configurations through Fault Management Tool.
- The System should be able to monitor Quality of Service (QoS) parameters configured to provide traffic classification and prioritization for reliable traffic transport. The solution should be able to discover and model configured QoS classes, policies and behaviors.
- The proposed service management system should provide a detailed business service dashboard view indicating the health of each of the departments/ offices in the organization and the health of the services they rely on as well as the SLAs.



- The system should provide an outage summary that gives a high level health indication for each service as well as the details and root cause of any outage.
- The system must be capable of managing IT resources in terms of the business services they support, specify and monitor service obligations, and associate users/ Departments/ Organizations with the services they rely on and related Service/ Operational Level Agreements.

Secure Network Configuration Management

- The system should provide both window and web based consoles for accessing the EMS.
- The system should have web based interface with user id and password authentication.
- A user attempting to modify a device configuration from Network Operation Console should be forced to choose from a list of users that have the “configuration change approval” privilege to obtain approval from. The approver should be notified of the request through email.
- The approver should be able to view the proposed configuration change and choose to approve or deny from links within the email. The requester should be then notified by email of the approval or denial.

Performance Management System

System should provide comprehensive end-to-end Network performance management across key parts of the network infrastructure. The proposed Network Performance Management System must provide the following features:

- The performance management should integrate with fault management to forward performance alarms by defining notified rules and associated alarms shall be visible against monitored device in fault manager console
- The system shall identify over-and under-utilized links and assist in maximizing the utilization of current resources. The proposed system shall provide Performance of Network devices like CPU, memory & buffers etc, LAN and WAN interfaces and network segments.
- The proposed system must have a cognos based report authoring tool built-in which will enable complete customization flexibility of performance reports for network devices and monitored servers.



The tool should provide a live trend diagram displaying the various resource utilization levels of various critical devices and links in the managed infrastructure.

The tool should provide a live exceptions list displaying the various health and threshold exceptions that are occurring in the managed infrastructure.

The proposed system should use intelligent alarm de-duplication algorithms to learn the behaviour of the network infrastructure components over a period of time.

The proposed system should be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits.

Baseline setting should be as follows out-of-the-box:

- For a daily Health report, the baseline should be 6 weeks (42 days) by default.
- For a weekly Health report, the baseline should be 13 weeks by default (for a weekly my Health report, it should be 6 weeks).
- For a monthly Health report, the baseline should be 12 months by default. The Proposed Performance Management must provide following charts for all kinds of Health Reports:
- Availability Chart ,Availability Chart (CIO Summary Report) Average Health Index Chart ,Average Network Volume and Call Volume Charts, Avg. Response Chart Bandwidth Utilization Chart, Element Variable Report Element Volume vs. Baseline Chart, Exceptions Detail Report ,Exceptions Detail Table ,Exceptions Summary Report, Failed Attempts Chart ,Health Index Change Leaders Chart ,Health Index Leaders Chart , Jitter Chart ,Latency Chart , Network Interface Utilization Chart Network Volume Chart, Paging Rate Chart ,Partition Utilization Chart etc.
- Performance Management mapping should match elements such as routers and switches to corresponding models in Fault Management so that Fault Manager can provide performance reporting options for the models in Network Operation Console. Further element to model mapping should allow performance alarms to be visible for the respective model in fault management Network Operation Console.
- Proposed performance management should be integrated with proposed fault management using in built single sign on mechanism which should allow fault manager



users to access performance management user interface without a need to re-login. SSO Users can be imported from LDAP directory or can be defined inside SSO component.

Traffic analysis system should be deployable for optimum performance.

The solution should be of the type passive monitoring without a need to install any probe or collector for data collection. The solution must provide the following flow based metrics: Rate utilization, Byte count, Flow count, IP hosts with automatic DNS resolution, IP conversation pairs with automatic DNS resolution, Router/ Interface with automatic DNS SNMP name resolution, protocol breakdown by host, link, TOS or conversation, Utilization by bit pattern, matching of the TCP ToS field, AS number, BGP next hop address, IPv6 address.

The network traffic analysis system must be from same OEM providing Network Fault & Performance Management System for seamless integration.

The proposed traffic analysis system should provide visibility into new and unknown traffic patterns which is critical for ensuring the performance of networked applications, as well as identifying security risks. It should provide real-time analysis of traffic behaviour for every client and server in infrastructure to help ensure network delivers application services reliably and securely.

Traffic Analysis System must provide Search for any traffic using a specific configurable destination port, or port range, autonomous system (AS) number, BGP next hop IP address, ToS bit, clients or servers that are experiencing more than a specified number of TCP resets per hour, IPv4 or IPv6 conversation bad IP Header, unreachable destination, TTL expired, trace route requests, MAC addresses, TCP flags, VLAN.

The proposed solution must keep and report on unique hosts and conversations per day for each monitored interface

The proposed tool must provide availability and performance for server nodes and deliver scalable, real-time management of critical systems.

The proposed tool should be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, log files ,daemons etc. It should be possible to configure and define thresholds for warning/critical states and escalate events to event console of enterprise management system.

The proposed tool should integrate with network performance management system and support operating system monitoring for various platforms including Windows, LINUX/ UNIX.



Proposed solution should provide light weight monitoring agents reporting to network performance server.

Application Performance Management

System should determine if the root cause of performance issues could be inside the monitored application, in connected back-end systems or give indications about problems at the network layer from a single console view.

System should monitor .NET/ Java based applications.

System should proactively monitor 100% of real user transactions 24x7 identifying the user name and IP address; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes.

System must have ability to monitor transactions that include XML, SOAP and other identifiable protocols over HTTP/S.

System must be able to monitor complex web pages comprised of multiple components like frames, Java-script, images, and other HTTP components.

System must be able to combine multiple transactions into a logical business process.

System should monitor end-to-end, REAL user transactions

System should not allow end users to install/ upload software on to their desktops.

System should provide for self-monitoring of internal health with reports pages and alerts on errors or issues.

System should have provision for automatic transaction discovery, for example by setting up some bounding parameters to describe transactions like the web site, the language, and parameters (such as post, query, and cookies).

System must support monitoring on:

- Transactional level
- Business Process level
- User and User group level



System shall be capable of real-time detection of errors and performance problems that affect the ability of customers to execute successful transactions, thus able to proactively identify errors and problems customers are experiencing and enable trouble shooting to begin before an increasing number of customers are impacted and call for support.

The management reports from the solution allows viewing the details for each defect and aggregate like defects into an incident, and also provides the ability to quickly see commonality across defects while still providing the ability to drill down to view the metrics for a specific defect.

System should be able to see exactly what request was sent by the end users' browser sent and the response by the application, when a defect occurs.

System must be able to provide root-cause probability graphs for performance problems showing the most probable root-cause area within application infrastructure.

System must quickly create a baseline for performance over a period of time from the live production application.

System must have ability to automatically generate and distribute PDF formatted reports via email on a daily, weekly, or monthly basis.

System must be able to provide the ability to create user groups based on location/geographic area.

System must have ability to create user groups based on URL string, cookie value, XML attribute, IP Addresses or HTTP header

System must be able to extract data from Http request header and body to assist in identifying transactions or extract user, session and other parameters.

Solution should generate a graphical map of the complex transactions showing the path of the transaction across multiple application components. Map view should also highlight any triage to enable quick identification of the problem.

System must provide ability to monitor performance of applications going up to the method level of execution (Java/ .Net method) 24x7 in production environments with negligible impact on monitored application (minimum overhead).

All application stakeholders (i.e. DBA, Operations, and Application developers) must get performance data pertaining to their specific areas from single Java/ .NET Application Agent within the application server and be able to display them on dashboards



Helpdesk Management

The proposed ITIL-based Helpdesk Management System must provide the following features:

- The proposed helpdesk solution must provide flexibility of logging, viewing, updating and closing incident manually via web interface. The web interface console would also offer power-users tips.
- The proposed helpdesk solution must support all ITILv3 processes like request management, problem management, configuration management and change order management with out-of-the-box templates for various ITIL service support processes. Bidder should provide ITIL v3 certification letter on all processes.
- Each incident must be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.
- The proposed helpdesk solution must be able to provide flexibility of incident assignment based on the workload, category, location etc.
- Each escalation policy must allow easy definition on multiple escalation levels and notification to different personnel via window GUI/ console with no or minimum programming.
- The proposed helpdesk knowledge tools solution must provide grouping access on different security knowledge articles for different group of users.
- The proposed helpdesk solution must have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.
- The proposed helpdesk solution must support tracking of SLA (service level agreements) for call requests within the help desk through service types.
- The proposed helpdesk solution must be capable of assigning call requests to techal staff manually as well as automatically based on predefined rules, and should support notification and escalation over email, web etc.
- The proposed helpdesk solution must integrate tightly with the Knowledge tools and CMDB and should be accessible from the same login window.
- The proposed helpdesk solution must have a built-in workflow engine. The proposed helpdesk solution must support Non-linear workflows with decision based branching



and the ability to perform parallel processing. It should also have a graphical workflow designer with drag & drop feature for workflow creation and updates.

- It should support remote management for end-user & allow analysts to do the desktop sharing for any system located anywhere, just connected to internet.
- Web based remote desktop management feature should be supported as part of helpdesk troubleshooting
- It should allow IT team to create solution & make them available on the end – user login window for the most common requests

EMS integration with Helpdesk:

When certain user tries to make any change on network device through fault management console a helpdesk ticket should be generated automatically. The Service Desk operator must have the ability to view the proposed configuration change once the ticket is approved the user is automatically notified and is able to proceed with the change. The proposed Fault Management Solution must support integration with proposed help desk or trouble ticketing system such that integration should Associates alarms with Service Desk tickets in the following ways:

- Manually creates tickets when requested by Fault Management GUI operators
- Automatically creates tickets based on alarm type
- Provides a link to directly launch a Service Desk view of a particular ticket created by alarm from within the Network Operation console.
- Maintains the consistency of the following information that is shared between alarm and its associated Service Desk ticket including status of alarms and associated tickets and current assignee assigned to tickets.

Helpdesk ticket number created for associated alarm should be visible inside Network Operation Console .It should be integrated in a way that Helpdesk incident can be launched once clicked on ticket number for associated alarm from within Network Operation Console.

The proposed network fault management system should integrate with the helpdesk system by updating the Asset with CI information to support viewing history or open issues in helpdesk on the particular managed asset and associate an SLA to the ticket in the helpdesk. The proposed network fault management system should attach an asset identifier when submitting a helpdesk ticket. In case the asset is not found in the helpdesk database, it should



be automatically created prior to submitting the ticket. NMS console must show associated helpdesk ticket number for the alarms that generated those tickets.

SLA's violation on monitored end user response time must open a helpdesk incident out of the box. Proposed performance management system and traffic analysis system must integrate through common network performance portal depicting drill down performance views on performance utilization and type of traffic flowing through monitored interface.

Identity & Access Management

Requirements for the Identity and Access Management System

The Identity and Access Management Solution consisting of Identity Management, Provisioning, Password Management, Web Access Management, Web SSO, and Single Sign-On for thick client applications and Server Access Control must be from a single OEM to enable smooth and easy out-of-the-box integration among the various sub components.

The bidder shall provide undertaking by OEM of Identity and Access Management Solution whose software products have been offered for associating Project Manager during the project execution period.

The proposed Server Access Control Solution should be able to protect critical server infrastructure and minimize security risks by regulating access to confidential data and mission critical services. The solution should provide policy-based control of who can access specific systems, what they can do within them, and when they are allowed access. Specifically, it should proactively secure access to data and applications located on Linux, UNIX and Windows system servers throughout the infrastructure.

Server Access Control

The Host Access Control should be able to protect business critical infrastructure and minimizes security risks by regulating access to confidential business data and mission critical services. The solution should provide policy-based control of who can access specific systems, what they can do within them, and when they are allowed access.

Host based security solution must allow controlling of access to system resources including data files, devices, processes/daemons and audit files.

- The solution should Self-protect itself – Must be able to prevent hackers with root access from circumventing or shutting down the security engine. Must use a self-protected database for storing all security information.



- The solution should provide Rights Delegation - Must provide the ability to designate specific users as Administrators, Auditors, and Password Managers etc with appropriate rights. Must also provide the ability to designate specific users as Subordinate or Group Administrators, to manage users and file permissions for their Group
- The solution should support cross platform Management – Must support management and policy distribution across Windows, Linux and UNIX platforms from a central management console. It must support the deployment of the same policies across multiple servers ensuring consistency of security policies across machines in the enterprise.
- The solution must provide capability to allow access to sensitive resources only through approved programs.
- Administrators must be able to define critical files that are not supposed to change. If these files are modified, the process that checks the sensitive files must find that the files have changed and write an audit record.
- The solution should allow protection of files on even non-NTFS file systems like FAT and CDFS.
- The solution must provide support for IPv6 and FIPS140-2 and must provide Services and Registry Values Protection on Windows
- The solution must provide administrative password checkout function. It should provide workflow for requesting and checking out a system-generated. The solution should provide the functionality to force the user to check the password in once their task is completed, or PUPM should provide the capability to be configured to automatically check the password in after a specific time period; and it can be a manually forced check in as well.
- The privilege user password management (PUPM) must provide a fully functional and customizable workflow that provides common out-of-the-box use cases for PUPM. The solution must provide a break glass feature. A break glass scenario occurs when a privileged user needs immediate access to an account that they are not authorized to manage. Break glass accounts are privileged accounts that are not assigned to the user according to their role. However, the user can obtain the account password immediately, without approval, if the need arises. This eliminates the possibility of a



delay for an admin to approve the request. All transactions related to the break glass scenario must securely be logged for audit purposes.

- The solution should provide a feature to eliminate passwords from scripts. Via PUPM, it should be possible to replace hard-coded passwords in scripts with privileged account passwords that are generated by PUPM only when needed.
- The solution should provide a unified web based console which consolidates all aspects of privileged user management under a single console — host access control and privileged user management across physical and virtual systems, devices and applications.
- The PUPM must support a wide range of virtualization platforms including but not limited to: VMware ESX, Solaris 10 Zones, LDOMs, Microsoft Hyper-v, IBM VIO, AIX LPAR, HP-UX VPAR, Linux Xen and Mainframe x/VM, providing for more consistent security management of access control risks across these virtual partitions, in addition to physical platforms.

Web Access Management and Web Single Sign-On

The Web Access Management solution should provide a secure access to business content, applications, and information across its organization, while allowing management of multiple user communities across the organization.

The proposed web access security management solution:

- Must include out-of-the-box support for specified relevant third-party technologies - Authentication, PKI, and smart cards.
- Must provide access to only those applications/ resources that the user/ customer has authority to.
- Must not have an agent installed on application, database or directory servers where users need to be provisioned.
- Must be able to integrate with user administration product
- Web access management system itself should use 128-bit RC4 encryption between its distributed components.
- Solution must support all following authentication method: Passwords, Two factor tokens, X.509 certificates, Passwords over SSL, Smart cards ,Combination of methods ,Forms-based ,Custom methods ,Full CRL & OCSP support



- Web access management system should support off-line generation and management of encryption keys using N cipher with the strength (size of encryption key) of the encryption algorithms of 128-bit RC4
- Strong authentication (such as the use of a smart card) should be required to access certain administrator functions
- Web access management system should support single sign-on across security domains.
- If a user is authenticated at a low level of security (e.g., password), then they should be forced to re-authenticate when they attempt to access a more sensitive resource (e.g., one protected by a token card).
- The priority of these authentication methods should be Administrator specified .It should not be hard-wired into the product, and Administrator should be able to control the priority of each Authentication method. 1000 levels of priority should be supported.
- Solution should support both session and idle timeouts on a per-resource basis.
- Administrator should be able to specify rules for generating and rolling over encryption keys (e.g., periodically, or upon command).
- Authentication management system should be capable of supporting automated fallback to alternative authentication systems.
- Solution should support directory chaining.
- Solution should provide protection from cross-site scripting & SQL Injection attacks.
- Solution should support time or location-based policies.
- Administrator should be able to create a policy for any user, any group (including dynamic groups), any role, or even any ad-hoc set of users who share certain attributes.
- Administrator should be able to integrate dynamic/ external data (at run-time) in the enforcement of my policies via a Web service.
- Solution should support controlled “impersonation” of users allowing certain users to temporarily use the entitlements of other users without sharing of passwords.
- Solution should support fine-grained control of access to file, page, or objects.
- Solution should support full replication of all components.
- Solution should support automatic failover and failover between the clusters
- Solution should support 4 & 8-way SMP servers.
- Solution should do dynamic load balancing across all servers.



- Solution should also load balance across directories.
- Solution should provide “2nd-level caching”, so that recently used policies are separated out into a separate cache. And these caches should be tunable for each environment; also the caches should be either flushed or refreshed on administrator command.
- Solution should work with existing user directory.
- API should support workflow capabilities.
- There should be an API to allow custom directories to be used for user storage.
- Must log users into any resource requiring a sign-on which includes client server applications, email, databases applications and Web enabled applications. The solution must provide capabilities to manage all environments from access management perspective.
- Integration between Web SSO and enterprise SSO should be out of the box.

Role, Compliance and Identity Management

- The proposed solution should allow efficiently sort through extremely large volumes of user and privilege information to quickly discover potential roles.
- The proposed solution should provide a clean set of user entitlement data to support role management efforts.
- The proposed solution should periodically validate that users, roles or resources have appropriate access rights to meet compliance requirements.
- The proposed solution should provide role custodians or resource owners to view the current entitlements of their respective entities, then certify that they are appropriate or identify privileges that should be removed.
- The proposed solution should provide a centralized engine that establish and enforce a consistent set of identity compliance policies to minimize security risk.
- The proposed solution should prevent Identity vulnerabilities using consistent identity compliance policy enforcement.
- The Solution should have built-in reputed reporting engine such as Business Objects.
- Must provide centralized administration of user-ids and password management.
- Must provide a central directory of users, their real-world business information, their accounts, and their access rights across the enterprise without requiring changes to end-systems.



- Must allow accounts on end-systems to be discovered, and linked to users within the administration utility, which can be subsequently used as the single point of administration.
- Cross Platform/ Application - Must provide easy and cost-efficient administration of users and resources across enterprise security systems and directories like NT, UNIX, Microsoft Exchange and others specified.
- Scalable - Must be scalable, open, extensible, and built around standards-based LDAP/ X.500 technology.
- Audit - Must provide a consolidated audit trail of administrative operations.
- Other Requirements
- Must have APIs to enable additional user management operations on UNIX, NT over and above the default operating system account set-up.
- Must have LDAP interface to enable queries/ updates by authorized third-party customer tools.
- Must support enforcement of a centrally-defined security policy, e.g. for access rights, user names, password lengths
- Role-based Administration
- Role Based & Rule Based User Provisioning.
- Must provide access rights based on job function to support implementation of role-based administration.
- Must have a web-interface for simplified user administration that can be used by HR, business managers to introduce and delete users, and assign them to job functions
- Should be able to integrate with HR application, CRM application so as to enable creation of user ids based on data fed to CRM and HR applications.
- Must allow users to access critical data through a single, secure login, while reducing security/ password administration.
- Should have an embedded work flow which would help in automating routine tedious tasks like approval processes.
- Must provide advanced Web support, to allow for smooth access and personalization of the user interface for each user. Once a user has been authenticated to the sign on



system, access to all authorized Web applications and resources must be handled by this system.

- Must be easy to deploy and maintain.
- Must work across specified platforms, databases, and applications.
- Must include out-of-the-box support for specified relevant third-party technologies - Authentication, PKI, and smart cards.
- Must have a highly scalable architecture and must allow incremental implementations.
- Must provide access to only those applications/ resources that the user/ customer has authority to.
- Must be able to integrate with user administration product.
- Provide capabilities to perform recertification of identities across the Enterprise.
- Perform Identity Auditing for entitlement violations and validations.
- Out-of-Box integration with Web Services.
- Should provide capabilities to have Corporate Directory as well as Provisioning Directory.

Security Log Record Collection & Management

- The system shall provide a graphical user interface/ wizard to rules for normalizing custom log sources or modifying existing integrations
- The system shall provide automated update mechanism for Content (product integrations and reports). This process shall occur seamlessly and transparently without any customer intervention as part of the subscription update process.
- "The system shall support the following methods for log collection :
- Windows Management Instrumentation, Syslog, Open Database Connectivity (ODBC), Text Log (flat file), Open Platform for Security (OPSEC)"
- The system shall provide a mechanism to monitor the current status and relative health of the logging infrastructure.
- The system shall have the capability to drag and drop building of custom queries & reports
- The system shall have the capability for updates delivered and applied via an update service provided by the vendor to keep the system up-to-date. This includes the agents and it should be pushed centrally without having to reinstall the agents.



- The system shall have a secure and preferably embedded log repository to store logs that does not require separate database expertise to administer and manage.

Data Loss Protection

- The solution should protect against all relevant user activity including use of a Web browser, e mail, launching applications or installers, printing documents and copying files to removable media such as a USB thumb drive. The solution should use application and device names along with full content inspection to leverage identity, context and concepts to accurately evaluate user activity while reducing unwanted alerts.
- The solution should perform an unlimited number of tasks, each with its own set of defined local or remote scanning locations. Tasks can be executed on-demand or during scheduled times. The solution should deploy entirely within the file server, repository or collaboration server, or deploy as a remote scanning server. The highly scalable and distributed architecture allows data to be scanned at rates exceeding 500GB per hour. Once sensitive information is discovered, it can be deleted, copied or moved to another location. Source files can even be replaced with a stub file of the same name containing an informational message. Also, source document properties can be set to specific values for use in downstream analysis and control.
- The solution should exclude known application program files which are positively identified from the National Software Reference Library (NSRL) maintained by the US National Institute of Science and Technology (NIST). The solution should provide deep content inspection with the ability to leverage identity, context and concepts within detection methods, reduce the possibility of tagging a document incorrectly and ensures that all potential threats are controlled.
- The solution should protect and control messages that are sent within the organization and accessed by Web e-mail applications and mobile devices such as Blackberry and Treo. The solution should provide direct Exchange and Lotus integration and not just scanning of logs and libraries. E-mail integration provides superior filtering of e-mails and reduces internal e-mail information risks.
- The solution should take the right action once a violation is found. The message can be blocked, quarantined, encrypted or ingested for monitoring and review. Additionally the



user should be warned or informed that the message they are about to send is in violation of policies. The solution should prevent users from inadvertently sending personally identifiable information via OWA or iNotes.

2. Server Load Balancer

- 10/ 100/ 1000Mbps Ethernet Ports – minimum 2 ports upgradeable to 4 ports
- Memory: Minimum 4 GB
- Minimum of 2 Gbps throughput
- Minimum of 1 Gbps SSL throughput
- Minimum of 4000 SSL connections scalable to 7500 SSL connections
- Server Load Balancing Mechanism
 - Cyclic, Hash, Least numbers of users
 - Weighted Cyclic, Least Amount of Traffic
 - NT Algorithm/ Private Algorithm/ Customizable Algorithm/ Response Time
- Redundancy Features
 - Supports Active-Active and Active-Standby Redundancy
 - Segmentation/ Virtualization support along with resource allocation
- Server Load Balancing Features
 - Server and Client process coexist
 - UDP Stateless
 - Service Failover
 - Backup/ Overflow
 - Direct Server Return
 - Client NAT
 - Port Multiplexing-Virtual Ports to Real Ports Mapping
 - DNS Load Balancing
- Load Balancing Applications
 - Application/ Web Server, MMS, RTSP, Streaming Media
 - DNS, FTP- ACTIVE & PASSIVE, REXEC, RSH,
 - LDAP, RADIUS
- Content Intelligent SLB
- SLB should provide protection against DoS/ DDoS attack
- HTTP Header Super Farm
- URL-Based SLB
- SLB should support below Management options
 - Secure Web Based Management
 - SSH
 - TELNET
 - SNMP v1, 2, 3 Based GUI
 - Command Line



3. Link Load Balancer (may be proposed if State has to build own DC in case SDC's is not operational)

- 10/100/1000Mbps Ethernet Ports – minimum 2 ports upgradeable to 4 ports
- Memory: Minimum 2 GB
- Minimum of 2 Gbps throughput
- Link Load Balancing Algorithm
 - Round robin, weighted round robin, response time, shortest response etc.
- Link Load Balancer should support below Management options
 - Secure Web Based Management
 - SSH
 - TELNET
 - SNMP v1, 2, 3 Based GUI
 - Command Line

4. Production CAS (State) Application Services related servers (Web, Portal, Application, Database, Directory, etc)

Blade Chassis Specification

- Single blade chassis should accommodate minimum 9 (Quad core Processor)/ 18 (Dual core Processor) or higher hot pluggable blades.
- Processor should be latest series/ generation for the server model being quoted (Xeon processor Preferred)
- 6U to 12U Rack-mountable
- Dual network connectivity for each blade server for redundancy should be provided. Backplane should be completely passive device. If it is active, dual backplane should be provided for redundancy.
- Should accommodate latest high speed processor in compatible with the OEM's of blade servers.
- Should have the capability for installing industry standard flavors of Windows, Linux and Unix Operating environments.
- Single console for all blades in the enclosure or KVM Module.
- DVD ROM can be internal or external, which can be shared by all the blades allowing remote installation of S/W and OS.
- Should provide external USB port.
- Two hot-plug, redundant Ethernet modules with minimum (8 – 10) x 1Gbps Ethernet ports (cumulative) having L2/ L3 functionality.
- Two hot-plugs/ hot Swap redundant 4 Gbps Fiber Channel for connectivity to the external Fiber channel Switch and ultimately to the storage device.
- Power Supplies
 - Hot Swap/ hot plug redundant power supplies to be provided.
 - Power supplies should have N+N. All Power Supplies modules should be populated in the chassis.
- Hot Swappable/ hot pluggable and redundant Cooling Unit.
- Management



- Systems Management and deployment tools to aid in Blade Server configuration and OS deployment.
- Remote management capabilities through internet browser.
- It should provide Secure Sockets Layer (SSL) 128 bit encryption and Secure Shell (SSH) version 2 and support VPN for secure access over internet.
- Ability to measure power historically for servers or group of servers for optimum power usage.
- Blade enclosure should have provision to connect to display console/central console for local management like trouble shooting, configuration, system status/ health display.
- Built in KVM switch or Virtual KVM feature over IP.
- Dedicated management network port should have separate path for management.
- Support heterogeneous environment: AMD, Xeon and RISC/ EPIC CPU blades must be in same chassis with scope to run Win2003/ 2008 Server, Red Hat Linux/ 64 Bit UNIX, SUSE Linux /64 Bit UNIX /Solaris x86.

Blade Servers (Web, Portal, Application, Directory, etc...)

- Blade can be half/ full height with I/O connectivity to backplane.
- 2 Quad core @ 2.0 GHz or above with 4 MB shared L2 cache, 1066 MHz / 2000MT/s FSB
- Processor should be latest series/ generation for the server model being quoted (Xeon processor Preferred)
- Min 32 GB FBD/ DDR3 RAM with minimum 8 no. free slots for future expandability.
- Minimum Memory: 32 GB scalable to 128 GB per blade
- The Blade should have redundant 4 Gbps Fiber Channel HBA (only for database server)
- Min 2 X (1000BASE-T) Tx Gigabit/ equivalent or better LAN ports with TCP/ IP offload engine support/ dedicated chipset for network I/O on blade server.
- 2 x 146GB HDD or more hot plug/ hot swap system disk with mirroring using integrated raid 0,1 on internal disks or min 16 GB compact flash card to be provided. It should be possible to hot swap the drives without shutting down the server.
- VGA/ Graphics Port/ Controller.
- Should support heterogeneous OS platforms.

Blade Servers for Infrastructure Services (EMS, Backup, DNS, Antivirus, etc...)

- Blade can be half/ full height with I/O connectivity to backplane.
- 2 Quad core @ 2.0 GHz or above with 4 MB shared L2 cache, 1066 MHz/ 2000MT/s FSB
- Processor should be latest series/ generation for the server model being quoted (Xeon processor Preferred)
- Min 16 GB FBD/ DDR3 RAM with min 8 Nos. free slots for future expandability.
- Minimum Memory: 16 GB scalable to 128 GB per blade.
- The Blade should have redundant 4 Gbps Fiber Channel HBA
- Min 2 X (1000BASE-T) Tx Gigabit/ equivalent or better LAN ports with TCP/ IP offload engine support/ dedicated chipset for network I/O on blade server.
- 2 x 146GB HDD or more hot plug/ hot swap system disk with mirroring using integrated raid 0,1 on internal disks or min 16 GB compact flash card to be provided. It should be possible to hot swap the drives without shutting down the server.



- VGA/ Graphics Port/ Controller
- Should support heterogeneous OS platforms

Database Server

- Minimum 4x Quad core processor with 2.1 GHz or above with 1066 MHz FSB/ 2000MT/s is scalable up to 8 processors 8 physical processor with minimum 4 MB L3 cache per processor.
- Processor should be latest series/ generation for the server model being quoted (Xeon processor Preferred)
- OS support: Microsoft® Windows Server 2003/ 2008, Enterprise Edition/ Red Hat® Enterprise Linux 5 & 4 AP/ SUSE® Linux Enterprise Server 9/ Solaris for x86.
- Memory (RAM): Min 64 GB scalable to 256 GB.
- RAID controller with RAID 0, 1, 5, 6 with 256 MB cache.
- HDD hot pluggable: 4 x 146 GB 2.5" 10K RPM HDD or more.
- Disk bays: Support for min 8 small form factor hot plug SAS/ SCSI hard drives in disk drive carriers.
- At least 4 x 10/ 100/ 1000 Mbps Ethernet ports or more.
- 2 x 4 Gbps Fiber Channel Ports.
- Ports Rear: Two USB ports (Ver 2.0); RJ-45 Ethernet; keyboard and mouse;
Front: One USB (Ver 2.0)
- Graphics controller: SVGA/ PCI bus/ ATI® ES 1000/ min 16MB SDRAM std/max/ 1280x1024 at 16M colors
- Optical/ diskette: 8X/ 24X slim-line DVD ROM drive shared across chassis
- Security: Power-on password/ boot without keyboard.
- Power supplies: Hot Plug/ Swap redundant power supply to be provided
- Management feature to identify failed components even when server is switched off.
- Rack Mountable
- It should provide Secure Sockets Layer (SSL) 128 bit.
- Encryption and Secure Shell (SSH) version 2 and support VPN for secure access over internet.
- Should be able to manage systems through a web-browser.



5. Storage and Backup Solution

SAN Switches

- Min 16 Active Ports (each with minimum port speed 4 GB) within same switch upgradeable to 24 port with minimum 2 Nos. of additional 10/ 8 GBBS FC ports.
- All cable of length of 10 meter each and accessories for connecting Servers/ Devices to SAN.
- Should have capability of ISL trunking of minimum 8 ports.
- Should support multiple OS.
- Non disruptive subsystem maintenance.
- Should have dual hot plug/ hot swap fans and hot plug/ hot swap power supplies switching and service modules
- Should have web based management software for administration and configuration.
- Non disruptive microcode/ firmware upgrades and hot code activation.
- Switch shall support in built diagnostics, power on self test, command level diagnostics, online and offline diagnostics.
- Should support hardware ACL based Port security, Port Zoning and LUN Zoning.
- Should support Secure Shell (SSH) encryption to provide additional security for Telnet sessions to the switch.
- Should support multilevel security on console access prevent unauthorized users from altering the switch configuration
- Should support Fiber Channel trace route and Fiber Channel Ping for ease of troubleshooting and fault isolation
- Should support the following diagnostics:
 - Online Diagnostics
 - Internal Loopbacks
 - FC Debug
 - Syslog
 - Online system health
 - Power on self test (POST) diagnostics
- Should support Applications for device management and full fabric management. The management software shall be able to perform following:
 - Fabric View
 - Summary View
 - Physical View
 - Discovery and Topology Mapping
 - Network Diagnostics
 - Monitoring and Alerts



Storage Area Network

- SAN controller
 - Dual Active Controller
- Cache
 - 8 GB Total Mirrored Cache for Disk IO Operations scalable to min 16 GB
- Host interface
 - 4 host ports per controller, Fibre Channel (FC), 4 Gbps per port
- Drive interface
 - 4 drive ports per controller—Fibre Channel (FC) Switched or FC Arbitrated Loop (FC-AL) standard per controller, 4 Gbps per port
- RAID levels Supported 0, 1, 5, 6
- Fans and power supplies
 - Dual redundant, hot-swappable/ hot pluggable
- SAN support
 - Box should be compatible of SAN environment
- SAN specifications shall have the following
 - The storage array shall be configured with at least 8 GB cache scalable to min 16GB mirrored across two storage controllers for disk I/O operations.
 - Storage subsystem shall support 300 GB/ 450/ 600 or higher FC/ SAS 10K RPM disks. 750 GB/ 1TB or higher SATA/ FATA/ equivalent 7200 RPM drives in the same storage array.
 - Presently, the storage sub system shall be configured with 300 GB of Performance drives and 750 GB or higher on SATA/ equivalent for archiving purpose.
 - The storage system must provide upgrade path to larger or future array controller and software technology by controller upgrade or data migration.
 - The storage array proposed should have an upgrade path from the earlier generation product to the current generation product. Hence the bidder should provide the solution data migration from existing array to new array or upgrade the array.
 - All the necessary software to configure and manage the storage space, RAID configuration, logical drives allocation, virtualization, snapshots (including snap clones and snap mirrors) for entire capacity etc.
 - Redundant power supplies, batteries and cooling fans and data path and storage controller.
 - Load balancing must be controlled by system management software tools.
 - The Multi-path software should support supplied or heterogeneous storage and operating.
 - The storage array must have complete cache protection mechanism either by de-staging data or providing complete cache data protection with battery backup for up to 72 hours or more.
 - The Storage should have at least 2ports of 4 Gbps Frontend ports and 2 no's of back end ports of 4Gbps"
 - The storage array must have the capability to do array based remote replication using FCIP or IP technology.
 - The storage array should support block level Synchronous and Asynchronous replication on homogenous or heterogeneous storage arrays.



- The storage array should support Operating System Platforms & Clustering including: Windows Server 2003 (Enterprise Edition), Sun Solaris, HP-UX, IBMAIX, Linux / Solaris for x86. Any software or license required to enable connectivity to all these OS should be included.
- Storage should support non-disruptive online firmware upgrade for both Controllers and disk drives.
- The storage array should support hardware based data replication at the Block level across all models of the offered family.
- The storage should provide automatic rerouting of I/O traffic from the host in case of primary path failure.
- Should provision for LUN masking, fiber zoning and SAN security.
- Should support storage virtualization, i.e. easy logical drive expansion & automated load leveling across new drives to minimize performance bottleneck.
- Should support hot-swappable physical drive raid array expansion with the addition of extra hard disks
- The storage system should be scalable from 20TB to 60TB of raw capacity using 40% on Fiber Channel drives and 60% on SATA/ equivalent drives using the same configuration
- Should be able to support clustered and individual servers at the same time.
- Should be able to take "snapshots" of the stored data to another logical drive on a different Disk/ RAID Group for backup purposes
- Should be configured with "snapshots and clone (local and remote)", licenses for the storage & clone features should support resync.
- Vendor should also offer storage performance monitoring and management software.
- The vendor must provide the functionality of proactive monitoring of Disk drive and Storage system for all possible hard or soft disk failure

Tape Library

- Tape drives
 - Minimum 2 latest generation LTO drives. The State can size for more as per their requirements.
- Interface
 - Fiber Channel Interface

Other Specifications

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



Backup Software

- The proposed Backup Solution should be available on various OS platforms such as Windows and UNIX platforms and be capable of supporting SAN based backup/ restore from various platforms including UNIX, Linux, and Windows etc.
- Centralized, web-based administration with a single view of all back up servers within the enterprise. Single console must be able to manage de-duplicated and traditional backups.
- The proposed backup solution should allow creating tape clone facility after the backup process.
- The proposed Backup Solution has in-built frequency and calendar based scheduling system.
- The proposed backup Solution supports the capability to write multiple data streams to a single tape device or multiple tape devices in parallel from multiple clients to leverage the throughput of the Drives using Multiplexing technology.
- The proposed backup solution support de-multiplexing of data cartridge to another set of cartridge for selective set of data for faster restores operation to client/ servers
- The proposed backup solution should be capable of taking back up of SAN environment as well as LAN based backup.
- The proposed backup solution shall be offered with 4 Nos. UNIX based licenses, 26 Nos. Windows based licenses and the rest 20 Nos. LINUX based licenses for both SAN based backup and the LAN based backup.
- The proposed solution also supports advanced Disk staging.
- The proposed Backup Solution has in-built media management and supports cross platform Device & Media sharing in SAN environment. It provides a centralized scratched pool thus ensuring backups never fail for media.
- Backup Software is able to rebuild the Backup Database/ Catalog from tapes in the event of catalog loss/ corruption.
- The proposed Backup Software should offer online backup for all the Operating Systems i.e. UNIX, Windows & Linux etc
- The proposed Backup Solution has online backup solution for different type of Databases such as Oracle, MS SQL, and Sybase/ DB2 etc. on various OS.
- The Proposed backup solution shall provide granularity of single file restore.
- The Proposed backup solution shall be designed in such a fashion so that every client/ server in a SAN can share the robotic tape library.
- Backup Solution shall be able to copy data across firewall.
- The backup software must also be capable of reorganizing the data onto tapes within the library by migrating data from one set of tapes into another, so that the space available is utilized to the maximum. The software must be capable of setting this utilization threshold for tapes
- The backup software should be able to support versioning and should be applicable to individual backed up objects.
- Should have the ability to retroactively update changes to data management policies that will then be applied to the data that is already being backed up or archived.



FC – IP Router

- Fibre Channel Ports
 - Min 4 FC ports
- FC Port Speed
 - Autosensing 1/ 2/ 4 Gb/s
- iSCSI (Ethernet) Ports
 - Min 8 Ethernet ports
- iSCSI (Ethernet) Ports speed
 - 1 Gigabit Ethernet
- Aggregate Bandwidth
 - Min 125 MB/s
- Protocol Support
 - FC
 - iSCSI
- High Availability Features
 - Two way active/ clustering with failover and failback capabilities
 - Multiple iSCSI connections provide multi-pathing support from a single gateway to as many as 100 servers
- Management Features
 - CLI (by Telnet, SSH or console)
- iSCSI Gateway Manager
 - SNMP
 - Allow for monitoring traffic statics on each storage and network interface, fan and temperature and iSCSI session details.



6. Appliance based HSM for PKI Security and Encryption

S. No	Specification
1	Should support windows 2000/ 2003/ 2008, Linux, Solaris, HP-UX 11i, VMWARE, AIX 5.3
2	Should comply to standards like FIPS 140-2 Level-3, CC EAL4+, ROHS, FCC part 15 Class B
3	Key Exchange Mechanism: DES/ Triple DES, AES Algorithm
4	Hash/ HMAC algorithm: MD5, SHA 1, SHA 2, SHA 256
5	Symmetric Algorithm : AES, MD5, SHA 1, SHA 2, SHA-256 , DES, Triple DES
6	Support for various cryptographic algorithms: Asymmetric Key with Diffie-Hellman (1024-4096 bit), RSA (512-4096 bit) and (PKCS#1 v1.5, OAEP PKCS#1 v2.0), Digital Signing via RSA (1024-4096-bit), DSA (512-1024-bit), EC Brain pool Curves (named and user-defined), Suite B Algorithm Support and ARIA support.
7	Published API for various above functionalities for integrating with the Application software.
8	Signing speed: 5000 S/S
9	Remote PED Support for Authentication
10	Onboard key generation, Digital Signing & Verification process to be done inside the HSM only for better performance and security
11	HSM should be integrated with the applications running inside the Data Center
12	Complete hardware based storage of key material for entire Life cycle
13	24/ 7 telephonic/ email support infrastructure based out of India
14	TCP/ IP Network based appliance
15	Key Length Supported (1024 to 4096)
16	Public Key Algorithm RSA encrypt/ decrypt, RSA sign/ verify, ECC (Electric Curve cryptography)
17	Keys are always in Hardware and never stored in Software in any form
18	Compatibility: PKCS#11 , CAPI, Open SSL, JCE/ JCA
19	Scalable Up to more than 15 unique partitions
20	Private key generation and import: Archival and duplication mechanism to be specified. Give the procedure for key transportation from one HSM card to other HSM card.
21	Contents can be securely stored on Backup Tokens to simplify backup, cloning, and disaster recovery.
22	Onboard key generation, Digital Signing & Verification process to be done inside the HSM only for better performance and security.
23	Additional/ specific software's if any, required supporting multiple HSM appliances to be provided.



7. KVM Switch

Keyboard, Video Display Unit and Mouse Unit (KVM) and/ or other Control Devices/ PCs may be used for the IT Infrastructure Management for which the necessary consoles/ devices shall be placed by MPSEDC in the location earmarked. The KVM unit should provide the following functionalities:

- Rack-mountable.
- Minimum 8 ports scalable upto 24 ports.
- Should support local user port for rack access.
- Support for USB and PS/2 connections.
- Capability of storing username and profiles.
- Should support high resolution of minimum 1280 x 1024
- Capability to auto scan servers
- Should work on CAT 6/ CAT 7 cables.
- Rack Mountable LCD Monitor with In-built Keyboard & Mouse
 - 1 U Rack Mount.
 - Display size: 17 inches diagonal.
 - Contrast Ratio: 700:1
 - Display colors: 16 million.
 - Resolution: SXGA 1280 x 1024.
 - Brightness: 300 nit.
 - Compatible to both PS/2 and USB based inputs.



8. Networking Equipments (SDC/ DR/ all other Police Locations)

Router

a) General Architecture:

- High speed CPU
- Rack mountable configuration
- Health LED for all modules to indicate status

b) Router Port Requirements:

- 10/ 100 Mbps Ethernet - 2 Nos
- WAN Ports E1 - 2 Nos
- Packet Forwarding Speed - Minimum 160 Kpps

c) Router Features:

- Support for router redundancy protocol
- Router software must have on line reconfiguration facilities
- High MTBF
- Capable of booting from a remote system where router image is present
- Support for standard routing protocols like OSPF, RIP & BGP
- Should have adequate memory and flash for proper functioning of all features with no performance degradation.
- Minimum of 256 MB RAM
- Configurationally changes should be done without rebooting the router or modules
- Stateful firewall functionality.

d) Software features:

- **Following standard IP routing protocols:**

- Static
- RIP, OSPF
- OSPF Over Demand Circuits
- Policy Routing
- IP version 6 Support
- Support for IPSec& 3DES through a simple software upgrade as and when required.

- **Following WAN protocols:**

- PPP
- Multilink PPP
- Compression-Payload and TCP/IP Header

- **Following Multicasting and Quality of Service (QoS):**

- Resource Reservation Protocol (RSVP) as per RFP 2205 and Internet Group Management Protocol version 2 (IGMPv2) as per RFC 2236.
- Support for IP Precedence, Committed Access Rate (CAR),
- DiffServQoS



- The router shall support Application recognition and it should be possible to frame policies based on the applications or equivalent functionality.

e) Security Features:

- Support DES/ 3 DES/ AES
- PPP PAP or CHAP support.
- VPN support
- Time based Access Lists
- Multiple Privilege Levels.
- Support for RADIUS or AAA.

f) Power: 230 V AC, 50 Hz

Switches:

a) 16 Port Switch:

- 16 x 10/ 100BASE-TX, auto-negotiation ports
- Interface: RJ-45 10BASE-T, 100BASE-TX
- LED indicators: Power, Link/ Act
- Transfer Method: Store and Forward
- MAC Address Learning: Automatically learning, automatically Update
- Power Supply: 100 – 240 VAC, 50/60Hz
- 16-Port 10/100 Switch
- Safety & Emission: FCC, CE
- Rack mount Kit
- IEEE 802.3 10Base-T Ethernet, IEEE 802.3u 100Base-TX Fast Ethernet, IEEE 802.3 Nway Auto-negotiation, IEEE 802.3x Flow Control, IEEE 802.1p Qos Prioritization

b) 48 port Layer 3 Switch:

- Layer 3 stackable switch
- 48 x 10/ 100/ 1000 ports, auto-negotiating
- 4 No SFP-based Gigabit Ethernet ports
- Non-blocking architecture
- 32 Gbps switching fabric capacity and 38 mpps forwarding rate
- Support IGMP Snooping with Broadcast Control IGMP v3.
- Support for minimum 8000 MAC addresses.
- Ethernet, Fast Ethernet support
- Spanning tree/ Rapid Spanning Tree support
- Per VLAN Spanning Tree
- Support for dynamic VLAN Registration
- Dynamic Trunking Protocol or equivalent.
- VLAN Trunking Protocol or equivalent
- Traffic classification should be based on user-definable application types: TOS, DSCP, Port based, Mac address, IP address, TCP/ UDP port number
- Multicast filtering per port should be supported
- Support SNMP upto version 3
- Prioritization support



- Minimum 250 VLAN
- SNMP and Telnet support
- Web-based and CLI management
- Four RMON groups (1,2,3&9)
- Additional features: Advanced QoS, Rate limiting
- L3 Features : Static routes & RIP
- Mounting: 19" Rack mountable
- Source power supply: 230V AC Single phase 50Hz

Perimeter Firewall

- a) Physical Attributes
 - Rack Mountable
 - Modular Chassis
 - Redundant Power Supply
- b) Interfaces
 - 4xGE Upgradable to 8
 - 1xConsole Port
- c) Performance
 - Firewall Throughput: Min 2 Gbps
 - Concurrent Connections: Min 500K
 - Simultaneous VPN tunnels: Min 2K
- d) Routing Protocols
 - Static Routes
 - RIP v1, RIP v2
 - OSPF v2 & v3
- e) Protocols
 - TCP/IP, PPTP
 - RTP, L2TP
 - IPSec / GRE, DES/ 3DES/ AES
 - PPPoE, EAP-TLS, RTP
 - FTP, HTTP, HTTPS
 - SNMP, SMTP
 - DHCP, DNS
 - Support of IPv6
- f) Other Support
- g) 802.1Q, NAT, PAT, IP Multicast Support, Remote Access VPN, Time based ACLs, URL filtering, Support VLAN, Layer 2 Firewall, Virtual Firewall, RADIUS/ TACACS
- h) Management
- i) Console, Telnet, SSHv2, Browser based configuration
- j) SNMP v1, SNMP v2



9. Minimum Technical Specifications Requirement at Police Units:

Minimum Technical specifications for Desktops at Police Stations		
Desktop Configuration		
1	Processor:	Intel Core i5 or higher
2	Motherboard:	OEM Motherboard
3	Memory Type:	4 GB DDR3 expandable to 8 GB
4	Cache:	6 MB
5	Internal Hard Disk:	320 GB SATA (7200 RPM) or higher
6	Optical Drive:	DVD ROM Drive
7	Display size:	18.5 inch (measured diagonally)
8	Graphics Controller:	Integrated graphic Controller
9	Form Factor:	Convertible Minitower
10	External I/O ports:	2.0, headphone and microphone; Expansion slots: 1 full-height PCI, 2 full-height PCI Express x1, 1 full-height PCI Express x16
11	Rear:	6 USB 2.0, 1 serial port (optional), 1 parallel port (optional), 1 PS/2 (Keyboard), 1 PS/2 (Mouse), 1 RJ-45, 1 VGA, audio in/out.
12	Front:	2 USB
13	Network interface:	Integrated 10/100 Mbps Ethernet Adapter (RJ-45),
14	Management:	Desktop Management Tool
15	Bilingual Keyboard:	PS/2 or USB Standard Keyboard
16	Pointing device:	USB 2-Button Optical Scroll Mouse
17	Security management: (Optional)	TPM 1.2 TPM Security Chip (except for Russia), TPM Pre-Boot
18	Authentication: (Optional)	Smartcard Pre-boot Authentication (via BIOS), Stringent
19	Operating System	Preloaded Windows 7 Business Edition
20	Software Security	Security Software, Serial, Parallel, USB Enable/Disable (via BIOS), Write/Boot Control, Power-On and Setup Password (via BIOS)
21	Warranty:	3 Years Part, 3 Years Labor, 3 Years On-Site
Minimum Technical Specifications for Multi-Function Laser Printer		
Multi-Function Laser (Print/ Scan/ Copy)		
1	Printer	High-speed printing, Black-and-white: up to 35ppm (draft); up to 15ppm, Duty Cycle: Upto 15,000 pages per month. Automatic two-sided printing, 250-sheet input tray, Print, scan and copy unattended with the Automatic Document feeder, monitoring and troubleshooting in the network, from anywhere on the network
2	Scanner	Flatbed with automatic document feed, upto 4800 dpi; Enhanced upto 19200 dpi; Scan size max (flatbed): 215.9 x 297 mm (8.5" x11.7"), front panel scan
3	Copier	Black-white colour-Upto 1200x600 dpi, Copy speed (black, draft quality, A4):Up to 35 cpm, Copy resolution (black graphics): Up to 1200 x 600 dpi, Copier resize: 25 to 400%, Maximum number of copies: Up to 99, Copier smart software features: Up to 99 multiple copies, reduce/enlarge from 25 to 400%, 2-up or 4-up allowing 2 or 4 pages to be copied onto 1 page, contrast (lighter/darker), resolution (copy quality), tray select, collate, margin, shift.



Minimum Technical Specifications for Duplex Laser Printer

Duplex Laser Printer – all Police Units/ Offices

1	Laser Printer	<p>Speed:</p> <ul style="list-style-type: none"> • 28 PPM (A4) or higher <p>Processor:</p> <ul style="list-style-type: none"> • 400 Mhz or higher <p>Resolution:</p> <ul style="list-style-type: none"> • Min. 1200 x 1200 dpi <p>Duty Cycle:</p> <ul style="list-style-type: none"> • Min. 50,000 page/month <p>Memory:</p> <ul style="list-style-type: none"> • 64 MB or higher <p>Interface:</p> <ul style="list-style-type: none"> • USB 2.0 (High Speed) with USB Cable <p>Duplex:</p> <ul style="list-style-type: none"> • Automatic <p>Paper support:</p> <ul style="list-style-type: none"> • A4, Legal <p>Compatibility:</p> <ul style="list-style-type: none"> • Windows XP/Windows Vista/Windows 7/ Linux
---	----------------------	--

Minimum Technical Specifications for UPS

SNMP Based 3kVA UPS - all Police Units/ Offices

1	SNMP	<ul style="list-style-type: none"> • ISO 9001 certified brand • True On Line Type • Backup period should be at least 2 Hr with minimum 7200VAH for 3 kVA • IGBT with High Frequency PWM (Pulse with Modulation) Technology • Output wave form should be Sine wave • Compatible with local Electricity Power Generator. • Total Harmonic Distortion should be less than 3%. • Support input voltage range of 160 V to 270 V. • Output Voltage should be 230 Volt AC (+/- 1%) • Output frequency should be 50 Hz +/- 0.05 Hz (Crystal Controlled) • Closed housing for batteries with suitable stand. • Inherent protection should be provided for over loading, low battery, over temperature, short circuits, over and under input voltage. • LED indicators should be provided for at least load indication, load on battery, low battery, overload, Mains ON. • Audible indicator should be provided for at least load on battery, low battery, Mains failure, Overload. • Galvanic Isolation to be provided through inbuilt double wound transformer at output.
---	-------------	---



Minimum Technical Specifications for DG Set

2.5 KV DG Set - all Police Units/ Offices

1		<p>The proposed DG set should be able to support the Police Unit equipments, in absence of primary power source. Engine shall be vertical multi cylinder 4 stroke type in accordance with IS 10002-1981 with latest amendments.</p> <p>Type: Multi cylinder Method of starting: Electric start 12 V DC Type of cooling: Water cooled / Air cooled Type of governor: Mechanical/ Electronic Type of fuel: High speed diesel Rating: Continuous Output: Suitable HP rated to match the alternator Rated speed: 1500/ 3000 RPM Over load capacity: 10% overload – minimum 1 hour 50% overload – minimum 1 minute</p> <ul style="list-style-type: none"> • Flywheel to suitable diameter and fuel injection equipment • Air cleaner • Lubricating oil cooler • Electric motor starting equipment like motor, battery, charging generator with voltage regulator etc. • Heavy duty radiator with fan • Residential type silencer with exhaust piping with vibration isolator • Fuel tank suitable for 8 Hrs of continuous running with necessary piping and fuel gauge, drain valve, inlet and outlet connections. • Anti vibration mounting pads (Dunlop) • Speed controlling governor • Suitable coupling system to the Alternator • Tachometer • Lubricating oil pressure gauge • Hour meter to indicate number of Hrs of operation • Auto trip on low oil pressure • Over speed alarm with trip • Thermal insulation for exhaust line with glass wool, Aluminum sheet, chicken mesh, Diesel line 12 mm dia including beads flanger etc • Battery 12 V with lead and terminal • Battery charger. • Protection: Protection against low lubricating oil pressure, high water temperature and over speed shall be provided for engine with alarm and fuel shut off.
---	--	--



Minimum Technical Specifications for Finger Print Reader

Finger Print Reader - all Police Stations

1	<p>Fingerprint Sensor:</p> <ul style="list-style-type: none"> • Scanner: Optical sensor • Resolution: 500 dpi at 256-bit (416 X 416 pixels) • Platen Area: 0.83 in x 0.83 in (45.7 mm x 45.7 mm) PIV System included • Distortion: <1% <p>Biometric Matching:</p> <ul style="list-style-type: none"> • Authentication: <1 second (including detection, encoding and matching) • Identification: <2 seconds in 1:3000 mode (including detection, encoding and matching) • False Acceptance Ratio (FAR): 1 in 10,000 or better, configurable • based on security specifications <p>Interfaces:</p> <ul style="list-style-type: none"> • Standard USB <p>Environment:</p> <ul style="list-style-type: none"> • Temperature: 0° C to 50° C • ESD Protection: 15 KV <p>Format Supported:</p> <ul style="list-style-type: none"> • AANSI/ INCITS 378, • ISO 19794-2
---	--

Minimum Technical Specifications for Digital Pen

Digital Pen- all Police Stations

1	<p>Average battery life:</p> <ul style="list-style-type: none"> • Min. 2.5 hours continuous writing use <p>Average usage life:</p> <ul style="list-style-type: none"> • 3 – 4 years <p>Approximate battery recharge time:</p> <ul style="list-style-type: none"> • 2 hours <p>Battery type:</p> <ul style="list-style-type: none"> • Lithium-ion polymer rechargeable battery: <p>Standard Connectivity:</p> <ul style="list-style-type: none"> • USB 1.1 (also called High Speed USB 2.0) <p>Humidity non operating:</p> <ul style="list-style-type: none"> • 0 to 95% RH (excluding rain, non-operating) <p>Humidity range:</p> <ul style="list-style-type: none"> • 0 to 95% RH (excluding rain) <p>Operating range:</p> <ul style="list-style-type: none"> • 0 to 90% RH (non-condensing, operating) <p>Operating temperature maximum:</p> <ul style="list-style-type: none"> • 104°F <p>Operating temperature recommended range:</p> <ul style="list-style-type: none"> • 32 to 104°F <p>Storage temperature range:</p> <ul style="list-style-type: none"> • -4 to 104°F <p>Storage life:</p> <ul style="list-style-type: none"> • 3 – 4 years
---	---



		<p>Image compression:</p> <ul style="list-style-type: none"> • Pattern images to X, Y coordinate samples with relative time of capture <p>Image processing rate:</p> <ul style="list-style-type: none"> • 75 Hz <p>Image resolution:</p> <ul style="list-style-type: none"> • At least 500 dpi <p>Image scaling:</p> <ul style="list-style-type: none"> • Perspective, rotation, tilt, and error correction <p>Internal fixed memory:</p> <ul style="list-style-type: none"> • At least 10 MB (1.3 MB available for user strokes)
--	--	---

--	--	--

Minimum Technical Specifications for Digital Camera

--	--	--

Digital Camera - all Police Stations

1		<ul style="list-style-type: none"> • At least 14 Mega Pixels • Sensor size: 1/2.3-inch • Sensor type: CCD • Optical Zoom: 4x • Precision Digital Zoom: Yes, needed • Lens: Carl Zeiss or equivalent • Min aperture wide f3.1 - 3.5 • Min aperture tele f5.8 - 8.0 • Auto Focus Range (W: Approx. 4cm to Infinity, T: Approx. 60cm to Infinity) • Compatible Recording Media Memory Stick Duo/ Memory Stick PRO Duo/ Memory Stick PRO Duo (High Speed)/ Memory Stick PRO-HG Duo/ SD Memory Card/ SDHC Memory Card • LCD: 2.7 (6.9 cm) (230K pixels), Clear Photo LCD • Battery Life: 240 shots or 120mins • Battery System: Lithium ION Battery • USB 2.0 Hi-Speed
---	--	---



C. ANNEXURE XIII – INDICATIVE HARDWARE BILL OF MATERIAL

Hardware Distribution at Non-CIPA, CIPA and all other Higher Office's:

Description	Indicative Quantity at Non-CIPA P/S (167)	Indicative Quantity at CIPA P/S (23)	Indicative Quantity at SDPO (72)	Indicative Quantity at DPO (25)	Indicative Quantity at ASP Office (19)	Indicative Quantity at Range Office (7)	Indicative Quantity at Zone Office (2)	Indicative Quantity at PHQ (2)	Indicative Quantity at SCRB (1)	Indicative Quantity at Jails (15)	Indicative Quantity at Forensic Labs (2)	Indicative Quantity at Fingerprint Bureau (1)	Indicative Quantity at PCR (27)	TOTAL	Make	Model
Desktops																
Desktop with pre-loaded OS	668	-	216	250	57	28	8	60	10	15	2	1	81	1396		
Other Hardware																
Printer (Duplex Laser)	167	-	-	-	-	-	-	-	-	-	-	-	-	167		
Multi Function Printer (Print/ Scan/ Copy)	167	-	72	25	19	7	2	2	1	-	-	-	-	295		
UPS (3kVA)	167	-	72	75	19	7	2	16	3	-	-	-	-	361		
DG Set (2.5KV)	167	23	-	-	-	-	-	-	-	-	-	-	-	190		
16 Port Switch	167	23	72	25	19	7	2	2	1	-	-	-	-	318		
HDD 160 GB (External)	167	23	-	-	-	-	-	-	-	-	-	-	-	190		
Digital Camera	167	23	-	-	-	-	-	-	-	-	-	-	-	190		
Electronic Pen	167	23	-	-	-	-	-	-	-	-	-	-	-	190		



Fingerprint Reader	167	23	-	-	-	-	-	-	-	-	-	-	-	190		
Site Preparation ¹	167	23	72	25	19	7	2	2	1	-	-	-	-	318		
Other Software																
Operating System (Win 7 Professional)	668	92	216	250	57	28	8	60	10	15	2	1	81	1488		
Microsoft Office Suit	668	92	216	250	57	28	8	60	10	15	2	1	81	1488		
Antivirus Software*	668	92	216	250	57	28	8	60	10	15	2	1	81	1488		
Operational Expenses for 3 Years	167	23	72	25	19	7	2	2	1	-	-	-	-	318		

Site Preparation¹: Include Adequate Furniture, Electrical Cabling, Earthing & Earth Pit, Wall Mountable Network Rack - 9 U, Patch Panel 12 Ports CAT 6, Cat 6 Cable with Cabling (In Meters), Information Outlet CAT 6 and Patch Cords 2 Mtr. CAT 6

Operational & Maintenance for 5 years

* Antivirus Software: Symantec / Trend Micro / McAfee enterprise solution can be quoted



Hardware Distribution at Data Centre and Disaster Recovery Site:

The details pertaining to the proposed DC and DR the Police Department

Items	Qty	Make	Model
Network Server Racks 42 U	2		
Application Server (Rack Server)	2		
Test & Development Server (Rack Server)	1		
Database Server (Rack Server)	2		
Web Server (Blade Server)	2		
Portal Server (Blade Server)	2		
Backup Server (Blade Server)	1		
Directory & Access Server	2		
Communication & Mail Server	2		
Blade Chassis	2		
Storage Box (SAN)	2		
Storage Area Switch	2		
SAN Storage Management Software	1		
Automated Tape Library	2		
DR Recovery Storage	1		
Back-up Software	1		
HSM for PKI Security and Encryption (2No at DC and 1 at DR)	3		



Router	2		
FC – IP Router	2		
Load Balancer	2		
Link load Balancer	2		
Core Switch L3 Gigabit 48 Port	2		
KVM Switch	2		
Patch Panel 24 Ports CAT 6	2		
CAT 6 Cable (305 Mtr. Box)	3		
Information Outlet CAT 6	36		
Patch Cord 2 Mtr CAT 6	36		
UTM Firewall with VPN and IPS	2		
Data Center Software (Server OS with CAL, Server Management, Intranet Portal, MIS & Reporting Dashboard etc.)	18		
Database Software (Processor Based for unlimited users)	6		
Antivirus Software for Servers	18		
Email Security Software Required features; Anti-spam Anti-virus Anti-spoofing Anti-phishing Anti-spyware (Attachments) Denial of Service Data Leak Prevention	2		
Enterprise Management System (EMS)	1		
Outsourced manpower for datacenter 2 nos. × 3 shifts for 5 Years	-		



AMC for five (5) years	-		
------------------------	---	--	--

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

DR hardware and software should operate 50% replica of DC except storage



Handholding Support:

S. No.	Items	No. of Police Station	For the period of 6 Months
1.	Handholding Support	190	

Data Digitization:

S. No.	Items	No. Of Case Files to be Digitized (For last 10 Years)
1.	Digitization	102857

Capacity Building:

Expenditure Head	No. Of Units
SCRB _x Infrastructure	1
District Training Centre ,Site preparation	25
District Training Centre	25
RTC/ PTC/ Academy	6
Training for Police Personal	42441



4. RFP Volume 2

A. **3. BIDDING PROCESS DETAILS – General Instruction to Bidders**

Stand amended as:

3.2.9 Earnest Money Deposit

- 1) Bidders shall submit, along with their Bids, EMD of ₹2 Crore only, in the form of a Demand Draft issued by the scheduled bank pledged in favor of 'Managing Director of PHC (SDA)' payable at Jammu for J&K State at Jammu and Kashmir Bank and will remain current till completion of the Project. Bid security in any other form will not be accepted.
- 2) The bid security of all unsuccessful bidders would be refunded/ released by JK Police through the Nodal Officer CCTNS Project within three months of the bidder being notified by JK Police as being unsuccessful.
- 3) JK Police will not be responsible to pay any interest to either the successful or unsuccessful bidders on their EMD, in whatever form they have submitted it.
- 4) The bid submitted without bid security, mentioned above, will be liable for rejection without providing any further opportunity to the bidder concerned.
- 5) The bid security may be forfeited.
 - a) If a bidder withdraws its bid during the period of bid validity.
 - b) In case of a successful bidder, if the bidder fails to sign the contract in accordance with terms and conditions.

**B. 3. BIDDING PROCESS DETAILS – Bid Opening and Evaluation Process**

Stand amended as:

3.4.4 Pre-Qualification Criteria

- 1. Point 6(d),** The Bidder must have a proven track record of providing a successful ‘Turnkey Solution’ for at least five (5) IT-projects in last 5 years as date of submission of bid. At least one of the 5 quoted projects should be an integrated turnkey project of a value of not less than Rs. 10 Crore or above in India including setting up and configuring the hardware (Servers, Desktop, Network Clients) and implementing software solution including Operating Systems, Infrastructure Management Software, RDBMS, establishment of LAN/ WAN including Firewalls, IPS, PKI, etc. and providing life cycle support. Bidder must provide as a supporting documentary proof in form of work orders confirming year and area of activity, value of services to be delivered for each of the five projects, completion/ partial completion Certificate from client confirming year and value of Bidder’s scope of work, scope of work completed by the Bidder and its value along with reference details of the client.
- 2. Point 6(e),** The Bidder must have a proven track record of implementing at least two (2) e-Governance projects to summing up to a value of Rs. 10 Crore or above. Bidder must provide as a supporting documentary proof in form of work orders confirming year and area of activity, value of services to be delivered for each of the two projects, completion/ partial completion Certificate from client confirming year and value of Bidder’s scope of work, scope of work completed by the Bidder and its value along with reference details of the Client.
- 3. Point 6(h),** The bidder must have been assessed and must possess a valid ISO 9001:2008 or above certificate as on the date of contract signing and the certificate should be valid for at least a period of one year from the date of submission of the bid.



Note: Following points are added to this corrigendum:

- 1) All the Licenses shall have to be procured by the selected SI for the successful implementation of the project. The system software licenses mentioned in the bill of materials shall be genuine, perpetual, full use and should provide patches, fixes, security patches and updates directly from the OEM. All license and support (updates, patches, and bug fixes) should be in the name of JK Police.
- 2) The SI shall provide with a full use database license. All the licenses and support (updates, patches, and bug fixes) should be in the name of JK Police.
- 3) The software proposed should be from an OEM with presence in India (and easy availability of skilled resources for the product in India).
- 4) SI shall provide a comprehensive warranty that covers all components after the issuance of the final acceptance by JK Police department. The warranty should cover all materials, licenses, services and support for both hardware and software. SI shall administer warranties with serial number and warranty period. SI shall transfer all the warranties to the department at no additional charge at the time of termination of the project. All warranty documentation (no expiry) will be delivered to the department.
- 5) The OEM must authorize the selected SI for products listed below,
 - a) Operating System Name and Version.
 - b) RDBMS Name and Version.
 - c) Directory Server Name and Version.
 - d) Office productivity suit Name and Version.
 - e) Reporting Server Name and Version.
 - f) Application Server Name and Version.
 - g) Web Server Name and Version.
 - h) Enterprise Management Server Name and Version.
 - i) Antivirus Server Name and Version.