CRIME & CRIMINAL TRACKING NETWORK AND SYSTEM (CCTNS)

CORRIGENDUM No. 02, DATED 21-MAY-2011

To

REQUEST FOR PROPOSAL

FOR

SELECTION OF SI FOR

IMPLEMENTATION OF CCTNS

IN ODISHA

DEPARTMENT OF HOME, GOVERNMENT OF ODISHA

TABLE OF CONTENTS

LIST OF TABLES

1. Request for Proposal Volume I

1.1 Section 5: Scope of Services During Implementation Phase

1. Clause 5.5: Site preparation at Police Stations and Higher Offices

Table 14 as mentioned in Clause 5.5 *stands amended as*

Table 1 Client Site-Bill of Material

Sr. No.	Items	Quantity (Indicative only)
1.	Client Systems	3216
2.	Operating System-Pre Loaded Windows 7 Professional	3216
3.	Licenses for MS Office	869
4.	Open Offices (All Desktops excluding ones with MS Offices)	2347
5.	HDD 160 GB	579
6.	Duplex Laser Printer	579
7.	Multi-Function Laser	1177
8.	UPS for 120min backup	742
9.	2KVA Generator	579
10.	16-Port Switch	742
11.	Fingerprint Reader	579
12.	Digital Camera	579
13.	Electronic Pen	579

1.2 Section 6: Scope of Services During Post-Implementation (Operation & Management) Phase

Bidder is expected to assume the below details for estimating costs for consumables:

1. Fuel for Generators:
    a) 125 Police Stations have no power or have difficulty in terms of availability of power.
    b) For Police Stations in Bhubaneshwar/Cuttack an average of 3 hours power-cut per day can be considered.
    c) For Higher Offices an average of 3 hours per day power-cut can be assumed.
    d) The actual approval for this will be done by NCRB.

2. Toner:
    a) 1 Toner for Multi-Function printer for every 2 months for each of the PS and higher offices
    b) 1 Toner for Laser Jet Network Printer for every 2 months for each of the PS and higher offices

3. Paper:
    a) Higher offices – 3 reams of paper/Month

PS – 2 reams of paper/Month

PS in remote locations (125 as mentioned above) – 1 reams of paper/Month

Please note that above indicative number is for bidding purpose only; actual consumption may vary from the above. Bidder is advised to quote the unit price for each of the above items. The actual payment to SI for the consumables would be based on the actual consumption and the unit price quoted

1.3 Section 7: Implementation And Roll-Out Plan

INDICATIVE PLAN *stands amended as*

The Geographic 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. To cover all District SP Offices.
    iii. To cover all State Level Higher Offices.
    iv. 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 and Higher Offices, 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.

c. Phase 3 – 30% of the Police Stations and remaining higher offices.

   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.

d. Phase 4 – 30% of the Police Stations and remaining higher offices.

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.

e. Phase 5 – 30% of the Police Stations and remaining higher offices.
   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

Geographic Implementation Plan
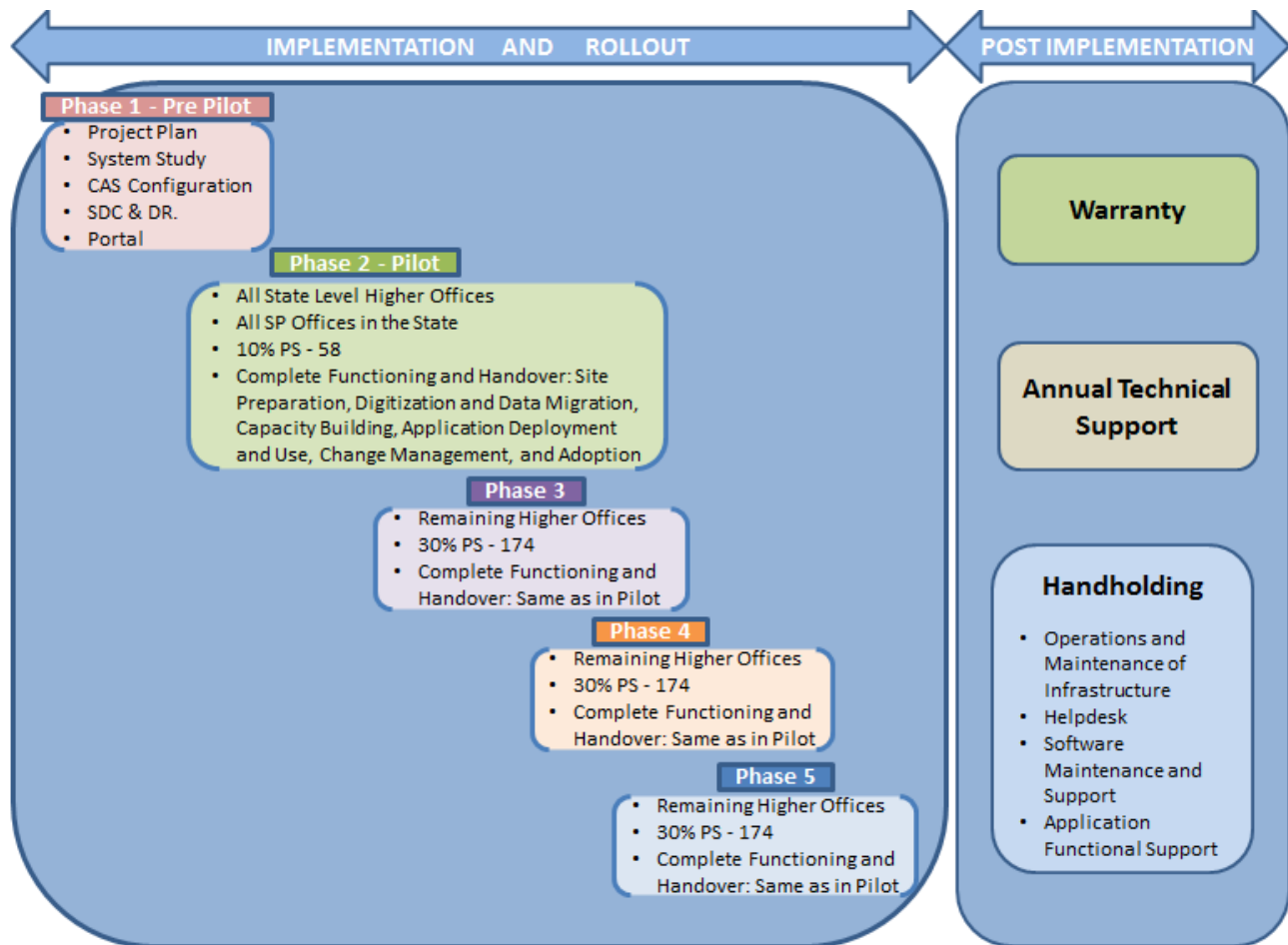
SI to carry out rectification of the defects pointed out and / or enhancements suggested by the SPMU during the O&M period.

Indicative Activity Based Timelines for Deliverables

Indicative Activity Based Timelines mentioned in Table 22 _stands amended as_

Table 2 Timelines of Deliverables

1.	**Preparation of detailed Project plan**	T1
1.1.	Work Plan	T1+2 Weeks
1.2.	Resource Plan	T1+4 Weeks
1.3.	Risk Plan	T1+5 Week
2.	**Capacity Building in State**	**T2**
2.1.	Preparation of the Training and knowledge transfer Plan	T2+3 Weeks
2.2.	Preparation of training material	T2+9 Weeks
2.3.	Conducting training for Police personnel	T2+62 Weeks
3.	**Phase One: Implementation in Pilot District**	**T3**
3.1.	Customisation of CAS(State)	
3.1.1.	Refinement of Functional Requirements Specifications (FRS)	T3+2 Weeks
3.1.2.	Preparation of Software Requirement Specification of customisation of CAS(State)(SRS)	T3+3.5 Weeks
3.1.3.	Design Document for Customisation of CAS(State) (HLD, LLD)	T3+6.5 Weeks
3.1.4.	Parametric Customisation of Odisha CAS	
3.1.5.	Preparation of Test plan	T3+7.5 Week
3.1.6.	Preparation of Test cases	T3+9.5 Weeks
3.1.7.	Preparation of Test report	T3+10.5 Week
3.1.8.	Integration testing of CAS(State)	T3+13.5 Weeks
3.1.9.	User Acceptance testing	T3+14.5 Week
3.1.10.	Acceptance testing, Audit and certification	T3+16.5 Weeks
3.1.11.	Release of CAS(State)	T3+17 Weeks
3.2.	Setting of Data Centre	T4
_3.2.1._	Site preparation for setting up of Data Centre	T4+2 Weeks
_3.2.2._	Setting up of Hardware & Networking infrastructure for data Centre	T4+6 Weeks
_3.2.3._	Installation of Database server, Application server etc	T4+8 Weeks
_3.2.4._	Testing of functioning of DC	T4+10 Weeks
3.3.	Setting up of Disaster Recovery	T5
_3.3.1._	Setting up of Hardware & Networking infrastructure for DR	T5+2 Weeks
_3.3.2._	Installation of Database server, Application server etc	T5+5 Weeks
_3.3.3._	Testing of functioning of DR	T5+7 Weeks
3.4.	Supply & Commissioning of Hardware at Pilot District	T6
_3.4.1._	Preparation of Distribution list for Hardware to the PS	T6+1.5 Weeks
_3.4.2._	Identification of Site Preparation need at remote & dilapidated PS	T6+2.5 Week
_3.4.3._	Site Preparation at PS	T6+6.5 Weeks
_3.4.4._	Setting up of LAN and connectivity at PS	T6+8 Weeks
_3.4.5._	Distribution of hardware to PS	T6+10 Weeks
_3.4.6._	Testing of functioning of PC & its connectivity	T6+10.5 Weeks
3.5.	Rollout of CAS(State) in district (Roll out plan)	T6+ 20 Weeks
3.6.	Testing of connectivity & resolution of performance issues	3 Weeks
3.7.	Data Digitization at Pilot Districts	2 Weeks

7

4.	**Phase Two: Implementation across the state**	T7
4.1.	Supply & Commissioning of Hardware at Police Station	T7+20 Weeks
4.1.1.	Preparation of Distribution list for Hardware to the PS	T7+21.5 Weeks
4.1.2.	Distribution of hardware to PS	T7+30.5 Weeks
4.1.3.	Site Preparation at PS	T7+34.5 Weeks
4.1.4.	Setting up of LAN and connectivity at PS	T7+37.5 Weeks
4.1.5.	Testing of functioning of PC & its connectivity	T7+40.5 Weeks
4.2.	Rollout of CAS(State) in district	1.5 Weeks
4.3.	Testing of connectivity & resolution of performance issues	1 Week
4.4.	Data Digitization at Pilot Districts	9 Weeks
4.5.	Maintenance of hardware	From Procurement to End of AMC/Contract (Whichever is later)

1.4 Annexure 3: Service Levels

1. 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.

Stands amended as

RPO should be less than sixty minutes

Severity of Violation: High. Each instance of non-meeting this service level will be treated as two (2) violations.

2. *Addition of following point:*

Delays that are solely and exclusively attributable to BSNL will be considered and appropriate relaxation, if any, will be made in evaluation of SI's SLAs. Further changes, if any, may be made to this clause in light of the agreement between MHA and BSNL.

1.5 Annexure 7: Client Side Computing Infrastructure

Technical Specification of Client Site Infrastructure *stands amended as*

1.   Desktop

Table 3 Specification-Desktop

Sr. No.	Make & Model - (To be filled by the Supplier)	Complied / Not Complied
1.	Processor: Intel Core i5-650 processor (3.2 GHz) with Q57 Chipset or higher Core i5-650 Processor / AMD Phenom X4 955 , Clock Speed 3.2 GHz or higher	

Sr. No.	Make & Model – (To be filled by the Supplier)	Complied / Not Complied
2.	Memory Type: 2 GB DDR-III @ 1066 MHZ or higher	
3.	Memory Slot: 4 DIMM Slots	
4.	Internal Hard Disk/Speed: 250 GB SATA (7200 RPM) or higher	
5.	Optical Drive: SATA DVD Writer Drive	
6.	Display size: 18.5" TFT or more LCD Monitor 1280 x 1024 resolution with 5 ms or better response time, TCO 5.0 certified	
7.	Graphics Controller: Integrated HD graphics	
8.	Form Factor: Small Form Factor	
9.	External I/O ports: Rear: 6 USB 2.0, 1 standard serial port, 1 optional serial port, 1 optional parallel port, 2 PS/2, 1 RJ-45, 1 VGA, 1 Display Port, audio in/out; Front: 2 USB 2.0, headphone and microphone	
10.	Expansion slots: 2 full-height PCI, 1 full-height PCI Express x1, 1 full-height PCI Express x16	
11.	Network interface: Integrated Gigabit Network Connection (Intel 82567LM or equivalent or higher)	
12.	Power requirements: Indian Standard with energy star certified	
13.	Management: Desktop Management Tool	
14.	Bilingual Keyboard: PS/2 or USB Standard Keyboard (Same make as of pc)	
15.	Pointing device: USB 2-Button Optical Scroll Mouse (Same make as of pc)	
16.	System with Power management features & Desktop Management Interface implementation	
17.	Write/Boot Control, Power-On Password (via BIOS), Setup Password (via BIOS)	
18.	OS Support: Windows 7 / Linux /Centos 5.5/Ubuntu (Latest Version) Drivers should be freely available on OEM's web site	
19.	Certification: FCC, UL, Energy Star	
20.	**Preloaded Software:** Above configuration preloaded with Windows OS (Latest Version), Office Suite with Odiya Unicode fonts, Antivirus with all necessary Plugins/ utilities and driver software including bundled in DVD Media. For the four desktops in each Police Station, One should have MS Office and other three should have open office.	

2.   Multi-Function Printer (MFP: Print, Scan, Copy)

<div align="right">Table 4 Specification-MFP</div>

Sr. No.	Parameters	Specifications	Complied / Not Complied
1.	Print speed, black	Minimum 20 ppm	

Sr. No.	Parameters	Specifications	Complied / Not Complied
2.	Print resolution, black	Minimum 600 x 600 dpi	
3.	Print technology	Laser	
4.	Monthly duty cycle	Minimum 8000 pages	
5.	Memory, standard	64 MB	
6.	Print languages, standard	Host-based printing, PCL 5e	
7.	Duplex printing (printing on both sides of paper)	Manual (driver support)	
8.	Media sizes, standard	Letter, legal, executive, postcards, envelopes (No. 10, Monarch)	
9.	Media sizes, custom	250-sheet input tray: 5.8 x 8.27 to 8.5 x 14 in; priority feed slot: 3 x 5 to 8.5 x 14 in	
10.	Media types	Paper (laser, plain, photo, rough, vellum), envelopes, labels, cardstock, transparencies, postcards	
11.	Scanner type	Flatbed, ADF	
12.	Scan resolution, optical	Minimum 1200 dpi	
13.	Scan size	8.5 x 11.7 in	
14.	Scan speed	Up to 6ppm	
15.	Supported file formats	PDF; TIF; BMP; GIF; JPG	
16.	Copy resolution	Minimum 600x 400 dpi	
17.	Maximum number of copies	Minimum 99 copies	
18.	Accessories included	USB cable , Driver CD ,Utility software , UTP patch cable & One printing cartridge	
19.	Connectivity	Hi-Speed USB 2.0 port; 10/100Base-T Ethernet network port	
20.	Network ready	Standard (built-in Ethernet)	
21.	Power consumption	<=450 watts	
22.	Power Consumption (Standby)	<=10 watts	
23.	Operating temperature range	50 to 90F	
24.	ENERGY STAR® Qualified	Yes	

3.   Laser Jet Network Printer (Duplex)

Table 5 Specification-Laser Jet Printer

Sr. No.	Parameters	Specifications	Complied / Not Complied
1.	Print speed, black	Minimum 26 ppm	
2.	Print resolution, black	Minimum 1200 x 1200 dpi	
3.	Print technology	Laser	
4.	Monthly duty cycle	Minimum 8000 pages	
5.	Memory, standard	32 MB	
6.	Print languages, standard	Host-based printing, PCL 5e	
7.	Duplex printing (printing on both sides of paper)	Automatic (standard)	
8.	Media sizes, standard	Letter, legal, executive, postcards, envelopes (No. 10, Monarch)	
9.	Media sizes, custom	250-sheet input tray: 5.8 x 8.27 to 8.5 x 14 in; priority feed slot: 3 x 5 to 8.5 x 14 in	
10.	Media types	Paper (laser, plain, photo, rough, vellum), envelopes, labels, cardstock, transparencies, postcards	
11.	Accessories included	USB cable , Driver CD ,Utility software ,Cat5/6 UTP patch cable & One printing cartridge	
12.	Network ready	Standard (built-in Ethernet)	
13.	Power consumption	<=450 watts	
14.	Power Consumption (Standby)	<=10 watts	
15.	Operating temperature range	63.5 to 77° F	
16.	ENERGY STAR® Qualified	Yes	

4.   On-Line UPS (2KVA) Single Phase Input & Single Phase Output

Table 6 Specifications-UPS (2KVA)

Sr. No.	Parameters	Specifications	Complied / Not Complied
1	Capacity	2KVA	
	Battery Backup	120minutes	
2	General		
	Inverter Technology	Pulse Width Modulation (PWM) using IGBTs, double conversion	
	Switching frequency	20 KHz or higher	
	Total Harmonic Distortion (THD) Voltage	< 2% for 100% linear load < 3% for 100% non-linear load	
	Noise level	Less than 55 dB at 1 Meter	

Sr. No.	Parameters	Specifications	Complied / Not Complied
	Operating Temperature	0°- 50° C	
	Output Wave Form	Pure sine wave	
	Cooling	Air Cooled	
	Quality	ISO 9001 & ISO 14001 Certified	
	Compatibility	UPS to be compatible with DG Set supply	
3	Input		
	Voltage Range	160 V AC to 280 V AC	
	Frequency range	50 ± 6% Hz	
	D/G set comp ability	Required	
	Input Power Factor	0.9 or better at full output load leading to Unity with power factor correction (PFC)	
4	Output		
	Voltage	230V AC +1 %, single phase	
	Regulation	Less than + 1% in the following conditions 1. No load to full load/Full load to no load 2. 0.8 lagging 3. During Entire Backup time. 4. Complete Input Voltage Range	
	Frequency	50 Hz + 0.5 %	
5	Efficiency		
	Overall	Efficiency 80 % or better on rated full load of 0.8 PF & 230V, 50Hz AC output	
	Inverter Efficiency	90% or better on rated full load of 0.8 PF & 230V, 50Hz AC output	
6	Overload Capacity	110% for 2 min. & 125% overload for 30sec.	
7	Load Power Factor	0.6 lag to Unity PF	
8	Protection	Required for: Short Circuits / Over Loading/ Over Temperature / Input low/ high voltage control/ DC low/high voltage trip	
9	Battery Make	Complying with JIS C 8702 test.	
	Battery recharge time (after complete discharge to 100% charge) & charge rating	Battery recharge time should not exceed 8 hours and charger should be capable to charge battery on C10 rating.	
11	Battery Capacity		
	Capacity of UPS	At least 120 minutes back up with minimum 4032 VAH	
	UPS & Battery Housing	Powder coated UPS & battery cabinet with caster wheel should be of minimum 1mm thick good quality material and should be free from sharp edge, scratches, nicks, & burs etc. Enclosure should conform to protection requirement of IPL21 to IS13947 (Part 1)/1993 (reaffirmed 2004).	

Sr. No.	Parameters	Specifications	Complied / Not Complied
12	L.C.D. meter	To measure and monitor input voltage, output voltage, output current, DC current, DC voltage, input / output frequency	
13	Indications	Mains on/ Load on Battery/ Inverter/ Battery level/ Load level/ Inverter over load	
14	Audible Alarm	Over Temperature / Main failure/ Battery low/ Inverter Overload	
15	Switches	Main ON/OFF MCB/ Battery ON/OFF MCB/ Inverter push button with reset.	
16	Output Connection	O/P Terminals of standard quality should be provided. 03 Nos. of 5/15A/230V female ISI/ IEC Mark socket and all 3 sockets should	
17	Isolation	Isolation transformer and Transient Voltage Surge Suppressor (TVSS). TVSS shall be as per following specifications: • The unit shall have a Maximum Continuous Operating Voltage (MCOV) rating of min 320Volts • It should have minimum two modes of protection (L-N and N-G) with 0.5 ns response time • TVSS should have LED indications for physical monitoring • Input Connection (Line) Socket & Output Connection (Load) Plug should be as per IEC C14 & IEC C13 guidelines respectively	

Note –More than two battery banks should not be used in parallel in the configuration.

4.   Generators 2KVA

Table 7 Specifications-Petrol/Diesel Generators

S. No.	Parameter	Required Specifications	Complied / Not Complied
The proposed DG set should be able to support the Police Unit equipment along with AC, in absence of primary power source. Engine shall be vertical Single/multi cylinder 4 stroke type in accordance with IS10002-1981 with latest amendments.			
1	CAPACITY	2 to 2.5 KVA	
2	ENGINE:		
	Type	Single/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:	Petrol	
	Rating:	Continuous	
	Rated Output/HP:	Minimum 5 HP at 3000 rpm	

	Alternator rated speed:	3000 RPM	
	Over load capacity	10% overload – minimum 1 hour	
	Makes of engine:	Honda/ Mahindra/ Kirloskar / Yamaha/ Briggs & Stratton / Greaves/ Eicher	
	Ignition Type	Magnetron Electric	
	General	Engine should be four stroke with Double ball bearing on PTO & Flywheel with Over Head Valves and should have Cast Iron Sleeve	
3	ACCESSORIES:		
		• 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 • 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, Aluminium 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 and over heat shall be provided for engine.	

5. 16 Port Managed Switch

Table 8 Specification-16 Port Managed Switch

Sr .No	Parameters	Specifications	Complied / Not Complied

14

Sr .No	Parameters	Specifications	Complied / Not Complied
1.	Network Ports	The switch should have minimum 16 x 100/1000 Mbps Ports	
		It should have more than two non-shared open SFP ports for Gigabit Fibre connection/UTP RJ-45 ports	
2.	Protocol	CSMA/CD	
3.	Standards Compliance	IEEE 802.3 10 Base-T Ethernet	
		IEEE 802.3u 100BASE-TX Fast Ethernet	
		IEEE/ANSI 802.3 Auto Negotiation	
		IEEE 802.3x Full duplex Flow Control	
4.	Data Transfer Rates	Ethernet 10 Mbps(Half-duplex, 20 Mbps Full duplex)	
		Fast Ethernet 100 Mbps(Half Duplex), 200 Mbps(Full-Duplex), Giga Ethernet 1000Mbps	
5.	Performance	802.1q VLAN, SNMP managed,	
		Static Route and advance Access control list.	
		RSTP/MSTP support	
		LLDP and UDLD and L4 prioritization	
6.	Specifications	Bandwidth: 32 Gbps or above	
		Mac Address Database 8k	
7.	Power Supply	100V-240VAC	
8.	General	Should support RMON (Remote monitoring) and RADIUS	
		Software updates: Free downloads from the Web	
		OEM Make - Top 5 in IDC /Gartner reports (quarter ending December '10 or March '11) in terms of market share of units sold	

6.   Finger Print Reader

Table 9 Specifications- Finger Print Reader

Sr. No.	Parameters	Specifications	Complied / Not Complied
1.	Sensor Type	Optoelectronic	
2.	Prism Architecture	Single Prism	
3.	Size of window	46mm x 46mm or above	
4.	Resolution	Minimum 500 PPI or above	
5.	Image grey scale	256 level Dynamic	
6.	Image Capture Ability	Minimum 10 frames / second	
7.	Distortion rate	0.1%	
8.	Computer interface	USB2.0, USB Powered	
9.	Operating temperature	0 – 55 Degree C	
10.	Environmental humidity	Up to 90%	
11.	Finger Print Image Quality	Forensic – Quality Flat Fingerprint Image	
12.	Light Rejection	Should have Ambient Light Rejection	

Sr. No.	Parameters	Specifications	Complied / Not Complied
13.	Operating system Support	Windows and Linux	
14.	Certifications	FBI PIV-071006, FIPS 201 PIV, ISO-IEC 19794-4:2005, EN 55022:2006, EN 55024:1998 + A1:2001+ A2: 2003	
15.	Standards	FBI Standard CJIS-RS-0010 (V7), IAFIS Image Quality Specifications (IQS) for Scanners, ANSI/NIST/ISO Biometric Standards	

7. Data Base Server And Other Servers (Application, Web, Mail Etc.)

OS support: Microsoft® Windows Server 2003 / 2008, Enterprise Edition / Red Hat® Enterprise Linux 5 & 4 AP / SUSE® Linux Enterprise Server 9 / Solaris for x86

Stands amended as

OS support: Support for Microsoft® Windows 2008 & latest version of Linux / Solaris

8. SAN Switch

Table 10 Specification-SAN Switch

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
The SAN switch should have adequate populated ports to cater for the redundancy in connectivity from any other equipment.	
Switch should have non-blocking architecture	
All the 24 ports should be concurrently active	
Throughput of each port in the SAN switch should be 4 Gbit/sec full duplex with no over-subscription.	
All the ports should operate at min 4Gbps in a non-blocking backplane	
Setting of the port speed to 4Gbps or 8Gbps from the lower speed should not impact the other ports in the same port blade.	
The Power Supplies and FANs of the SAN Switch should be Hot Swappable	
The Power Supplies, FANs & Ports(SFPs) of the SAN Switch should be Field Replaceable Units	
The SAN Switch should support Virtual Fabrics feature / Advanced Zoning feature	
The SAN Switch should enable partitioning of a physical SAN into logical fabrics	
The SAN Switch should enable isolation of logical fabrics by application	
The SAN Switch should provide advanced zoning capabilities	
The SAN Switch should allow health monitoring capabilities	
The SAN Switch should allow performance monitoring capabilities	
The SAN Switch should have support for web based management	
The SAN Switch should support CLI.	
The SAN Switch should have proactive fault detection to avoid any hot-spots in the fabric.	

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
The SAN Switch should have alerting capability to avoid any hot-spots in the fabric.	

9.   Server Load Balancer

Table 11 Specification- Server Load Balancer

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
Architecture	
Should have minimum 6 x 10/100/1000 BaseT Ports plus 2 x 1000Base-Lx Port.	
Should have dedicated 10/100/1000 BaseT port for out-of-band management.	
Should have minimum 8 GB RAM and upgrade-able	
Support minimum 2,000,000 Concurrent L4 TCP connections	
Should capable to handle 100,000 L4 connections per second	
Should provide minimum 2 Gbps Layer-7 throughput and can be scalable to 4-Gbps throughput.	
Should have non-blocking 24Gbps backplane	
Should provide minimum 5000 SSL TPS for SSL offloading scalable to 15,000 TPS for future requirement.	
Should provide minimum 1Gbps server-side hardware/software based http compression.	
Should provide minimum SSL throughput equal to the compression throughput i.e. 1Gbps	
Should provide minimum hardware based SSL offloading	
Should support Dynamic routing protocols like OSPF, RIP1, RIP2	
Load Balancing Features	
Support for 2000 servers	
Support for minimum 512 Virtual IP	
Should support load balancing algorithms: Least amount of Bytes,	
Least number of users/session, Cyclic, weighted Cyclic, SNMP Parameters; like Server CPU utilization, memory utilization and combination of both.	
In case of Server / Application failure device should detect it in not more than 30 seconds	
In case of Server failure traffic should be diverted to another Server automatically	
Should support content based Load balancing features: HTTP Header based redirection, URL-Based Redirection, Browser Type Based Redirection, Preferential Treatment (Cookie-Based)	
Should Support session persistency Based on: IP, DNS, Cookie-based, URL Parameters, SSL Session ID-based etc.	
Should support Client NAT & Server NAT	
Should support TCP optimization and TCP Multiplexing	
Should support HTTP 1.1 protocol based caching	
Should support hardware/software based web compression	
Server Management Feature	

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
Should support Graceful shutdown of Servers	
Should support Graceful Activation of Servers	
Should able to redirect traffic based on Source IP, Destination IP & TCP PORT	
Redundancy	
Should Support standard VRRP (RFC - 2338) or alternate industry standard protocols with equivalent functionality	
Should support transparent failover between 2 devices	
Support for Global Server Load Balancing Algorithms	
Should support DNS based redirection	
Should support HTTP redirection	
Should support RTSP Redirection	
Should support VIP advertisement via Dynamic Routing	
Health Monitoring	
Should provide individual health check for each Server & Application	
Should be able to do health check on protocols like HTTP, SMTP, POP etc	
Should able to check the health of Server OS, Application & contents as well	
Should provide AND & OR Grouping mechanism between health check for granular approach for detecting path failure in multi-tier application architecture like core banking solution	
Health Check configuration should be via simple GUI interface and easy to understand, it should not require any scripting or CLI configuration.	
Device Management & Reporting	
Should provide GUI interface for configuration & reporting	
Should provide HTTP / HTTPS interface management	
Should provide SSH / Telnet / CLI interface	
Should support SNMP V1, V2c, V3	
Should provide Detailed LIVE reporting for traffic on each farm	
Should provide detailed historic reporting for server traffic	

10.   Firewall + IPS

Table 12 Specifications-Fire Wall

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
Hardware Feature	
The Firewalls should be Hardware based, Reliable, purpose-built security appliance with at least 6 No.s of 10/100/1000 Base Tx interfaces & upgradeable to 8 Interfaces for future expansion with 2 USB ports & 1 console port	
Should be redundant supporting Active/Active or Active/Standby Firewall for High Availability & Scalability	
Firewall Throughput of minimum 8 Gbps	
IPSEC 3DES Throughput of Up to 3 Gbps	
Concurrent Sessions of at least 1,400,000	

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
IPSec VPN Peers of up to 2500	
Virtual Interfaces (VLANs) support for at least 1000 VLANs for forming Secure server Farms and DMZs	
Scalability through clustering and load balancing	
Software Features	
Application Security Services	
The Firewall should have Integrated specialized inspection engines for protocols like HTTP, FTP, DNS, SNMP, ICMP, NFS, H.323, SIP, RTSP and many more	
The Firewall should provide advanced inspection services to detect and optionally block instant messaging, peer-to-peer file sharing, and other applications tunneling through Web application ports	
Inspection of H.323, SIP based voice and multimedia streams	
To provide TCP stream reassembly and analysis services to help detect attacks that are spread across a series of packets	
Network Containment and Control Services	
Inbound and outbound access control lists (ACLs) for interfaces, time-based ACLs, and per-user or -group policies for improved control over network and application usage	
Powerful reporting and troubleshooting capabilities that help enable collection of detailed statistics on which ACL entries are triggered by network traffic attempting to traverse a security appliance	
Rich dynamic, static, and policy-based NAT and PAT services	
Secure Connectivity Services	
IPSec VPN services for up to hundreds of simultaneous remote devices	
Support for Internet Key Exchange (IKE) and IPSec VPN standards with hub-and-spoke or meshed VPN configurations	
High-Availability Services	
Support for Active/Active & Active/Standby failover.	
Support for bidirectional state sharing between Active/Active failover pair members for support of advanced network environments with asymmetric routing (PBR) topologies, allowing flows to enter through one Firewall appliance and exit through the other, if required	
Support for Synchronizing all security association state information and session key material between failover pair members	
Support to perform software maintenance release upgrades on the Firewall failover pairs without affecting network uptime or connections	
Intelligent Networking Services	
Support for multiple virtual interfaces on a single physical interface	
Comprehensive OSPF & BGP dynamic routing services	
Capability to forward DHCP requests from internal devices to an administrator-specified DHCP server, helping enable centralized distribution, tracking, and maintenance of IP addresses	
Support for NTP to provide convenient method for synchronizing the clock on the firewall appliance with other devices on a network	

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
Flexible Management Solutions	
Support for Built-in Management Software for simple, secure remote management of the security appliances through integrated, Web-based GUI	
Should provide a wide range of informative, real-time, and historical reports that give critical insight into usage trends, performance baselines, and security events	
Accessible through variety of methods, including console port, Telnet, and SSHv2	
Strong authentication of users through the Firewall appliance through a local user database or through integration with enterprise databases, either directly using RADIUS and TACACS+	

11.   Gateway Level Antivirus

Table 13 Specifications- Gateway Level Antivirus

Make & Model Offered - (To be filled by the Supplier)	Compliance (Yes/No)
Gateway level Anti Virus should provide high-performance protection against viruses in SMTP, POP3, IMAP, HTTP and FTP traffic. It should block viruses and worms from penetrating into an organization's internal network through e-mail attachments, malicious Web pages, and files obtained through FTP.	
Virus gateway should provide real-time detection of viruses and malicious code at the gateway for SMTP, POP3, IMAP, HTTP, and FTP Internet traffic.	
The proposed solution should be licensed per unit and should support unlimited users	
Virus Gateway should have option to configure to respond to virus detection in several ways ie. Delete the file, quarantine the file, Alert email	
Frequent updates of virus pattern files should be available from the Web site, and option for scheduling for automatic download and installation should be available.	
In terms of SMTP AV scanning the solution should not act as mail relay or MTA by itself.	
Should have facility to block files based on file extensions over HTTP, FTP, SMTP, POP3 as well as IMAP	
Should have reporting facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc.	
If it is not integrated within firewall appliance then stand alone solution should not introduce delays	
Antivirus throughput of the appliance should be more than 900 Mbps minimum.	

12.   Intrusion Prevention System (IPS)

Table 14 Specification-Intrusion Preventive System

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
IPS should be either integrated with firewall and should have 2 Gbps IPS throughput or an external device.	

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
Should not induce Latency into the Network, Latency should be less than 200 microseconds	
The appliance monitors upto 4 inline segment and has 8 10/100/1000 interfaces for the same.	
The appliance should have separate dedicated 10/100/1000 Mbps interface for management console. None of the monitoring ports should be used for this purpose.	
The IPS should be deployable in the following modes: Passive or IDS mode, Inline Protection Inline Simulation	
IPS vendor should have its own original threat intelligence analysis center and is not overly dependent on information available in the public domain.	
IPS should detect and block all known, high risk exploits along with their underlying vulnerability (not just one exploit of that vulnerability).	
IPS should employ full seven-layer protocol analysis of all internet protocols and data file format.	
IPS should operate effectively and protect against high risk, high impact malicious traffic via default out of box configuration, should be able to block more than 2000+ attacks by default.	
IPS should have option of automatic download of signatures through vendor's own signature database and not relying on any third party updates. IPS should perform stateful packet inspection	
IPS should detect and block malicious web traffic on any port.	
Does TCP stream reassembly?	
Does IP defragmentation.	
Does Protocol anamoly detection	
Does Bi- directional inspection	
Detects attacks within protocols independent of port used	
Does RFC Compliance	
Does Protocol tunneling	
IPS should do attack recognition inside IPv6 encapsulated packets	
IPS should do active blocking of traffic based on pre-defined rules to thwart attacks before any damage is done.	
Accurately detects intrusion attempts and discerns between the various types and risk levels including unauthorized access attempts, pre-attack probes, suspicious activity, DoS, DDoS, vulnerability exploitation, brute force, hybrids, and zero-day attacks.	
Allows full policy configuration and IPS sensor control via encrypted communications with remote management system.	
Can enable/disable each individual signature.	
Each signature should allow granular tuning.	
Supports assigning of ports to custom applications.	
Filters traffic based on IP address or network range, protocol, and service in support of organizational security policy to allow/disallow specific types of activity between hosts.	
Should support Active/Passive and Active/Active for the appliance, the HA should be out of the box solution and should not requires any third party or additional software for the same.	
HA solution should support High Protection that is should maintain state such that there is no	

Make & Model Offered - (To be filled by the Supplier)	Complied / Not Complied
gap in protection during failure of one of the appliances.	
IPS should fail open in case of power, software or hardware failure when deployed in stand alone mode.	
IPS should notify console of unit interruption. The console should receive alert and/or provide additional notification to administrator should any component become non-operational or experience a communications problem.	
IPS should support granular management. Should allow policy to be assigned per device, port ,VLAN tag, IP address/range	
Management Console should be able to integrate and correlate with vulnerability assessment solution of the same brand/ third party.	
IPS should offer variety of built-in responses including console alerts, database logging, email notifications, SNMP traps, offending packet captures, and packet captures.	
IPS should offer Includes built-in reports. The console should be capable of producing graphical metrics and time-based comparison reporting.	
IPS vendor should have 24/7 security service update and should support real time signature update.	
Firewall, IPS, Antivirus and IPSec VPN solution should be ICSA/ FIPS 140-2 Level 2 certified	

13.   Back-Up Software

Table 15 Specifications- Back up Software

Make and Model Offered - (To be filled by the Supplier)	Complied / Not Complied
Backup Solution should be available on various Operating System platform like, UNIX (SUN Solaris, HP-UX and IBM AIX etc.), Linux, Netware, and Windows and etc. Should support clustered configurations of the backup application in a cluster. i.e. backup application should failover as a highly available resource in a cluster.	
The backup software should be capable of doing full, incremental, differential, and variable block based deduplicated backups.	
The backup software should be capable of performing self healing of backup indexes, this would include consistency checking on its indexes to verify if there is any corrupt data.	
The backup software should be able to encrypt the backed up data using 256-bit AES encryption.	
Software should have full command line support on above mention operating systems.	
Should have SAN support on above mention operating systems. Capable of doing LAN free backups for all platforms mentioned above.	
Should support "Hot-Online" backup for different type of Databases such as IBM DB2, Oracle, MS SQL, Sybase etc.	
Software should have an inbuilt feature for Tape to tape copy feature (cloning, within the tape library) to make multiple copies of the tapes without affecting the clients for sending tapes offsite as part of disaster recovery strategy.	
Should have the optional ability of staging the backup data on a disk and then de-stage	

Make and Model Offered - (To be filled by the Supplier)	Complied / Not Complied
to a tape based on the policy for faster backups.	
Should support NDMP backup to disk. Should support NDMP multiplexing of NDMP and no NDMP data to the same tape. The software should be capable of doing NDMP configuration through the GUI.	

14.   Enterprise Management System (EMS)

Table 16 Specifications- EMS

Make and Model Offered - (To be filled by the Supplier)	Complied / Not Complied
Functional and technical requirements (DR servers & DR networks can be monitored from primary site)	
The Enterprise & Network Management System should be used to manage all enterprise resources with a solution that encompasses the heterogeneous networks, systems, applications, desktops and databases present in the system. It should have the capability to consolidate all the information to one console with a support for providing a Web interface. Proposed solution must be from same OEM for seamless integration as well as OEM products should be recognized by industry analysts like Gartner/Forrestor/IDC.	
The discovery services in the EMS should discover systems, network devices and the topology. This capability allows for a complete inventory of all visible IT resources. The inventory scanning process should be able to discover any custom IT resources, such as CSC interface application etc.	
Solution should be inclusive with hardware, OS, patches, etc. and should have compatibility to standard RDBMS	
Solution should provide for future scalability of the whole system without major architectural changes.	
Should provide fault and performance management for multi-vendor TCP/IP networks.	
User Interface	
EMS should provide a Graphical User Interface which is user-friendly to depict all the IT infrastructure and applications, making IT management much more intuitive.	
The EMS should offer a Web browser interface. The Web browser interface should enable management of IT resources via Internet or Intranet access or through Dial Up/remote access. EMS should be integrated with GIS solution.	
Event Management	
The EMS should offer a unique solution to the problem of managing exception events. It should correlate and filter events from different types of IT resources, and pinpoint the root cause of a problem.	
This event manager should also permit integrating custom applications with the EMS. It should be used to integrate not only management applications, but also general business applications to make them easier to manage. With event filtering and correlation, multi-level managers and agents, automatic corrective measure, the EMS should provide comprehensive event management capabilities. It should eliminate the clutter of spurious alarms and simplify the	

Make and Model Offered - (To be filled by the Supplier)	Complied / Not Complied
management of complex IT infrastructure.	
It should help to notify through cell phone and email, of various/selective events occurring in the enterprise.	
Software Distribution	
The software distribution function should provide flexible and scalable delivery, installation, and configuration of software.	
The software distribution should support customizable distribution schedules, alternate methods, heterogeneous network protocols, diverse operating systems including UNIX, and both push and pull distribution modes.	
Compression should be supported while distributing the software across WAN.	
Furthermore, its integration with the event management functions of the EMS should provide complete tracking, logging, and automated correction of failures during the delivery and installation process. In addition, its integration with the security functions of the EMS should enable administrators to deliver software with peace of mind.	
It should be possible to store images of the servers and desktops and restore images from the image server automatically.	
Network & Server Management	
The Network Management function must monitor performance across heterogeneous networks from one end of the enterprise to the other.	
It should proactively analyze problems to improve network performance.	
The Network Management function should have extensive reporting facility, providing the ability to format and present data in a graphical and tabular display	
The Network Management function should collect and analyze the data. Once collected, it should automatically store data gathered by the NMS system in a database. This enterprise-wide data should be easily accessed from a central location and used to help with capacity planning, reporting and analysis.	
The Network Management function should also provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment and the top-contributing hosts, WAN links and routers.	
Alerts should be shown on the Event Management map when thresholds are exceeded and should subsequently be able to inform Network Operations Center (NOC) and notify concerned authority using different methods such as pagers, emails, etc.	
It should be able to automatically generate a notification in the event of a link failure to ensure proper handling of link related issues.	
The Systems and Distributed Monitoring (Operating Systems) of EMS should be able to monitor: • **Processors**: Each processor in the system should be monitored for CPU utilization. Current utilization should be compared against user-specified warning and critical thresholds. • **File Systems**: Each file system should be monitored for the amount of file system space used, which is compared to user-defined warning and critical thresholds. • **Log Files**: Logs should be monitored to detect faults in the operating system, the communication subsystem, and in applications. The function should also analyze the files residing on the host for specified string patterns. • **System Processes**: The System Management function should provide real-time	

Make and Model Offered - (To be filled by the Supplier)	Complied / Not Complied
collection of data from all system processes. This should identify whether or not an important process has stopped unexpectedly. Critical processes should be automatically restarted using the System Management function. • **Memory**: The System Management function should monitor memory utilization and available swap space. • **Event Log**: User-defined events in the security, system, and application event logs must be monitored.	
Reporting	
The Reporting and Analysis tool should provide a ready-to-use view into the wealth of data gathered by Management system and service management tools. It should consolidate data from all the relevant modules and transform it into easily accessible business-relevant information. This information, should be presented in a variety of graphical formats can be viewed interactively (slice, dice, drill down, drill through).	
The tool should allow customers to explore the real-time data in a variety of methods and patterns, and then produce reports to analyze the associated business and service affecting issues.	
The presentation of reports should be in an easy to analyze graphical form, enabling the administrator to put up easily summarized reports to the management for quick action (Customizable Reports). The software should be capable of supporting the needs to custom make some of the reports as per the needs of the organization.	
Provide Historical Data Analysis: The software should be able to provide a time snapshot of the required information as well as the period analysis of the same in order to help in projecting the demand for bandwidth in the future.	
SLA Monitoring	
EMS should integrate with the application software component of portal software that measures performance of system against the following SLA parameters: • Response times of Portal; • Transaction handling capacity of application server in terms of number of concurrent connects; • Uptime of data center/ Servers; • Meantime for restoration of Data Center, Services etc. • Network Specific SLAs • System Specific SLAs • Application Specific SLAs • End-to-End Service Based SLAs	
EMS should compile the performance statistics from all the IT systems involved, including the EQMS and compute the average of the parameters over a month, and compare it with the SLA metrics laid down in this document;	
The EMS should compute the weighted average score of the SLA metrics and facilitate arriving at service charges payable to the Agency, after applying the system of penalties and rewards.	
The SLA monitoring component of the EMS should be under the control of the authority that is nominated to the mutual agreement of Purchaser & the Supplier, so as to ensure that it is in a trusted environment.	
Helpdesk Management	

Make and Model Offered - (To be filled by the Supplier)	Complied / Not Complied
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 proposed helpdesk solution must support at least 3 ITILv3 processes like request management, problem management, configuration management and change management with out-of-the-box templates for various ITIL service support processes. Bidder should provide ITIL v3 certification from OGC on at least 3 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 technical 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	
The proposed helpdesk solution must allow the IT team to see the CI relationships in pictorial format, with a specified number of relationships on single 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.	
The proposed helpdesk solution must have an integrated CMDB for better configuration management & change management process.	
It should support remote management for end-user & allow analysts to do the desktop sharing for any system located anywhere, just connected to internet.	
Remote desktop sharing in Service desk tool should be agent less & all activity should be automatically logged into the service desk ticket.	
It should allow IT team to create solution & make them available on the end – user login window for the most common requests	
The proposed Fault Management Solution must support integration with proposed help desk or trouble ticketing system in the following ways: • Creates tickets when requested by Fault Management operators • Automatically creates tickets based on alarm type • Provides a link to directly launch a Service Desk view of a particular ticket created	

Make and Model Offered - (To be filled by the Supplier)	Complied / Not Complied
by alarm from within the Network Operation console.	
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 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.	
The proposed NMS should provide unified workflow.	
Application Performance Management System	
The proposed solution must determine if the root cause of performance issues is inside the monitored application, in connected back-end systems or at the network layer from a single console view	
The proposed solution must proactively detect business critical transactions from various locations before it affects the real users; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes	
The proposed solution must provide deeper end-to-end transaction visibility by monitoring at a transactional level and without deploying any software at end user desktop. The solution must provide a single view that shows entire end-to-end real user transaction and breaks down times spent within the application components, SQL statements, backend systems and external 3rd party systems.	
The proposed solution must be able to provide root-cause probability graphs for performance problems showing the most probable root-cause area within application infrastructure.	
The proposed solution must provide real-time monitoring of resource utilization.	
The proposed solution must identify any changes to application configuration files(.xml, properties etc), File system or application code and be able to correlate changes to application performance dynamically in production environments.	
The proposed solution must proactively identify any thread usage problems within applications and identify stalled or stuck threads. The proposed solution must also monitor web services across multiple processes	
The proposed solution should allow access to performance data both using a Graphical user interface (GUI) and web based access and provide ability to monitor performance of applications up to the method level of execution (Java/.Net method) 24x7 in production environments with negligible impact on monitored application.	
The proposed solution should measure the end users' experiences based on transactions without necessitating installation of client agents / probes on end-user desktops.	
The proposed system must be able to detect user impacting defects and anomalies and reports them in real-time. The proposed system must also be able to provide user usage analysis and show how user's success rate, average time and transaction count has changed over a specific period of time such as current week versus previous week.	
The proposed system must be able to pro-actively determine exactly which real users were impacted by transaction defects, their location and status.	
The proposed system must be able to provide the ability to detect and alert when users	

Make and Model Offered - (To be filled by the Supplier)	Complied / Not Complied
experience HTTP error codes such as 404 errors or errors coming from the web application.	
Network Configuration Management	
Network Configuration management is a critical part of CCTNS project it must have following features and seamlessly integrated with Network Fault and Performance Management: • The solution must provide a method of importing devices via network scan, CSV, using nmap & snmp, etc. • The Proposed solution should capture a snapshot of the current state of the network, including topology and virtual LAN (VLAN) information. • The Proposed solution should report all asset tracking related information, e.g. number & type of device, what OS devices are running, serial numbers, custom data fields etc. Companies can then verify accuracy of assets, service contracts etc • The Proposed solution should support tracking of differences from running to startup configuration files and provide a mechanism to easily resolve the synchronization issue. The Proposed solution should allow for rapid response and oversight to potential network outages due to mismatched startup configuration files. • The Proposed solution should provide comparison of any two configuration files with difference of changes (new lines/deleted lines/modified lines). This is helpful in troubleshooting and quickly identifying what changed. • The Proposed solution should help deploy configurations to devices for rapid rollback to known good states as well as for device replacement purposes, etc. The Proposed solution should able to generate scripts from proxy sessions. • System must provide a way for certain users to override the need for approval in an emergency, but not before entering mandatory reasons. For example, a network engineer needs to restore a device which is currently down at the middle of night, his manager will get notified about the overridden task and the why. • System must provide a full audit trail of approval process including owners / approvers, comments, rejections and re-submissions. Audit trails should provide accountability and help to ensure processes are functioning properly. • System must be able to define custom policy rules in a very flexible manner. For example, a network engineer wants to check all the vty lines in a group device are configured with passwords and ssh only. • Add/Remove ACL lines across multivendor groups of devices, should support group changes of ACL settings across multiple network devices and ACL IDs • The Proposed solution should support backing up of the OS images from the device in addition to the configuration file for full redeployment ability. The Proposed solution should not require any automation services to be stopped while updating devices. • The Proposed solution should support bidirectional monitoring integration • The Proposed solution should support Granular APIs, including Java, Perl, and SOAP for customizations • The Proposed solution should support integration with different vendors to automate download of security and compliance related patches.	

2. Request for Proposal Volume II

2.1 Section 3: Bidding Process Details

1. Clause 3.2.13: Venue & Deadline for submission of proposals

Addition of following point:
d) If the last date for submission of the Tender/Bid turns out to be a holiday, it will automatically be extended to next Government working day.

2. Clause 3.4.4: Pre-Qualification Criteria

a) Point g (iv)
The Bidder (System Integrator) should have net worth of not less than Rs. 30 Crores for each of the last three financial years (as Rs. **2 Crores** on 31-03-2010).

Stands amended as

The Bidder (System Integrator) should have net worth of not less than Rs 30 Crores for each of the last three financial years.

b) Point g(v)
The bidder must have prior experience of working on at least 1 Software Services Project3 for Government of India, any of the Odisha government. The project must be worth at least Rs 2 Crores.

Stands amended as

The bidder must have prior experience of working on at least 1 Software Services Project for Government of India/ any of the Odisha government. The project must be worth at least Rs 2 Crores.

3. Clause 3.4.6: Technical Evaluation Scoring Matrix

Addition of following point:
The evaluation of the bids will be done by Technical Committee to be constituted by the state and the details in this regard will be decided by the Competent Authority in due course. Bidders are advised to propose the best possible resources and solutions.

2.2 Section 5: Payment Terms and Schedule

1. Clause 5.3.1: Milestones and Payment Schedules for Implementation Phase

Payment Milestones for the Implementation phase as mentioned in Clause 5.3.1 *stands amended as*

Table 17 Payment Milestones

S. No.	Payment Milestones for the Implementation phase	% Payment of Sub-total for Services Provided During Implementation Phase .Refer to Component A (Sum of items 1 – 9) in the Pricing Summary Table
1.	M1: Completion of Preparatory Activities i. Project Plan and setup of Program Management Office ii. Configuration, Customization, and Enhancement of CAS (State) including Systems Study & Assessment, UAT Performance Testing & Intensive Field Testing iii. Procure, Commission and maintain Project Management, Configuration Management and Issue Tracker Tools iv. Site preparation, commissioning, operationalization of IT infrastructure of District Training Centers and Regional Training Centre v. Setup and management of IT infrastructure at the Data Center and DR Site	5%
2.	M2: Pre – Go Live Readiness in the Phase I Districts	5%
3.	M3: Go-Live in the Phase I Districts (<<Limit to one or two Districts in the State in Phase I>>)	10%
4.	M4: Pre – Go Live Readiness in the Phase II Districts	10%
5.	M5: Go-Live in the Phase II Districts	5%
6.	M6: Pre – Go Live Readiness in the Phase III Districts	15%
7.	M7: Go-Live in the Phase III Districts	5%
8.	M8: Pre – Go Live Readiness in the Phase IV Districts	10%
9.	M9: Go-Live in the Phase IV Districts	5%
10.	M10: Go-Live in all the remaining 10% of Police Stations Higher Offices	15%
11.	M11: Go-Live in all the remaining Police Stations / Higher Offices	5%
12.	M12: Successful integration with CAS(Center) and successful transfer of the data for three months in succession	10%

2.3 Section 6: Annexure

1. Clause 6.6.26: Technical Bill of Materials for Software

Technical Bill of Materials for Software Clause 6.6.26 Table No.19 *stands amended as*

Table 18 Bill of Materials for Software

The below list is indicative only In case the number of licenses offered are different for each of the services within the solution (ex, multiple services within EMS are provisioned with different licenses), please insert rows under the solution head and provide the information	Proposed Solution (Provide the Product Name or fill Custom Built, in case of a new development) It is possible that the SI has not suggested the solution as the list is indicative only. In case any of the item is not provided, the SI may indicate N/A in the corresponding cells	Unit of Measurement	Number of Licenses (UAT) Please indicate N/A where not applicable Please indicate N/L where there is no license requirement	Number of Licenses (Training) Please indicate N/A where not applicable Please indicate N/L where there is no license requirement	Number of Licences (Data Center - Production) Please indicate N/A where not applicable Please indicate N/L where there is no license requirement	Number of Licences (DR Site) Please indicate N/A where not applicable Please indicate N/L where there is no license requirement
CAS (State) Solution						
Webserver						
Application Server						
Database						
Operating System						
Others						

Reporting Engine						
Email/Messaging						
Search Engine						
Portal Server						
Workflow Engine						
Rules Engine						
Directory Services						
DMS/CMS						
Security						
Audit						
ETL						
Any Other Proposed						
CAS (State) Offline Solution						
Synchronization Solution						
Application Container						
Database						
Others						
Operating System (In case the suggested solution will need a particular kind of O/S on the client machine)						
Any Other Proposed						
Technical Environment at SCRB						
Configuration Management						

Issue Tracker						
Any Other Proposed						
Infrastructure Services (at DC/DR)						
EMS						
Server Load Balancer						
Backup Software						
Helpdesk						
Antivirus						
SAN Management Software						
Any Other Proposed						

2. **Clause 6.6.27: Technical Bill of Materials for Client Side Infrastructure.**

Bills of Material of Client site Infrastructure as mentioned in Table no.20 of _stands amended as_

<div align="right">Table 19 BOM Client Site Infrastructure</div>

Client Side Infrastructure	Quantity	Make and Model	Year of Introduction	Operating System along with version (if applicable)	Additional Information as required to indicate the compliance to the requirements in the RFP (ex, Capacity, Disk Space,….)	Compliance Matrix Provided as per the format given in the the RFP (Yes/No)	Data Sheets Provided in the Proposal (Yes/No)
Desktops							
HDD 160GB							
Duplex Laser Printer							
Multi-function Laser(Print/Scan/Copy)							
UPS(2KVA) for 120 minute back-up							
2 KVA Generator Set							
16-Port Switch							
Fingerprint Reader							
Digital Camera							
Electronic Pen							

Client Side Infrastructure	Quantity	Make and Model	Year of Introduction	Operating System along with version (if applicable)	Additional Information as required to indicate the compliance to the requirements in the RFP (ex, Capacity, Disk Space,….)	Compliance Matrix Provided as per the format given in the the RFP (Yes/No)	Data Sheets Provided in the Proposal (Yes/No)
Switch for Higher Offices							
Any Other Item as Required							

3. Clause 6.7.2: Form 1: Pricing Summary

Pricing summary as mentioned in clause in 6.7.2 _stands amended as_

Table 20 Pricing Summary

S. No.	Description	Total Price (INR)	Taxes and Other Duties	Total Amount (INR)	Total Amount in Words
	Services Provided During Implementation Phase				
1.	Project Planning & Management, Systems Study and Configuration Customization and Extension (New Modules) of CAS (State) and Integration with CAS (Center) and Support to 3rd party acceptance testing, audit and certification				
2.	Data migration and Digitization of Historical Data				
3.	Site preparation, commissioning, operationalization of IT infrastructure of District Training Centers and Regional Training Centre				
4.	Site Preparation at Police Stations and Higher Offices				
5.	Procurement, Delivery, Commissioning of IT Infrastructure at Police Stations and Higher Offices				
6.	Capacity building and Change Management				
7.	Co-ordination and management of network connectivity				
8.	Setup and management of IT infrastructure at the Data Center and Disaster Recovery Center				
9.	Handholding Support				
A	Sub-total for Services Provided During Implementation Phase (Sum of items 1 – 9):				
B	Blended Person Month Cost for 300 Person Months				
C	Blended Cost of Data Migration / Digitization of 1GB of data				
D	Blended Cost of Site Preparation for 10 Offices each of 1500 Sqft with 4 computers				
E	Blended Cost of Providing Handholding Support for all Police Stations (One person per Police Stations for a period of 6 months)				
Services Provided During Post Implementation Phase					
10.	Operations and Maintenance Services for the 1st year after "Go-Live"				
11.	Operations and Maintenance Services for the 2nd year after "Go-Live"				
12.	Operations and Maintenance Services for the 3rd year after "Go-Live"				
13.	Operations and Maintenance Services for the 4th year after "Go-Live"				

S. No.	Description	Total Price (INR)	Taxes and Other Duties	Total Amount (INR)	Total Amount in Words
14.	Operations and Maintenance Services for the 5th year after "Go-Live"				
F	Sub-total for Services Provided During Post Implementation Phase (Sum of items 10 – 14):				

4. Form 2: Procurement, Delivery, Commissioning of IT Infrastructure at Police Stations and Higher Offices

Details of Procurement, Delivery, Commissioning of IT Infrastructure at Police Stations and Higher Offices as mentioned in Table 26, clause in 6.7.3 _stands amended as_

Table 21 Details of Procurement,Delivery,Commisioning of IT Infrastructure at PS and Higher Offices.

	Original supplier	Item Desc.	Unit of measurement	# (units)	Price per unit	Total price	Taxes and other duties	Total amount (INR)
Desktops								
Client Side Software Licenses (OS, Office, Anti-virus,…)								
Please Insert Details as required.								
HDD 160GB								
Duplex Laser Printer								
Multi-function Laser(Print/Scan/Copy)								
UPS for 120 minute back-up								
2 KVA Generator Set								
16-Port Switch								
Fingerprint Reader								
Digital Camera								
Electronic Pen								

UPS 2KVA(for District SP Offices)								
UPS 2KVA(For DGP and Police Headquarters)								
Switch for Higher Offices								
Any Other Item as Required								
Please insert detail as required								
Total amount (INR)								

5. Form 3: Details of the software solution components

Details of Software Solution as mentioned in Table 27, clause in 6.7.4 stands _amended as_

The list of items mentioned below is indicative only. Bidder is advised to list down the components as per the solution proposed.

Table 22 Details of Software Components

Items	Original supplier	Item Desc	Unit of measurement	# (units)	Price per unit	Total price	Taxes and other duties	Total amount (INR)
CAS (State) Solution								
Webserver								
Application Server								
Database								
Operating System								
Others								
Reporting Engine								
Email / Messaging								
Search Engine								
Portal Server								
Workflow Engine								
Rules Engine								
Directory Services								
DMS/CMS								
Security								
Audit								
ETL								
Any other Proposed								

CAS (State) Offline Solution								
Synchronization Solution								
Application Container								
Database								
Any Other Proposed								
Technical Environment at SCRB								
Project Management Information System								
Configuration Management								
Issue Tracker								
Any Other Item as Required								
Infrastructure Services (at DC/DR)								
EMS								
Server Load Balancer								
Backup Software								
Helpdesk								
Antivirus								
SAN Management Software								
Any Other Proposed								
Total amount (INR)								

3. Request for Proposal Volume III

3.1 Section 2: Structure

1. Clause 2.7: Performance Bank guarantee

SI warrants to provide bank guarantee for the Contract as a whole, valued at 10% of value of the Contract valid for the Operative Period of Contract. **("Performance Bank Guarantee") or ("PBG")**

Stands amended as

SI warrants to provide bank guarantee for the Contract as a whole, valued at Rs. 5 Crore valid for the Operative Period of Contract. . **("Performance Bank Guarantee") or ("PBG")**

3.2 Section 4: Payment Terms

2. Clause 4.3 (c): Payment of Tax / Tax Considerations
In the event of any increase or decrease of the rate of taxes due to any statutory notification/s during the term of the Contract, the consequential effect shall be to the account of SI.

Stands amended as

Any **increase** in tax structure or statutory amendment subsequent to submission that results in any change in taxes, duties shall be borne by customer. Any **decrease** in tax structure or statutory amendment subsequent to submission that results in any change in taxes, duties shall be passed on to the customer; the prices charged shall stand reduced by the corresponding amount.

3.3 Section 5: Representation and Warranties

1. Clause 5.1 Point (q): Representations and Warranties and Covenants of SI
Provide support in terms of annual maintenance for a minimum period of three years from the date of Go Live

Stands amended as

Provide support in terms of annual maintenance for a minimum period of five years from the date of Go Live

3.4 Section 9: Termination And Transfer

1. Clause 9.4.1: Transfer of assets
A decision on balance payment left for the assets deployed before the date of termination will be taken on a case to case basis. Reasons for the Termination will be examined and payment will be considered only after the task is completed.

3.5 Section 27: Terms Of Payment Schedule

1. Clause 27.1: Performance Bank Guarantee

As required a PBG of 10% of value of the contract will be furnished by the SI in the form of a Bank Guarantee as per format provided in the RFP from Indian Public Sector Banks authorized by the Government to conduct Government transactions

Stands amended as

As required a PBG of Rs. 5 Crore of value of the contract will be furnished by the SI in the form of a Bank Guarantee as per format provided in the RFP from Indian Public Sector Banks authorized by the Government to conduct Government transactions