Table of Contents

32 Annexure 32- General Specifications for Hardware

The bidder shall be responsible for the complete IT hardware solution, any issues arising out of performance should be dealt as per the best practices, adherence to the SLA's, data integrity must be maintained of highest level and DDA should be notified immediately in case of any breach / deviation. The hosting arrangements shall at minimum meet the following criteria:-

a) The service provider will provide state of the art hardware with 24 X 7 monitoring.

b) The configuration of the all the hardware supplied for this project should be robust and capable of handling the load as per RFP termsand subsequent corrigendum issued (if any).

c) The bidder shall devise an appropriate framework for security at the data center and at a minimum shall include Firewalls, IDS, IPS, Antivirus, Anti spamming and regular security audits, etc.

Solution Procurement: - The Bidder shall provide various licenses to support DDA requirement under different categories as mentioned below. Bidder ~~Application Developer~~ will provide a comprehensive solution based on the information provided by DDA& load test results.

Hardware Procurement: The Bidder shall finalize and procure the hardware and network capability requirement in order to meet the performance requirement as specified, technical requirement including acceptance test / quality control parameters for tender document. The specifications should be provided for development, quality & production servers, storage and others as required including RDBMS and other applications suggested as an overall solution as per the project timeline set in. In addition, a well laid out approach and roadmap for hardware enhancements shall be devised.

The following section represents the minimum requirements of DDA in terms of hardware, software and other security and networking components required for implementing the solution. **Bidders are advice to use these as a bare minimum requirement and are encourage to propose best solution meeting the overall requirements.**

32.1 General Requirement Servers:

S. No.	Item	Description	Compliance (Yes/No)
1	**General Requirements of Server**	The servers shall be sized, procured and installed by Bidder independently considering the business requirements and workload details provided.	Yes
		Bidder shall provision the server infrastructure required for the solutions at the DC and DR sites.	Yes
		The infrastructure at the above sites will require different types of servers. Bidder is responsible for understanding the requirements of the application and provide servers as required to make the solution complete. The servers shall be sized such that it shall not utilize more than 70% of its resources (CPU and I/O) in normal course (with an exception to the batch	Yes

S. No.	Item	Description	Compliance (Yes/No)
		processes). The utilization shall not exceed 70% for a sustained period of more than 15 minutes.	
		All the proposed servers shall be full blade servers /rack servers (as per corrigendum clarification Point 31 of page 9 of 84 in Volume 1 of Pre-bid Clarifications) only with scalability for additional CPU, Memory and I/O. The servers shall have adequate number of CPUs with latest clock speed and cache as on last date of Bid.	Yes
		The servers shall be based on Symmetrical Multiprocessing (SMP) architecture. Each server shall be populated with adequate number of internal disks. The disks shall be Hot Swappable and shall be in hardware mirrored Each server shall be populated with adequate number of Gigabit full-duplex Ethernet controllers for LAN connectivity. The Ethernet controllers shall be configured for dual homing and they shall provide adequate throughput to each switch based on the solution deployed on the server.	Yes
		The servers that need connectivity to SAN shall be populated with adequate number of Fibre Channel Host Bus Adaptors (HBA) in redundant mode. The blade /rack servers shall be with redundant and hot swappable power supplies. All the servers shall be populated with read-only drive, capable of reading all types of CD / DVD.	Yes
		None of the servers shall be populated with any writeable media. Bidder shall propose switch based consoles within the datacentre for monitoring and managing the servers. Every server shall not be provisioned with monitor, keyboard and mouse individually. It is envisaged that the servers shall also be monitored remotely using the EMS solution. Bidder shall provide requisite licenses for all the software required for the respective servers including, but not limited to, Operating System, respective software database and application, etc.	Yes
		Bidder shall propose servers after taking into account the design consideration mentioned in the requirements specification	Yes

S. No.	Item	Description	Compliance (Yes/No)
2	**Web Servers**	The Web Servers will be mainly used for running the HTTP Server to manage connections of end-user sessions. Bidder shall provide requisite licenses for all the system software required for the web server including, but not limited to, Operating System, etc. The server would be used for providing access to the access control applications through internet / intranet. Using portal, relevant contents of the applications can be easily enabled, updated and deployed at the earliest. Web server would provide a base template to users who want to access the application via internet. The portal server shall allow users to access the application from internet and the same shall be configured in cluster mode.	Yes
3	**Application Servers**	Would mainly be used for running the business logic of the application. Shall be sized by the bidder independently considering users workload. Bidder shall provide requisite licenses for all the system software required for the application server including, but not limited to, Operating System, Application Server Software, etc. Application server would take care of the necessary workflow and web / portal server would be required for the interfacing with the end user. Both the portal and application server would be seamlessly integrated to provide high availability and performance. With the use of load balancers, user requests would be distributed among various clustered/common servers. The application servers will be configured in active – active and in cluster mode and shall also have the database configured accordingly. The solution should be able to detect a failed Application server so that no further traffic is directed to the failed node(s).	Yes
4	**Database Sever**	The dedicated database server shall have ability to process mixed transaction loads (batch and online) and have the ability to dynamically configure processor power according to workload requirements. The server shall be configured in active-passive mode. The Database solution must be benchmarked in TPC. The server shall have industry standard operating system such as Microsoft Windows, flavors of UNIX e.g. HP-UX, IBM AIX, Red Hat Linux, etc. Bidder shall undertake **Operating**	Yes

S. No.	Item	Description	Compliance (Yes/No)
		system hardening and security related measures through appropriate configuration and patch updates on a regular basis.	
5	**DNS Servers**	Bidder shall provision servers which will be mainly used for running the Domain Name Service (DNS) and Time Synchronization Service. The server shall run Domain Name Service for resolving the domain names for the application. This server shall also have the capability to run the Time synchronization service. This service shall be used to synchronize the clocks in all of the servers and devices in the Datacentre. The time synchronization service shall synchronize clocks of all the servers with the world time clock on a regular basis. **Bidder shall provide requisite licenses** for all the system software required for the DNS server including, but not limited to, Operating System, Domain Name Service, Time Synchronization Service, etc.	Yes
6	**Anti-virus Servers**	Bidder shall provision servers for running the Security Solution as per requirements mentioned Bidder shall provide an Anti-virus server for downloading anti-virus updates from internet. The Anti-virus servers shall be sized by bidder independently depending on the Anti-virus solution and as per the requirements provided. Bidder shall provide requisite licenses for all the system software required for the Anti-virus server including, but not limited to, Operating System, etc.	Yes
7	**Backup server**	Backup server would be used for backing up the key data on regular interval. The backing up of the data would be an automated process. Whenever desired the backed up data can be restored/retrieved to the desired system configuration.	Yes
8	**Firewall**	Firewall will be a part of network that is designed to block unauthorized access while permitting outward communication. Firewall will be installed at (PoD) server zone to provide features like high-availability and fault tolerance.	Yes

S. No.	Item	Description	Compliance (Yes/No)
9	**Load Balancer**	The load balancer would be required for distributing workloads to a set of networked computer servers in such a manner that the computing resources are used in an optimal manner. The load balancer will support segmentation/virtualization to distribute load for multiple services, servers. This would increase the availability of the server and will also increase the performance as multiple servers would be sharing the service load. The load balancer would be used for the following servers: Application Server, Database Servers, Web Server.	Yes
10	**AAA Server**	The AAA Server Software should come integrated along with its own operating system as a virtual appliance which could be hosted on a hypervisor. AAA Server should provide authentication services to all the users connecting to the network, should enforce security policies on the end stations. Should offer centralized command and control for all user authentication, authorization, and accounting from a Web-based, graphical interface, and distribute those controls to hundreds or thousands of access gateways in the network. Should provide the manageability and administration of user access through network devices like: routers, switches, firewalls, VPNs.	Yes
		The AAA Server should have the following features: Should control administrator access and configuration for all RADIUS enabled network devices in network. AAA server should provide Automatic service monitoring, database synchronization, and importing of tools for large-scale deployments. Should have support for Lightweight Directory Access Protocol (LDAP) and Open Database Connectivity (ODBC) user authentication. AAA shall support IP address allocation from RFC standard DHCP servers. IP address pools could be defined with actual address assignment made by DHCP, and these addresses shall be assigned to users anywhere on the network. AAA shall support DHCP extensions, allowing DNS	Yes

S. No.	Item	Description	Compliance (Yes/No)
		entries to be dynamically created and deleted. Support Flexible 802.1X authentication type, including EAP-TLS, PEAP, LEAP, EAP-FAST and EAP-MD5 Support downloadable access control lists for any Layer 3 device, including Routers, Firewalls, and VPNs Device command set authorization Network access restrictions, User and administrative access reporting Should have a Web-based user interface to simplify and distribute configuration for user profiles, group profiles. Lightweight Directory Access Protocol (LDAP) authentication forwarding support for authentication of user profiles stored in directories from leading directory vendors. Should also provide time-of-day, network use, number of logged sessions, and day-of-week access restrictions	
		Security: The system shall ensure Extensible Authentication protocol (EAP); EAP-MD5-Challenge Simple CHAP like password based authentication. Certificate based mutual authentication of client and access point server. EAP-Protected EAP (PEAP) Single sided Certificate authentication (like SSL) for secure EAP Different access levels for each AAA Server administrator-and the ability to group network devices-enable easier control and maximum flexibility to facilitate enforcement and changes of security policy administration over all the devices in a network.	Yes

32.2 Technical Fact Sheet of Servers

All below mandatory requirements need to be provided by the System Integrator as part of the solution. Noncompliance to any mandatory requirement shall not be considered and the bid shall be declared as Non-responsive. Non-responsive bids shall not be considered for further evaluation.

S. No.	Parameter	Specification	Compliance (Y/N)
1.	Server CPU	RISC/EPIC/x86 Server of latest make and model and minimum clock 2.20 GHz. Two Socket server should be configured with minimum of 24 coresper server and should have a minimum all cache of 60 MB Per Socket. Adequate number of Sockets/Processor Cores should be configured to meet the minimum performance criteria. The estimated SPECint2006_rate for offered clock should be made available at SPEC.org The servers that need connectivity to SAN shall be populated with adequate number of Fibre Channel Host Bus Adaptors (HBA) in redundant mode. The blade/rack servers shall be with redundant and hot swappable power supplies. All the servers shall be populated with read-only drive, capable of reading all types of CD / DVD	
2.	Memory	The System should be quoted with minimum 16 GB per Active core. Memory should be minimum DDR3 ECC, with minimum clock of 1066 MHz. The server should have enough free slots to scale to 1.5X of Memory Offered	
3.	Internal Disk	Minimum 6X600 GB 10K RPM SAS SFF-3 should be configured The server should be capable of total 8X600 GB SAS SFF-3 internal drives on the existing storage backplane and any further storage capacity can be taken to the SAN setup.	
4.	Input/output	Slots have to be minimum PCIe Gen 3Minimum 4 x 1G RJ 45 and 4X10G SR Ethernet ports across 2 different adapters (not inbuilt in mother board)Minimum 4X2Ports 8GBps FC Adapter across 2 different adapters.	
5.	Power Supply	Hot Swap and Redundant	

S. No.	Parameter	Specification	Compliance (Y/N)
6.	Virtualization	Virtualization software offered should be of Enterprise class and should allow dynamic movement of CPU resources	
7.	Operating System	64 bit Latest Generation OS with having min 4-5 years future roadmap	
8.	Clustering	All production apps and DB Instance, along with the DR infrastructure will be clustered using high availability clustering technology and there should not be any single point of failure in the offered solution. Each of the production components shall have dedicated fail-over mechanism. The Clustering Solution diagram must be submitted in the Technical offer. Each cluster should have multiple interconnect through different Ethernet switches. The servers/partitions specified in cluster shall be in high availability cluster. Redundant Heart beat paths to be provided.	
9.	Support	The High Availability cluster shall be with adequate redundancy and with equal performance and configuration, and will have access to the same database and storage. **5 Years 24*7 Support, Directly from Server Vendor**	

32.3 Technical Fact Sheet of Enterprise RDBMS

DDA contains record for citizens of the state. The Data Repository layer; where such citizen information is stored; should be:

a) Highly Available

b) Highly Performant

c) Highly Secured

d) Self-Managing

The Database shall comprise of:

a) A comprehensive electronic record **of approx. 1.5 crores residents of the state.** Also take into account 10% increase in population per year which should be considered while overall sizing for the project.

b) Capable to handle high volume transactions, approximately the peak value would be 1, 50,000 transactions per day and around 7000 users.

All below mandatory requirements need to be provided by the Bidder / System Integrator as part of the solution. Noncompliance to any mandatory requirement shall not be considered and the bid shall be declared as Non-responsive. Non-responsive bids shall not be considered for further evaluation.

S. No.	Specification	Compliance (Y/N)
1	The database software should be available in all the hardware architectures, operating systems (Major UNIX, Linux and Windows environments) with identical functionalities and user interface	
2	The database software should be able to work on Uniprocessor, SMP system, and cluster systems.	
3	The database software should have the capability to store relational, text, image, spatial data structures and datasets within the database	
4	The same Database should support mixed OLTP/OLAP workloads	
Availability and Scalability Characteristics		
5	Database should have native, active-passive clustering with objectives of scalability and availability of 24x7. It should be capable by masking outages from end users and applications by recovering the in-flight database sessions following recoverable outages.	
6	The database clustering solution should support vertical & horizontal scalability with no downtime and without repartitioning or changes to the database objects or 3rd party transaction routing mechanisms.	
7	~~THE DATABASE CLUSTERING SHOULD PROVIDE CONCURRENT ACCESS FROM MULTIPLE SERVERS TO THE SINGLE DATABASE IMAGE~~. REMOVED IN CORRIGENDUM.	
8	The database clustering should provide intelligent load balancing across all available nodes.	
9	The database clustering solution should provide multiple nodes to participate in the parallel execution of queries	
10	The database clustering solution should use a very efficient messaging and row-level locking based algorithm to avoid negative	

S. No.	**Specification**	**Compliance (Y/N)**
	performance impact.	
11	Database should have native capability to provide database level storage management mechanism, which should enable the availability by means of creating redundancy, automatically balance the data files across the available disks, I/O balancing across the available disks for the database for performance, availability and management.	
12	Database should provide horizontal scalability in such a manner that a new database node can be added (or removed) dynamically, as and when required in future, without disturbing the normal functioning of production system such as without shutdown. This should be online and supported by native database clustering components.	
13	Database should have built-in Disaster Recovery solution to replicate the changes happening in the database across multiple DR Sites with an option to run real-time reports from DR Sites without stopping the recovery mechanism	
14	There should be option of configuring Disaster Recovery environment in SYNC and ASYNC mode.	
15	Database should have the capability to offload backup and reporting at the Disaster Recovery site.	
16	DATABASE SHOULD HAVE THE CAPABILITY TO PROVIDE ZERO DATA LOSS AT ANY DISTANCE WITHOUT PERFORMANCE IMPACT AND WITH MINIMAL COST OR COMPLEXITY. However, "RPO<30 MINIUTES IS THE OBJECTIVE. BIDDERS ARE ADVISED TO PROVIDE BEST IN CLASS SOLUTIONS AS PER INDUSTRY STANDARDS TO MEET THIS."	
17	The Database at the disaster recovery site should have capability for corruption detection and automatic repair.	
18	Database should have extensive High Availability /Disaster Recovery support for customer applications as well as for any other custom applications.	
19	The database platform must provide flashback mechanism to recover rows, tables when accidentally deleted due to human errors	
Performance Characteristics		
20	Database should have public TPC-C and TPC-H benchmarks and should have leadership position in such benchmarks. Open Source	

S. No.	Specification	Compliance (Y/N)
	Database needs to have OSDB latest benchmark, compatible to TPC-C and TPC-H benchmarks.	
21	Database should be built-in capability to execute large complex queries with parallelism and database performance should not degrade with increase in data volume.	
22	Database should have the ability to handle deadlock situations, without any application slowing.	
23	Database should have the capability of partitioning of tables and indexes within database servers	
Security Characteristics		
24	The database should support role based access control, user based privileges.	
25	Should support password management mechanism with expirable passwords and password management.	
26	Should support the option to encrypt data before transferring over a network.	
27	Should support the option to encrypt the data stored in the database without changing application code.	
28	Should support Built-in encryption key lifecycle management, with assisted key rotation	
29	Should support Industry-standard algorithms including AES (128, 192, and 256 bit keys)	
30	~~Encryption technology should not cause performance degradation by using Hardware acceleration from Intel® AES-NI and SPARC T-Series~~ CHANGED IN CORRIGENDUM Encryption technology should not cause performance degradation by using Hardware acceleration from Intel® AES-NI OR SPARC T-Series	
31	Restrict Database Administrator and other highly privileged users to access application data stored in the database.	
32	Super users should not be able to select, insert, update or delete from the sensitive tables in the database.	
33	Restrict DBA access to the database through back-end even for	

S. No.	Specification	Compliance (Y/N)
	certain administrative activity.	
34	Flexible and adaptable controls over who, when, where and how applications, databases and data can be accessed.	
35	Database should have the capability to accurately detect and block unauthorized database activity including SQL injection attacks by monitoring traffic to any kind of databases	
Self-Managing Characteristics		
36	There should be single-vendor accountability for database and its management	
37	Database should have fault tolerance, parallel processing, linear scalability, mixed workload capability, recovery, real-time capability, manageability, Advice to Tune the Query, Query estimation time features.	
38	Should provide Single system management view for all the targets including database, database cluster, host, Application server etc. It should also provide plug-ins to manage 3rd party applications. Should be using client independent, centralized database management console over network for monitoring hardware, operating system and database resources.	
39	Should perform automatic performance diagnostics	
40	Should automatically maintained workload history facilitating historical performance analysis	
41	Should provide comprehensive system monitoring and event notification to deliver better quality of service.	
42	Should have the ability to perform real time performance analysis	
43	Should have ability to proactively detect and identify the root cause of performance issues	
44	Should have the capability to provide automatic SQL Tuning	
45	Database solution should provide complete integrated Database Life-cycle management including secure testing, provisioning, patch automation, configuration management, change management and best practices advisory.	
46	Warranty/Technical support on Database for 5 Years.	

32.4 Technical Fact Sheet of SLA & HELPDESK Management Software

All below mandatory requirements need to be provided by the System Integrator as part of the solution. Noncompliance to any mandatory requirement shall not be considered and the bid shall be declared as Non-responsive. Non-responsive bids shall not be considered for further evaluation.

S. No.	Specifications	Compliance (Yes/ No)	Reference/ Remark
1.	All the proposed NMS & Helpdesk solution should be from a single vendor.		
2.	Solution shall be open, distributed, scalable, and multi-platform and open to third party integration.		
3.	Solution shall support Web Interface.		
4.	The Solution shall provide future scalability of the whole system without major architectural changes.		
5.	The proposed solution shall be at High Availability Mode in respect to both Software & Hardware (Servers).		
6.	The proposed solution should attached with a Storage to avoid real-time data loss		
7.	Bidder should implement the entire solution in a virtualized environment like Hyper V, VMware etc. If any component of the solution specifically requires physical environment, then bidder must submit a letter from OEM that the mentioned item /items cannot be installed in a virtual environment.		
8.	The proposed EMS/ NMS solution should support and be installable on industry standard RDBMS including Open Source RDBMS only (i.e. Oracle/ MS-SQL/ DB2, etc.,) and licenses of RDBMS should be part of the proposed EMS/ NMS solution.		
9.	The bidder must provide Software licenses of all proposed NMS software for the following deployments/ environments. For production system. For a use on a hot stand by system.		
10.	Proposed visualization/ dashboard tool should employ a series of intuitive icons to access non-core customization, administration, and user management tasks, thereby providing more area for displaying user content.		

S. No.	Specifications	Compliance (Yes/ No)	Reference/ Remark
11.	Proposed EMS solution should provide native capability to deliver Business Intelligence (BI) reports; using an in-built industry-standard BI reporting tool.		
12.	Reporting tool should provide the ability to send reports via email. It should provide the output in HTML, PDF, Excel or CSV formats.		
13.	Reporting tool should provide active reports - Reports can have offline interactivity; more usable and engaging Interact with reports without the need for server requests. This means reports should be emailed with interactive features like clickable charts, sorting, radio button, tabs, cascading lists, checkbox filtering etc.		
14.	Reporting tool/ solution should provide a report canvas where you can drag and drop objects from other existing reports. A report workspace can be viewed as a report dashboard where the end user is designing the content without the assistance of an expert report author.		
15.	Reporting tool/ solution should provide the ability to schedule content to be delivered to user devices, sync via email or directly to the server		
16.	Reporting tool/ solution should provide the ability to easily modify format and layout, Resize widgets with a drag and Filter data with a few clicks.		
17.	The solution should allow for continuous discovery to be run on a continuous basis which tracks dynamic changes near real-time; in order to keep the topology always up to date. This discovery should run at a low overhead, incrementally discovering devices and interfaces.		
18.	The NMS must allow immediately determining the impact of a component failure and thus helping in prioritizing problem-solving efforts.		
19.	The NMS should provide very powerful event correlation engine and thus must filter, correlate & process, the events that are created daily from network devices. It should assist in root cause determination and help-prevent flooding of non-relevant console messages		
20.	Polling intervals should be configurable on a need basis through a GUI tool, to ensure that key systems are		

S. No.	Specifications	Compliance (Yes/ No)	Reference/ Remark
	monitored as frequently as necessary.		
21.	The topology of the entire Network should be available in a single map along with a Network state poller with aggressive/customizable polling intervals		
22.	The NMS application should provide a Unified Fault, Availability and Performance function from a single station only to reduce network and device loads with unified fault & performance polling.		
23.	The NMS performance system must provide out-of-the-box and highly customizable reporting across the network domain.		
24.	The Network performance operator console should provide operators with seamless transitions from fault data to performance reports and back. For example - select a node in NMS fault management system and cross launch it for historical and near real time data.		
25.	Should have MIB browsing, MIB loading, and MIB expression collection features.		
26.	NMS should be cloud ready, should have dynamic Root Cause Analysis capability		
27.	NMS should have Global Management capability, where in it can work in distributed environment.		
28.	NMS should support application based failover over the WAN.		
29.	NMS should have support for SNMPv3 & IPv6, including dual-stack IPv4 & IPv6 to provide flexibility in protocol strategy and implementation.		
30.	It should be able to correlate multiple occurrences of a specific fault on a device within a specified time frame to enable detection of chronic problems. At any given point in time there may not exist a fault for a chronic issue, but we need to know that the condition continues to happen. For example: Circuit down 20 times in last 24 hour, bandwidth thresholds exceeded 30 times in last month, etc.		
31.	The system should support a variety of discovery protocols. The system should take advantage of available		

S. No.	Specifications	Compliance (Yes/ No)	Reference/ Remark
	information to aid in discovery of the network. Protocols should include ARP, DNS, SNMP, BGP, EIGRP, OSPF, CDP (Cisco), EDP (Extreme), NDP (SONMP-Nortel), FDP (Foundry), EnDP (Enterasys), and LLDP (link-level discovery protocol).		
32.	Support for discovering and monitoring router redundancy groups using HSRP (Hot Standby Router Protocol) & VRRP (Virtual Router Redundancy Protocol) & recognizing situations that can result in multi-path conditions.		
33.	Should establish the status of network devices and interfaces with unified status calculation and visualization of network fault & performance data.		
34.	Should enable efficient workflows using contextual navigation between reports and rich interactive report configuration capabilities		
35.	Network Performance reporting tool must provide the following capabilities:		
36.	Data collection and thresholding of network device ports (any that support MIB2 including virtual interfaces):		
37.	Bytes In, Bytes Out, Discards, Errors, Network Delay		
	i. Data collection and thresholding of network devices: CPU, Memory, Buffers, Component statistics		
	ii. A variety of reports summarizing the data including: Home page summary, Calendar, Heat chart, Headline, Dashboard, Managed inventory report, Top ten, most changed, Data explorer		
38.	Should honour network fault management tools' secure grouping and multi-tenancy settings - Secure reports by group, Secure reports by tenant		
39.	Should support following single server scalability		
40.	Single station scalability up to 2,50,000 performance polled interfaces		
41.	Store as-polled data for up to 26 months		
42.	Should be able to schedule key reports for automated delivery		

S. No.	Specifications	Compliance (Yes/ No)	Reference/ Remark
43.	Distribute reports by email in HTML, Excel or pdf formats.		
44.	Network Configuration Management should provide policy monitoring with processes that include: ● Network discovery: Locating and identifying not only hardware components and firmware details, but also device configurations and topological relationships. Accurate network diagrams are a requirement for regulatory standards such as PCI DSS. ● Vulnerability and configuration assessment: Assessing each network device for compliance with policies that apply to groups of devices that perform a particular role. Compliance should be quantified and monitored for trends. ● Remediation and hardening: Enabling policies that can begin with out-of-the-box, generic standards that later are extended to meet the unique requirements of each network, depending on its topology, network technologies and management strategy. ● Change auditing: Detecting noncompliance, issuing alerts and proposing remedial action. In a misconfiguration, rollback should be automated. The ability to compare configurations is invaluable; system changes must be logged. ● Problem prevention: Providing functionality in a standard way with templated and parameterized command scripts. To automate data gathering, analysis and reporting for configurations, change, and event and network management should be integrated. ● Auditing: Recording every access to a device including not only scripted and automated access, but a full keystroke log. Who made what change, the reason for the change and associated ticket number must be captured. Out-of-band changes must be detected. ● Authentication, access control and entitlement management: Controlling with fine granularity the ability to view or edit device configurations, view reports, create command templates or edit and apply policies. All actions must be trackable by user.		
45.	The network change & configuration management key		

S. No.	Specifications	Compliance (Yes/ No)	Reference/ Remark
	features should include the following: - Enables accurate and rapid configuration changes - Full Device Configuration Backup with Versioning and Filtering - Full Configuration Search & Enable configuration comparisons across versions & devices to provide any Version to Version Diffs - Provide real-time and accurate validation of configuration changes including out of band detection and management of changes. - Offer direct command-line access to the device that is logged and auditable. Also permission setup should be possible, for example who can execute this function and which part of the network they can access. - Enforce change control process based on role and user access including comprehensive change management capabilities with multi-level approvals - Provide ability to define and reuse common configuration tasks (templates) - Provide out-of-the-box and customizable reports - Provide back-up and restore (with maintenance) of device configurations. - Maintain complete historical audit trail of all network changes to detect who did do what and when. - Allow easy integration with 3rd party applications - Protect end user for configuration errors (for errors like syntax, boundary and command order errors) and now parent and child relation within a device configuration.		
46.	In real time, detect configuration and asset information changes made across a multi-vendor device network, regardless of how each change is made and also support configuration deployment/rollback and configuration templates		
47.	Manage dual-stack and pure IPv6 environments. Manage SNMPv3 configurations and communicate over SNMPv3.		
48.	In real time, store a complete audit trail of configuration changes, (hardware, and software,) made to network devices, including critical change information.		
49.	Configure granular, customizable user roles to control permissions on device views, device actions, and system actions. Support common authentication systems, such as TACACS+, Radius, SecureID, Active Directory and LDAP.		
50.	Manage device access and authorization through a centralized control model that is integrated with your		

S. No.	Specifications	Compliance (Yes/ No)	Reference/ Remark
	standard workflow and approval processes.		
51.	Automate routine configuration tasks for updates, such as password or community string changes. Reduce the time needed to build automation scripts and increase accuracy with auto-generated scripts derived from device sessions.		
52.	Deploy and monitor operating system images from a centralized network management system.		
53.	Enforce change processes in real time. Model complex approval processes with flexible rules. Force approvals for changes, including changes made by a direct command line interface (CLI) session.		
54.	Implement high-availability and disaster-recovery solutions with Multimaster and Satellite deployments. Administrators can effectively manage geographically dispersed networks without a single point of failure.		
55.	The system must support heavily NAT environment and environments where network devices may have the same IP address.		
56.	Should offer service driven operations management of the IT environment to manage distributed, heterogeneous systems - Windows, UNIX & LINUX from a single management station.		
57.	The system must be agent based for managing the nodes and have the ability of storing events / data locally if communication to the management server is not possible due to some problem. This capability will help to avoid losing critical events. There should be a single agent on the managed node that provides the system performance data, and for event management it should be able to prioritize events, do correlation & duplicate suppression ability to buffer alarms and provide automatic actions with capability to add necessary annotations.		
58.	The System should have automated service discovery, policy deployment and actions to enable busy IT personnel to focus on more strategic initiatives and manage business-critical application services from the end-user perspective, and to be immediately aware of the business impact of lower level component failures or performance degradations.		

S. No.	Specifications	Compliance (Yes/ No)	Reference/ Remark
59.	Alarms with meaningful message text, instruction text, operator / automatic actions / linked graphs, duplicate message suppression. Should be configurable to suppress events at the agent or managed node level itself and be configurable to suppress events for key systems/devices that are down for routine maintenance or planned outage.		
60.	Agents on the managed node should be autonomous and can undertake automated corrective actions in isolation from the Management server. This provides management by exception for only forwarding actionable events to the Management server.		
61.	The system should integrate with Helpdesk / Service desk tool for automated incident logging and also notify alerts or events via e-mail.		
62.	Application should be able to export any graph or matrix presentation of data to XLS, CSV formatted files.		
63.	Application should provide a wizard or other GUI to facilitate the creation of customized graph templates. It should provide a list of metrics available for a given system type and allow for multiple metric selection. This template can then be used to create a graph for any system with the same attributes.		
64.	Should proactively identify database problems before they affect end-users and ensure high availability of mission critical databases.		
65.	Should monitor key operational activities and events to provide always-on availability.		
66.	– Alert log messages such as data block corruptions, queue resources exceeded, internal errors, and I/O read/write failures		
67.	Performance thresholds and graphs in following areas should be gathered and reported for the databases:		
68.	– Space management such as table space and free space		
69.	– Workload metrics such as CPU utilization, transaction throughput		
70.	– SQL related performance indicators such as percent sorts in memory, disk-sort rate		

S. No.	Specifications	Compliance (Yes/ No)	Reference/ Remark
71.	The solution should support mobility devices (ex. iPhone) to allow for role based views that can be accessed while away from the office. Ex. Line of business managers can track and analyse transactions while travelling and engineers can receive alerts and status information while traveling, enabling them to handle issues promptly without returning to their desks.		
72.	Ability to launch in-context to performance graphs or reports.		
73.	Ability to automatically calculate the threshold values based on the available historical performance data for previous days. This eliminates the need to set threshold values manually for each policy to suit a different environment.		
74.	The adaptive threshold capability automatically calculates a baseline from the historic samples to identify previous trends in performance. Based on these trends the threshold values are automatically and dynamically calculated. Once the automatic threshold values are set, comparing the current performance data with the adaptive thresholds indicates if the current infrastructure resource utilization is normal or not. An alert is generated when abnormal behaviour is detected.		
75.	Collection of performance data should average no more than 3%-5% system overhead		
76.	Ability to collect metrics per process to facilitate troubleshooting of system resource overhead on a process basis.		
77.	When many a combination of many events occurs in the monitored environment, the system must be able to automatically categorize them into causes and symptoms. The system needs to provide a single interface to view multiple layers of cause and symptoms.		
78.	The system should provide automatic chaining of Correlation Rules, meaning if I have a rule relating a database problem to a filesystem problem, and another rule that relates a filesystem problem to a storage problem, the system should be to link these rules together and link the database problem to the storage problem		

S. No.	Specifications	Compliance (Yes/ No)	Reference/ Remark
	during execution time		
79.	The system must allow modification and enhancement events during event processing. An event processing interface must be provided to enable event processing scripts to be integrated into the event processing pipeline and allow operations to enrich events programmatically. For e.g., to provide additional information by querying asset databases during event processing time and adding additional hints from the query to facilitate event correlation.		
80.	Server reporting tool should be able to collect and collate specific information regarding the relationships between the IT elements and the business services.		
81.	Tool should be able to report in the context of the business services that the infrastructure elements support—clearly showing how the infrastructure impacts business service levels		
82.	Tool should provide development environment where more Content/Reports can be created and data sources such as — Generic .csv files, and, Databases supporting JDBC. Should also be included to pull data and create reports from such data.		
83.	Tool should allow to configure downtime for Configuration Items and view the configured downtime in the reports.		
84.	The proposed helpdesk solution must support all 12 ITIL (IT Infrastructure Library)v3 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 12 process."		
85.	The proposed Helpdesk tool should be Axelos Gold level certified or PINK certified on at least 11 ITIL 2011 processes on all the 15 ITIL processes that are the most mature way to demonstrate that at least three IT organizations : Incident management, Problem Management, Change Management, Knowledge Management, Service Level Management, Service Asset and Configuration management, Service Catalogue and Request Fulfilment, etc.		

S. No.	Specifications	Compliance (Yes/ No)	Reference/ Remark
86.	DDA should be able to control access rights to modules and information by user profiles.		
87.	Should provide out-of-the-box categorization, as well as routing and escalation workflows that can be triggered based on criteria such as SLA, impact, urgency, Asset, location or customer.		
88.	Must be able to relate and link problems to specific incidents. Multiple incidents be linked to a single problem.		
89.	Service desk software licenses should be offered as single license which should provide us the capability to use it as helpdesk/ service desk as well as IT assets lifecycle management tool. It should natively provide both functionality i.e. the tool should offer unified service desk and IT Asset Lifecycle Management capability.		
90.	The Change Management module should provide a rule-based workflow system for controlling changes throughout their lifecycle: from initial request to approval, to planning and implementation, and to monitoring and evaluation.		
91.	Proposed service desk tool should provide an easy drag-and-drop visual workflow designer and configuration tooling, where no programming/ coding is required to define the process management workflows.		
92.	Proposed service desk tool should provide the capability of versioning for workflows. The service desk tool should facilitate us such that we should incrementally grow our workflows keeping the revisions of workflows as our business process changes and become more mature. If a new version of a workflow breaks, it should allow us to revert to a previous working version of workflow.		
93.	Should include automated impact analysis, calculated risk analysis, collision detection, and unplanned change detection and validation.		
94.	The Change Management module should provide the capability for Release Control Analysis inbuilt providing the stakeholders with automated decision-support to help make more informed assessment and approval decisions during the review process. It should also be able to provide the implementation team with real-time visibility		

S. No.	Specifications	Compliance (Yes/ No)	Reference/ Remark
	into all in-flight change activity to reduce downtime risks and increase communication between different teams during execution.		
95.	Should support closed loop incident process to more quickly and accurately discover incidents and execute triage and remediation.		
96.	Proposed solution should provide built-in chat facility that can be used to log tickets. Proposed service desk should provide the ability such that chat sessions should be recorded and stored in the ticket's Communication Log.		
97.	Ad-hoc reporting as part of proposed service desk solution should provide advanced ad hoc reporting capability that should not only enable our power users to develop more complex reports but also provides usability and performance features.		
98.	Ad-hoc reporting as part of proposed service desk solution should allow administrators to grant a subset of users the ability to create calculations as columns in a report. It should provide signature option access using which calculations can be created via standard mathematical operators & SQL syntax that is enabled by using an expression library. It should also provide the ability to validate the expression before it is added to the report and for our administrator to customize the expression library.		
99.	Ad-hoc reporting as part of service desk solution should provide a summary tab in the Ad Hoc dialog box, so that users can add summaries for selected attributes to the report. Based on the style of report that is selected, it should provide the facility so that the summaries can be displayed at the header or the group level. The summaries should provide high level overviews including counts, averages, minimum values, and maximum values.		
100.	Ad-hoc reporting as part of service desk solution should provide the ability of field selection and report development. It should provide the facility using which one can quickly enter data by using the Select buttons and hyperlinks for attributes.		
101.	Ad-hoc reporting as part of service desk solution should provide the ability of configuring improved performance		

S. No.	Specifications	Compliance (Yes/ No)	Reference/ Remark
	limits for our individual security groups. Using these limits one can restrict the number of records that users access when they develop a report during the preview stage of report development.		
102.	Must allow users to create sophisticated or detailed maintenance tasks. Must include a cost estimation tool that enables users to select a subset of maintenance tasks, and then calculate the estimated cost to run those tasks within a specified time frame.		
103.	If multiple SLAs are triggered, the strictest one must drive the workflow. The product must monitor SLAs against Service, Problem, and Change Management		
104.	The solution should show immediate (real-time) status of tickets.		
105.	Should support KCS (Knowledge Centred Support) best practices. Should provide out-of-the-box change category to manage KCS workflow.		
106.	Provide out of box and customizable reporting and personalized dashboard.		
107.	In order to reduce the incidents in the environment, the solution should be capable enough to provide suggestion articles of different related solution by identifying the user's keywords and by searching the same in knowledge base database before the end user logs any incident.		
108.	Vendor warranty/Technical support for 5 Years.		

32.5 Global Load balancer

S. No.	Specifications	Compliance (Yes/No)
1.	Should be high performance purpose built multi-tenant hardware with multicore CPU support.	
2.	Single hardware should support multiple instances including link load balancing, application load balancing & SSL VPN functions from same OEM with dedicated hardware resources for each virtual instance.	
3.	The appliance should have minimum 24 Gbps of system throughput from day one and must have option to scale up.	

	The appliance should have minimum 4 x10G SFP+ interfaces from day one Hardware based SSL acceleration with 18,750 SSL TPS 2K Keys from day one and must have option to scale up on the same hardware.	
4.	Platform should support minimum 6 virtual instances and must have option to scale upto 8 virtual instance on same appliance. Each instance must have assigned dedicated hardware resource such as CPU, memory, SSL & I/O for guarantee performance.	
5.	Appliance should provide full ipv6 support and OEM should be IPv6 gold-certified. OEM should be listed vendor for ipv6ready.org phase-2 certification only.	
6.	The appliance should have feature of GSLB for future requirement.	
7.	Script based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS. Load balancer should support Policies to customize new features in addition to existing feature/functions of load balancer.	

32.6 Network Access Switch

S. No.	Specifications	Compliance (Yes/ No)
1.	Networking L3 switch, 48x 1GbE + 2x 10GbE SFP+ Fixed Ports, Stacking, IO to PSU airflow, AC Stacking Cable, for Networking switches, 1m Installation and Layer-3 implementation 5Yr ProSupport: Next Business Day Service Lifetime Limited Standard Technical Support.	

32.7 Security gateway (Next Generation External Firewall)

S. No.	Specification	Compliance (Y/N)
1.	The application aware next generation security gateway with threat prevention must be appliance based and 19” Rack mountable solution.	
2.	Security gateway solution must provide application identification with integrated threat prevention modules including IPS, gateway antivirus/anti-malware, antibot& antispyware enabled from day one	
3.	4 x GE, upgradable to 8 GE	
4.	Console Port 1 number	
5.	Minimum RAM 1 GB, Upgradeable to 2 GB RAM	
6.	Should be having minimum 100 Gb local storage to store log	

S. No.	Specification	Compliance (Y/N)
	files/software images	
7.	Encrypted throughput: minimum 500 mbps	
8.	Threat prevention throughput should be 1 Gbps with all modules (IPS, gateway antivirus/anti-malware, anti-spyware &antibot) enabled from day one	
9.	Concurrent connections: up to 250,000	
10.	Simultaneous VPN tunnels: 1000	
11.	Static Routes	
12.	RIPv1, RIPv2	
13.	OSPF	
14.	TCP/IP, PPTP	
15.	RTP, L2TP/IPSEC	
16.	IPSec, GRE, DES/3DES/AES	
17.	PPPoE, EAP-TLS, RTP	
18.	FTP, HTTP, HTTPS	
19.	SNMP, SMTP	
20.	DHCP, DNS	
21.	Support for IPv6	
22.	802.1Q, NAT, PAT, IP Multicast support, Remote Access VPN, Time based Access control lists, support VLAN, Layer 2 Firewall, Virtual Firewall, Radius/ TACACS	
23.	QoS features like traffic prioritization, differentiated services, committed access rate. Should support for QoS features for defining the QoS policies.	
24.	Console, Telnet, SSHv2, Browser based configuration	
25.	SNMPv1, SNMPv2	
26.	The Firewall should be ICSA Labs certified for Enterprise Firewall or EAL 4 certified	
27.	It should be possible to operate the firewall in various modes like TAP mode, vWire mode, “bridge mode” and "transparent mode” apart from the standard NAT mode	
28.	Should have integrated Network Intrusion Prevention System (NIPS) and IPS must able to inspect for application vulnerabilities within identified applications Must have “Zero-day” protection against DoS/DDoS and worm attacks based on traffic behavior. Also it should mitigate Zero day http floods and brute force attack & vulnerability scanning attempts based on traffic behavior analysis	
29.	The IPS proposed solution shall support network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic	
30.	The IPS proposed solution shall have multiple mechanisms for classifying applications including application signature, SSL&SSH, protocol decoders and heuristics to handle unknown applications	
31.	Should perform Traffic Shaping of popular P2P applications like KaZaa, Gnutella, BitTorrent, WinNY, eDonkeyetc	

S. No.	Specification	Compliance (Y/N)
32.	Should support Gateway Data Loss Prevention (DLP)/ data filtering policies feature for popular protocols like HTTP, HTTPS, FTP, POP3, IMAP, SMTP, POP3S, IMAPS, SMTPS	
33.	The proposed solution must allow policy creation for application identification, user identification, threat prevention and content filtering in a single location: -Application Detection (at least 1750 apps), -Vulnerability Protection (Client and server side protection) -Gateway Virus Protection, -Gateway Spyware Protection -Content Filtering, -QoS (marking and/or traffic shaping)	

32.8 Internal Firewall

S. No.	Specifications	Compliance (Yes/ No)
1.	The next generation application aware Firewall must be appliance based and 19" Rack mountable.	
2.	The proposed solution will be a Next Generation Firewall with a capability of supporting at least 2Gbps of Application Identification.	
3.	Enabled Firewall throughput using 64 byte HTTP packet.	
4.	The proposed solution shall support network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactic	
5.	4 x GE, upgradable to 8 GE	
6.	Console Port 1 number and dedicated out of band management port	
7.	Minimum RAM 1 GB, Upgradeable to 2 GB RAM	
8.	Should be having sufficient local storage for the project duration to store log files	
9.	The Firewall should be ICSA Labs certified for Enterprise Firewall or EAL 4 certified	
10.	Concurrent connections: up to 250,000	
11.	It should be possible to operate the firewall in TAP mode, wire mode ,"transparent mode" apart from the standard NAT mode	
12.	Static Routes	
13.	RIPv1, RIPv2	
14.	OSPF	
15.	TCP/IP, PPTP	
16.	RTP, L2TP	
17.	IPSec, GRE, DES/3DES/AES	
18.	PPPoE, EAP-TLS, RTP	
19.	FTP, HTTP, HTTPS	
20.	SNMP, SMTP	
21.	DHCP, DNS	

S. No.	Specifications	Compliance (Yes/ No)
22.	Support for IPv6	
23.	802.1Q, NAT, PAT, IP Multicast support, Remote Access VPN, URL support VLAN, Layer 2 Filtering, Time based Access control lists, Firewall, Virtual Firewall, Radius/ TACACS	
24.	QoS features like traffic prioritization, differentiated services, committed access rate. Should support for QoS features for defining the QoS policies. Vide Pre-Bid Query No. 45: "These functionalities are usually performed by a router or a switch and hence request removal from firewall". **Our response: Agreed**: but there should not be any degradation in performance.	
25.	Console, Telnet, SSHv2, Browser based configuration	
26.	SNMPv1, SNMPv2	
27.	*The proposed solution shall support authentication services for user-identification: Active directory, LDAP, eDirectory, Lotus, exchange, API for custom integration to get the user information. The proposed solution shall be able to identify, decrypt and evaluate SSL & SSH traffic in an inbound and outbound connections Support for application heuristics to handle encrypted applications*	

32.9 WAN Optimization Solution

S. No.	Specifications	Compliance (Yes/ No)
1.	The solution should support optimization of WAN traffic from high user base office locations to the central datacenter location & should provide Network traffic optimization between the Datacenter & DR	
2.	It should be appliance based solution with purpose built hardware for high performance.	
3.	Datacenter device should support minimum 40 Mbps of optimized bandwidth scalable to 100 mbps	
4.	Minimum memory support 16 GB and scalable to 32 GB	
5.	The solution should support minimum storage for 3500 active users for caching purposes	
6.	Network Interface: 4 *10/100/1000 ports and 2 numbers of Inline Gigabit Ports	
7.	The solution should support TCP optimization for efficient data transfer across WAN, higher bandwidth utilization, faster recovery after any packet loss. TCP optimization, Slow start with congestion avoidance, Fast Convergence & Selective acknowledgements to ensure efficient throughput	

S. No.	Specifications	Compliance (Yes/ No)
8.	The solution should support standard compression mechanism and stream based differencing to avoid transmission of content that has been previously received in the local data store.	
9.	The solution should be able to support & recognize repetitive byte patterns, and be able to replace the repetitive data with reference records and other metadata.	
10.	The solution should avoid the transmission of repeated content across the WAN and to ensure efficient utilization WAN bandwidth	
11.	The solution should able to distinguish protocol used to transfer the contents for efficient disk utilization and better performance.	
12.	Proposed Solution should provide Layer 7 application intelligence to improve the performance of protocols like HTTP or iSCSI when they are used over a WAN. Should support real time payload identification for deduplication.	
13.	Proposed Solution must support HTTP acceleration to improve the HTTP performance	
14.	Should support caching which helps speed up the rendering of Web pages by eliminating repetitive trips over the WAN connection to validate the freshness of content	
15.	The solution should natively address protocol chattiness issues for the MAPI protocol used by emailing solution clients using application specific blueprints	
16.	The WAN optimization solution must address protocol chattiness issues for the CIFS protocol	
17.	The solution should be able to define classes of application traffic and apply Quality-of-Service policies to each class	
18.	The solution should support traffic shaping and provision to allocate Guaranteed Bandwidth to each class of applications	
19.	Proposed solution should integrate with application load balancer for application optimization. For better Integration & management Wan optimization and server load balancer preferably be from same OEM.	
20.	Proposed Should support remote notification capabilities, including SNMP v2c, v3, SMTP notification, and syslog notifications.	
21.	5 Years warranty/Technical support on devices.	

32.10Tape Library

S. No.	Specifications	Compliance (Yes/ No)
1.	Latest Backup Tape Library devices LTO-7 for backing up NAS backup with Backup application to backup 120 TB of DATA with 5 Years warranty/Technical support.	

32.11Internet & MPLS Router

Sr No	Minimum Required Specifications	Compliance (Yes/ No)
1	The router should support IP routing, voice telephony, IP multicast, QoS, IP mobility, multiprotocol label switching (MPLS), VPNs	
2	Router should have minimum 8 GB of DRAM/RAM and 8GB Flash.	
3	The proposed router should have following port configuration:	
	a. Should have 3 x GE WAN/LAN ports from Day 1	
	b. Should shave 8 x 10/100/1000 ports to be added as and when required	
	c. Should support 8 x E1 ports to be added as and when required	
4	Routers should have at least 2 free slots for future upgradation for LAN or WAN interface.	
5	Router shall have aggregate throughput minimum 100 Mbps from Day-1 and should be scalable to 300Mbps.	
6	Routers should support large selective of modular LAN and WAN connectivity options including Gigabit Ethernet, T1/E1, , V.35 Serial , 4G LTE interface modules.	
9	IPv4 and IPv6 enabled from day one	
10	HSRP/VRRP, Static Routes, RIPv1, RIPv2, RIPng, OSPFv2, OSPFv3, route reflector, BFD, Policy based routing IGMP V1/V2/V3, PIM-DM, PIM-SM, Ipv4 and Ipv6 tunneling, Routing over IPSec Tunnels enabled from day one	
11	Should support extensive support for SLA monitoring for metrics like delay, latency, jitter, packet loss	
12	Support for accounting of traffic flows for Network planning and Security purposes	
13	Pre-planned scheduled Reboot Facility	
14	Real Time Performance Monitor – service-level agreement verification probes/alerts	
25	Router must support IPv6 Neighbor Discovery V6 , DHCP V6, Route Advertisement V6	
16	The router should have a facility of visibility and control of the application.	
17	WAN optimisation feature. The solution support 750TCP connection and bandwidth of 15mbps..If the feature is not inbuilt, separate hardware for the same should be provisioned when required	
18	The router should support MPLS routing and security features (state full firewall ,IPSEC)at the same time	
19	Router should be scalable to 1000 IPSec tunnels, atleast 100000 routes (BGP) and Min 1K multicast routes.	
20	The proposed solution in WAN should support the basic payload encryption for traffic from any office to any other office location on demand.	
21	The Router shall support Deep inspection mechanism recognizing and classifying applications by inspecting packets	
22	The Router should be NDPP or EAL3 certified at the time of Bidding	
	The router should be IPv6 phase 2 certified by IPv6 ready forum.	
23	The router should have a facility of visibility and control of the application. Also the router should be able to categorize between mission critical and non-mission critical applications, with 1000 application visibility.	
34	The OEM should be leader in quadrant of Gartner report for wired & wireless infrastructure	

32.12Core Router

Item	Minimum Specifications	Compliance (Yes/ No)

General	Core router shall be chassis based with modular architecture for scalability with Redundant - Route Processor, Power supply, and shall deliver multiple IP services over a flexible combination of interfaces.	
	The router shall facilitate all applications like voice, video and data to run over a converged IP infrastructure along with hardware assisted IPSEC & Network Address Translation (NAT), capability. The router should also support hitless interface protection, In-band and out-band management, Software rollback feature, Graceful Restart, nonstop routing for OSPF, LDP, etc.	
	The platform shall have modular software that will run service & features as processes having full isolation from each other	
	Router shall have event and system history logging capabilities. Router shall generate system alarms on events and capable of log analysis	
	Router should have power supply redundancy. There should not be any impact on the router performance in case one of the power supplies fails.	
Ports	As per overall network architecture proposed by the bidder, the router should be populated with 6 x 1 GE port with required transceivers as per solution & one 10 gig interface.	
Interface modules	Should support minimum 1G/10G interfaces	
	Must have capability to interface with variety interfaces	
Protocol Support	The router shall have RIPv1, RIPv2, RIPng, BGP, OSPFv2 & v3, Policy Based Routing for both IPv4 & IPv6, IP Multicast Routing Protocols to facilitate applications such as streaming, webcast, command & control including PIM SM, PIM SSM, GRE (Generic Routing Encapsulation)	
	Tunneling with 1000 tunnels enabled from day one.	
	Router should support following MPLS features – LDP, Layer 2 VPN such as EoMPLSor equivalentwith LDP signaling, Route Reflector (RR), Traffic Engineering with RSVP-TE, Fast Reroute Link Node & Path protection enabled from day one. Support for these features can be considered optional for Internet routers	
Manageability	The router must support management through SNMPv1/v2/v3, support RADIUS and TACACS. The router must role based access to the system for configuration and monitoring &stateful packet inspection to recognize a wide variety of applications The router shall be provided with IETF standards based feature so that granular traffic analysis can be performed for advanced auditing, usage analysis, capacity planning or generating security telemetry events, also the router shall have SLA monitoring tools to measure state of the network in real time. The SLA operations shall provide information on TCP/UDP delay, jitter, application response time, Packet Loss etc	
Scalable	The router should be scalable. For each slot multiple modules should be available.	
	The chassis offered must have free slots to meet the scalability requirement of expansion of the project in the future.	

Traffic control/QoS	The router shall perform traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, DSCP and by some well-known application types through Application Recognition techniques.	
	The router shall support QoS policy in the router shall support dual Strict Priority Queue or Low Latency Queue per policy so that voice and video traffic can be put in different queue. It also should have hierarchical QOS (Inbound and Outbound) to ensure bandwidth allocation for all type of traffic during congestion and non-congestion scenario.	
Bandwidth & Performance	Backplane Architecture: The back plane architecture of the router must be modular and redundant. The back plane bandwidth must be minimum 20 Gbps from day one with minimum scalability upto 30 Gbps with minimum routing performance of 20 mpps from day one (1) scalable upto 30 mpps, with minimum three (3) open slots.	
	The Router should have individual dedicated control plane processor and data plane processor module. Data plane Processor module should be independent of the control plane Processor. Control plane Processor should have support for internal memory to support multiple software images for backup purposes and future scalability. The router processor architecture must be multi-processor based and should support hardware accelerated, parallelized and programmable IP forwarding and switching.	
Redundancy	Redundancy in terms of Power supply(s). Power supply should be able to support fully loaded chassis	
	All interface modules, power supplies should be hot- swappable	
Security features	The router should have support for hardware enabled Network Address Translation (NAT) and Port Address Translation (PAT) . The router shall support NAT6to4 function. Mention the number of sessions that it can support. The router shall support vrf-aware NAT function.	
	The router shall meet the following requirements for security: Access Control List to filter traffic based on Source & Destination IP Subnet, Source & Destination Port, Protocol Type (IP, UDP, TCP, ICMP etc) and Port Range etc. Router should support stateful packet inspection to recognize a wide variety of applications.	
	The router shall support firewall service in hardware on all interfaces for enhanced security to protect the backbone from malicious activities. The firewall performance shall be at least 5 Gbps (internal/external). In case of external firewall, bidder should propose the firewall with necessary 10G interface and redundant power supply.	

32.13Desktop/Work stations

S. No.	Item	Complete Description	Technically Compliant (Yes / No)
1.	Processor	The desktop should have latest generation (launched in year 2015/2016) Intel® Core™ i7 or AMD Ryzen™ 5, Quad-Core, Multi-Threaded Processor with 2.8 GHz or more Base Clock Frequency, 8 MB Cache or Better) or higher processor launched within last one year.	
2.	Motherboard & Chipset	Suitable chipset for quoted processor based motherboard.	
3.	Video	Professional Graphic controller with 2GB DDR4 2133MHz or higher dedicated graphics memory.	
4.	Network	Integrated Gigabit Ethernet controller	
5.	WiFi & Bluetooth	Integrated WiFi & Bluetooth enabled 5 Ports 3xUSB 2.0 or higher ports, One RJ45 Ethernet port, Headphone & mic out	
6.	HDD Controller	Integrated dual port SATA-III (6Gbps or higher) controller	
7.	Sound Controller	Integrated sound controller	
8.	Memory	8GB DDR3 1600MHz or higher expandable up to 32GB	
9.	Storage	2TB SATA 6Gbps or higher HDD 7200 RPM	
10.	Optical Drive	DVD WRITER	
11.	Keyboard & Mouse	Wireless (Keyboard & optical scroll mouse with pad) with heavy duty batteries	
12.	Monitor	21.5" or higher TFT display supporting a resolution1920 x 1080 and with inbuilt HD webcam (2MP or higher) supporting 30fps, built in stereo speakers of 1.5W each and mic.	
13.	Power Management & DMI	System with Power management features & Desktop Management Interface implementation	
14.	OS Support & Certification	OS Support & Certification Latest Version of Windows and Linux	
15.	Accessories	System user manual and all other necessary accessories	
16.	UPS	UPS 600 VA	
17.	Operating System	Preloaded with OEM Pack Windows 10 Professional (64 bit) or the latest one, all necessary Plugins/utilities and driver software, bundled in CD/DVD Media	
18.	Office Tools	MS office latest released edition.	
19.	Antivirus	Latest Antivirus	
20.	Compliance	Energy Star 6.0 Compliance.	
21.	Warranty	Five-year on-site comprehensive warranty support.	
22.	Make	Branded	

~~32.13~~32.14 Laptops

S. No.	Specifications	Compliance (Yes/ No)
1.	The Laptop should have latest or 8th generation Intel® Core™ i7 upto 4Ghz clock frequency, Quad Core, 8MB cache ORAMDRyzen Processor with Minimum 1.90GHz Base Frequency, 6MB Cache or Higher processor launched within last one year. Minimum 8GB RAM (1*8GB), 1TB~~,~~ 7200 RPM HDD, 14" LED HD Display (1920X1080) with Anti-Glare, 1VGA Port, 1~~/~~HDMI Port, 1 RJ 45, 3 * USB 3.0 Port, Integrated Webcam, Wi-Fi, Bluetooth, 1GB Ethernet Connectivity, Battery with 5Yrs Warranty, Windows 10 Professional (64 bit) or the latest one, MS-office professional~~,~~64bit, Antivirus, Laptop Bag pack, 5Yrs NBD Onsite Warranty, better Make or Brand	

~~32.14~~32.15 Network Multi-Function Printer (Mono) cum Fax

S. No	Feature	Specification	Specifications Offered	Compliance (Yes/No)	Deviations, if any
1.	Make	Must be specified		NA	
2.	Model	All the relevant product brochures and manuals must be submitted.		NA	
3.	Speed (min.)	min 25 PPM			
4.	Memory(min.)	min 64 MB			
5.	Resolution	1200 x 1200 dpi			
6.	Interface	USB, Ethernet (UTP) with respective cables			
7.	Monthly Duty Cycle	Min 18000 pages			
8.	Duplex	Automatic Duplex ADF, Fax, and Network ready			
9.	Drivers	Windows XP, Windows Vista, Windows 7, Windows 8, windows 10 or latest edition, MAC, OS 9.0, MAC OS X or latest edition, Linux, Kernel 2.4 or later			
10	Warranty/Technical support	5 Years			

~~32.15~~32.16 Network Multi-Function Printer (Colour) cum Fax

S. No	Feature	Specification	Specifications Offered	Compliance (Yes/No)	Deviations, if any
1.	Make	Must be specified		NA	
2.	Model	All the relevant product brochures and manuals must be submitted.		NA	
3.	Speed (min.)	min 25 PPM			
4.	Memory(min.)	min 64 MB			
5.	Resolution	1200 x 1200 dpi			
6.	Interface	USB, Ethernet (UTP) with respective cables			
7.	Monthly Duty Cycle	Min 18000 pages			
8.	Duplex	Automatic Duplex ADF, Fax, and Network ready			
9.	Drivers	Windows XP, Windows Vista, Windows 7, Windows 8 MAC, OS 9.0, MAC OS X, Linux, Kernel 2.4 or later			
10	Warranty/Technical support	5 Years			

~~32.16~~32.17 Scanner

S. No	Feature	Specification	Specifications Offered	Compliance (Yes/No)	Deviations, if any
1.	Make	Must be specified		NA	
2.	Model	All the relevant product brochures and manuals must be submitted.		NA	
3.	Scanner type	Legal size flatbed			
4.	Scanner Technology	Charge coupled device			
5.	Scan speed	Min 20 ppm			
6.	ADF Capacity	50 sheets			
7.	Duty cycle	Min 800 pages per day			
8.	Scan resolution	Min 600 dpi			

9.	Output resolution dpi settings	300, 600			
10	Colour bit depth	24 bit			
11	Grey scale level	256			
12	Double feed detection	Yes			
13	File formats	BMP, JPG, TIFF, TIFF (compressed), multi-page TIFF, PNG, PDF, RTF, TXT, UNICODE, HTM, DOC			
14	Connectivity	Hi-Speed USB 2.0			
15	Software	ISIS and Twain drivers			
16	Compatible Operating Systems	Windows XP, Windows Vista, Windows 7, MAC OS 9.0, MAC OS X, Linux Kernel 2.4 or later			
17	Warranty/Technical support	5 Years			

~~32.17~~32.18 Essential Requirement for Smart card based system:

Microprocessor based Smart cards (should be EIL4+ certified)
Personalization: Design with Member's Colour Photograph on front and Instructions in Black and White Text with respective sports complex details on back. Non personalised card with logo on both sides will also be required for use by temporary, casual members or for temporary replacement cards for members.
- Dimension: CR80 Standard Credit Card Size
- Transmission To be suggested by Bidder (can be RFID/Contactless)
- Memory 1024 bytes (Minimum)
- Antenna Embedded
- Operating Frequency 13.56 MHz
- Security level 4 Levels (0, 1, 2 & 3)

~~32.18~~32.19 Specifications for Digital Services Access Points

Services delivery to be made available through Internet Access at Computer at Home, Mobile, Cyber/Internet Cafes, Internet Service Access Centres (ISACs), Common Services Centres (CSCs), Mobile Van Service, NagrikSuvidhaKendras of DDA etc.

~~32.18.1~~32.19.1 NagrikSuvidha Kendra (NSK)

Sl. No.	Set Up of NagrikSuvidha Kendra (NSK)	Unit	Proposed Quantity	Compliance (Yes/No)
1	Desktop Computers with Operating system and MS office Software with UPS 600 VA. (with Warranty and AMC till 5Years) – specification for Desktop given in Section (32.11 above)	Nos.	5	
	LAN Connectivity among Computers	Nos.	1	
2	2 Internet Connections with 2 Mbps (broadband connectivity) shared among 5 Computers, from Two different service providers.	Annually	5	
3	Multifunction Network Printers (mono) with 5 Years support	Nos.	2	
4	Network Scanner high speed with 5 Years support	Nos.	2	
5	24 Port managed switches with 5 Years support	Nos.	1	
6	Internet Router with 5 Years support	Nos.	1	
7	TV Monitor 32 Inches with 5 Years support	Nos.	2	
8	Queue Management System (Token, Display Units)	Nos.	1	
9	Seating desk for persons	Nos.	5	
10	CCTV	Nos.	2	
11	Biometric machines (Authentications for AADHAAR Enabled services)	Nos.	2	
12	Internet Information Kisok Machine	Nos.	1	
13	Support staff (5 Persons) cost annually	Annually	5	
14	Card swiping machines (payment)	Nos.	2	
15	Telephone line with 5 extension numbers	Nos.	1	
	TOTAL			

~~32.18.2~~32.19.2 Mobile Van NagrikSuvidha Kendra

Sl. No	Set Up of Mobile Van NagrikSuvidha Kendra (MNSK)	Unit	Proposed Quantity	Compliance (Yes/No)
1	Mobile VAN 22 seater (example Tempo Traveller)	Nos.	1	
2	Desktop Computers with Operating system and MS office Software with UPS 600 VA. (with Warranty and AMC till 5Years) – Specification for Desktop Computer given Section 32.11 above.	Nos.	5	
3	LAN Connectivity among Computers			

4	2 Internet Connections with 2 Mbps each (broadband connectivity) from two different Service providers (MTNL, etc.) shared among 5 Computers.	Annually	5	
5	Multifunction Network Printers (mono) with 5 Years support	Nos.	2	
6	Network Scanner high speed with 5 Years support	Nos.	2	
7	Wireless Internet Router with 5 Years support	Nos.	1	
8	Monitor 17 Inches with 5 Years support	Nos.	5	
9	Queue Management System (Token, Display Units)	Nos.	1	
10	Seating desk for persons	Nos.	5	
11	CCTV	Nos.	1	
12	Biometric machines (Authentications for AADHAAR Enabled services)	Nos.	2	
13	Support staff cost annually (4 Tech + 1 Driver)	Annually	5	
14	Diesel Generator (Silent) Honda make with appropriate capacity	Nos.	1	
15	Card swiping machines (payment)	Nos.	1	
16	Telephone with Fixed wireless	Nos.	2	

~~32.18.3~~32.19.3 Internet Information Kiosk

Sl. No	**Supply and setup of Kiosk**	**Unit**	**Proposed Quantity**	**Compliance (Yes/No)**
1	Internet Information Kiosk with Ready to Use and complete setup. Should have built in computer with hard disk space, keyboard, touch screen, touch pad or mouse, with internet connectivity provisions. 1. Dimension : ~W-60 * D-50 * H-165 cm (+/- 1 cm) 2. Power Requirement : 110~240V,50 / 60 Hz 3. Working Temperature : -10℃ to 50℃ 4. Storage Temperature : -20℃ to 60℃ 5. Suitable Frame Colour 6. Warranty : One Year 7. AMC: 4 Years	Nos.	1	

Vendor can quote for 3 different models (Model-I, Model-II, Model-III) of ergonomics design, out of which DDA can choose while placing order.

~~32.19~~32.20 Record Room Management

Sl. No	Installation and maintenance of State-of-the-Art Record Room Management	Unit	Proposed Quantity	Compliance (Yes/No)
1.	Record Room Management Software	Nos.	1	
2.	Record Rooms (20X15X10 Feet Approx.) to be equipped with state of art Racking System	Nos.	50	
3.	Non-corrosive Rolling Record Box Storage Racks: Qty. to be estimated by visiting the DDA offices (Record Rooms)	Nos.		
4.	CCTV with associated software and computing supervisory resources at each record room o Fisheye Wide 360 vision: 3D vison with 360 panoramic lens o Mobile Surveillance: Fully function mobile app supporting iOS & Androids. 24*7 live view on your mobile phone. o Multiple views: 5 different type of views on mobile phone, o Motion Detection: Whenever any motion is detected, camera sends alert on user's mobile phone. Micro SD card slot. o Wireless connection with Wi-Fi router. P2P Cloud monitoring: with mobile phone / iPad. o Night Vison: IR night vison with crisp and clear image even in dark. o 1 year warranty: o AMC support for 4Years after Warranty period o 1 Fisheye 360 Smart Camera o 1 Power Adapter o 1 Camera Fixed chassis o 1 User Manual (Minimum Two required at each Record Room,		Minimum 100	

	Actual numbers can be estimated and ascertained by Vendor after visiting the site before Quoting the prices)			
5.	Skilled Documentalist/Librarians (with Library experience background) for Five Years (05 Years)- Reporting to Record Room Supervisor of DDA with appropriate SOP.	Nos.	50	

~~32.20~~32.21 RFID Management System for File Tracking Movement.

S. No	Description	Numbers	Qty. Quoted	Compliance (Yes/No)
1.	RFID Application	Lump Sum		
2.	Rate for 100,000 Files to be Tagged	1		
3.	Scanners	Nos.	500	