Annexure -7

Hardware Specification

The specifications mentioned herein below are indicative in nature. Equivalent or higher specifications acceptable to NKDA

S/No	Item	Description	Min Qty
1	Blade Enclosure	Enclosure for Housing Blades	As required
2	2P Blades	Servers for DB, Web, GIS and other applications & Management	4
3	SAN Storage	Centralized SAN Storage	1
4	SAN Switch	16/24 Port SAN Switch	2
5	Firewall	Firewall, IPS and Security	1

Detailed Specification is given below:

SL No	Item	Specification	
01	**Blade Enclosure**	**Enclosure**	The enclosure should be capable of accommodating Intel, AMD, RISC/EPIC Blades within the same chassiss.
		No of Server	The enclosure should support minimum up to 14 * Dual Socket server blades
		I/O Bays	The enclosure should have minimum 8 * I/O interconnect bays for different I/O Interconnects like Ethernet, FC, SAS, Infiniband etc.
		Power Supplies	The enclosure should be configured with N+N Redundat Hot Swappable Power Supplies
		Fan Modules	The enclosure should be configured with N+N redundant hot swappable Fan Modules
		Management Module	The Enclosure should be configured with Redundant Hot Swappable Management Modules
		Ethernet Interconnect	The enclosure should be configured with Dual Ethernet Interconnect modules with minimum 16 * 10Gb/s Downlink and 8 * 10 Gb/s Uplink Ports. The interconnect module should be able to provision 4 * NIC ports with individual MAC IDs oout of each 10Gb/s Ethernet Port on the Server
		Fiber Channel Interconnect	The enclosure should be configured with Dual 8GB FCInterconnect modules with minimum 16 * 8Gb/s Downlink and 8 * 8Gb/s Uplink Ports. The interconnect module should be support NPIV
02	**Server**	**Processor**	Latest generation x86-64 processor , 2 nos of 4-Core Latest Generation processors, 2.6GHz or more with

			Minimum 20MB Cache and Dual 8 GT/s QPI. Higest range of processor from OEM for the offered class of server should be offered
		Memory	64GB Load Reduced DDR3 RAM scalable to at least upto 512GB
		Memory Protection	Advanced ECC with multi-bit error protection supporting technologies of memory mirroring and memory lockstep mode
		Hard disk drive with carrier	2 * 600 GB hot plug SFF SAS drives
		Storage Controller	Integrated PCIe 3.0 based SAS Raid Controller with RAID 0, 1 with 512MB of Flash / Battery backed write cache
		Networking features	2 * 10Gbps network port which supports partitioning up to 4* Ethernet ports per 10Gbps port
		Interfaces	Minimum of 1 * internal USB 2.0 port and 1* internal SDHC card slot
		SAN Connectivity	Dual Ported 8Gb/s FC-HBA with NPIV Support
		Bus Slots	Minimum of 2Nos of 3.0 PCIe x16 based mezzanine slots supporting Ethernet, FC adapters
		Industry Standard Compliance	ACPI 2.0 Microsoft® Logo certifications USB 2.0 Support IPMI 2.0 Secure Digital 2.0 TPM 1.2 Support IEEE (specific IEEE standards dependent on Ethernet adapter card(s) installed) Advanced Encryption Standard (AES) Triple Data Encryption Standard (3DES) SNMP SSL 2.0 DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP) Active Directory v1.0 PCIe 3.0
		OS Support	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) Oracle Solaris VMware Citrix Xen-Server
		Form Factor	Blade
		Provisioning	Essential tools, drivers, agents to setup, deploy and maintain (not the OS) the server should be embedded inside the server. There should be a built -in Update manager that can update these tools online.

			System remote management should support browser based Graphical Remote Console along with Virtual Power button, Remote boot using USB / CD/ DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media / image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication.
		Remote Management	The server should support Active Health System which monitors and records continuously every hardware change, every configuration change, temperature and voltage variations, and alerts changes in the server hardware and system configuration without impacting server performance. This assists in diagnosing problems and delivering rapid resolution when system failures occur.
		Server Management	Applications to access the server remotely using popular handheld devices based on Android or Apple IOS should be available The Systems Management software should provide Role-based security Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD. Should support automatic event handling that allows configuring policies to notify failures via e-mail, pager, or SMS gateway or automatic execution of scripts. Should provide an online portal that can be accessible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contracts and status. The Portal should also provide a personalized desk-board to monitor device heath, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. Should support scheduled execution of OS commands, batch files, scripts, and command line apps on remote nodes Should be able to perform comprehensive system data collection and enable users to quickly produce detailed inventory reports for managed devices. Should support the reports to be saved in HTML, CSV or XML format. Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components. The Server Management Software should be of the same brand as of the server supplier.

03	**SAN Storage**	**Operating System & Clustering Support**	The storage array should support industry-leading Operating System platforms including: *Windows Server 2008, Windows 2012*, Vmware, Sun Solaris, HP-UX, IBM-AIX and Linux.
		Capacity & Scalability	1. The Storage Array shall be offered with 20TB usable Capacity using 450GB or lesser size SAS 10K RPM drives and 20TB usable capacity using NL SAS 2TB/3TB Drives (1TB = 1024GB) 2. Storage shall be scalable to minimum of 400TB
		Cache	1. Offered Storage Array shall be given with Minimum of 32GB cache in a single unit and shall be scalable to 64GB without any controller change. 2. Cache shall be used only for Data and Control information. OS overhead shall not be done inside cache. 3. Cache shall be dynamically managed for both Read and Write operations.
		Architecture & Processing Power	Controllers shall be true active-active so that a single Logical unit can be shared by both controllers at the same time.
		No Single point of Failure	Offered Storage Array shall be configured in a No Single Point of configuration including Array Controller card, Cache memory, FAN, Power supply etc.
		Disk Drive Support	Offered Storage Array shall support 6Gbps dual-ported 300 / 450 / 600 / 900GB hot-pluggable Enterprise SAS hard drives, Minimum of 100 / 200GB SLC & 400 GB MLC SSD Drives along with SAS MDL 1TB / 2TB / 3TB drives.
		Raid Support	Offered Storage Subsystem shall support Raid 0, 1, 1+0, 5 and Raid 6.
		Data Protection	Incase of Power failure, Storage array shall have de-stage feature to avoid any data loss.
		Host Ports & Back-end Ports	1. Offered Storage shall have minimum of 12 host ports for connectivity to servers running at 8Gbps speed and shall be scalable to 16 host ports without any controller change. 2. Offered storage shall also support additional Quad 10Gbps native ISCSI ports.

		Global Hot Spare	1. Offered Storage Array shall support distributed Global hot Spare for offered Disk drives. 2. Global hot spare shall be configure as per industry practice.
		Performance and Quality of Service	1. Shall have capability to use more than 30 drives per array group or raid group for better performance. 2. Storage shall be provided with Performance Management Software. 3. Offered Storage array shall support quality of services so that required performance (IOPS) or bandwidth or both can be "Guaranteed" into the environment.
		Thin Provisioning and Space Reclaim	1. Offered storage array shall be supplied with Thin provisioning and Thin Re-claim to make the volume thin for an extended period of time for complete array supported raw capacity.
		Maintenance	Offered storage shall support online non-disruptive firmware upgrade for both Controller and disk drives.
		Snapshot / Point in time copy / Clone	1. Offered Storage shall have support to make the snapshot and full copy (Clone) on the thin volumes if original volume is created on thick or vice-versa. 2. The storage array should have support for controller-based snapshots functionality for pointer-based snapshots (At-least 64 copies), 3. Storage array shall have functionality to re-claim the space from Thin Provisioned Deleted snapshot automatically. Vendors shall provision at-least 20% additional space over and above the actual requirements, if space re-claim from thin provisioned deleted snapshot is not possible automatically.
		Storage Array Configuration & Management Software	1. Vendor shall provide Storage Array configuration and Management software. 2. Software shall be able to manage more than one array of same family.
		Storage Tiering	1. Offered storage shall support dynamic migration of Volume from one Raid set to another set while keeping the application online. 2. For effective data tiering, Storage subsystem shall support automatically Policy based Sub-Lun Data Migration from one Set of drive Tier to another set of drive tier.

		Remote Replication	1. The storage array should support hardware based data replication at the array controller level across all models of the offered family. 2. The Storage array shall also support three ways (3 Data Centers) replication to ensure zero RPO in native fashion without using any additional replication appliance. 3. Replication shall support incremental replication after resumption from Link Failure or failback situations.
04	**SAN Switch**		

1. Non-blocking architecture with minimum of 16 ports and scalable up to 24 ports in a single domain concurrently active at 8 Gbit/sec full duplex with no oversubscription.
2. Minimum Dual switches shall be offered
3. The switch should support auto-sensing 1, 2, 4, and 8 Gbit/sec capabilities.
4. The switch shall support different port types such as FL_Port, F_Port, M_Port (Mirror Port), and E_Port; self-discovery based on switch type (U_Port); optional port type control in Access Gateway mode: F_Port and NPIV-enabled N_Port
5. The switch should be rack mountable.
6. Non disruptive Microcode/ firmware Upgrades and hot code activation.
7. The switch shall provide Aggregate bandwidth of 192 Gbit/sec: 24 ports × 8 Gbit/sec (data rate) end to end.
8. Shall have optional support for Adaptive Networking services such as Quality of Service (QoS) to help optimize application performance in consolidated, virtual environments. It should be possible to define high, medium and low priority QOS zones to expidite highpriority traffic.
9. SAN switch shall have support to restrict data flow from less critical hosts at preset bandwidths.
10. The Switch should be configured with the Zoning and shall also support ISL trunking when more than 2 switches are configured in a single fabric.
11. The switch shall be able to support ISL trunk up to 64 Gbit/sec between a pair of switches for optimal bandwidth utilization and load balancing.
12. Exchange-based load balancing across ISLs should be supported with Dynamic Path Selection included in Switch OS
13. SAN switch shall have support to isolate the high bandwidth data flows traffic to specific ISLs.
14. Switch shall support to measure the top bandwidth-consuming traffic in real time for a specific physical or virtual device, or end to end across the fabric.
15. Support for web based management and should also support CLI.

		16. The switch shall support advanced zoning and ACL to simplify administration and significantly increase control over data access. 17. Offered Switch shall have support to configure the switches with alerts based on threshold values for temperature, fan status, Power supply status, port status.
06	**Firewall**	Single box solution supporting Firewall, IPS and IPSec/SSL (Web VPN) VPN functionality. Minimum of 4 Nos 10/100/1000 Mbps ports Concurrent Sessions 250,000. IPSec VPN Peers 300 upgradeable up to 750. WebVPN Peers 300 upgradeable up to 750. X.509 Certificate and CRL Support It shall support Simple Certificate Enrollment Protocol (SCEP)-based enrollment and manual enrollment with leading X.509 solutions from Baltimore, Cisco, Entrust, iPlanet/Netscape, Microsoft, RSA, and VeriSign It shall be able to interoperate with large-scale Public Key Infrastructure (PKI) deployments through n-tiered certificate hierarchy support It shall deliver robust Stateful inspection firewall services which track the state of all network communications It shall provide flexible access-control capabilities for more than 100 predefined applications, services, and protocols, with the ability to define custom applications and services It shall support inbound/outbound ACLs for interfaces, time-based ACLs, and per user/ per-group policies for improved control over network and application usage It shall simplify management of security policies by giving administrators the ability to create re-usable network and service object groups that can be referenced by multiple security policies, simplifying initial policy definition and ongoing policy maintenance Advanced Application and Protocol Inspection It shall have specialized inspection engines that provide rich application control and security services for protocols such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Extended Simple Mail Transfer Protocol (ESMTP), Domain Name System (DNS), Simple Network Management Protocol (SNMP),

		Internet Control Message Protocol (ICMP), SQL*Net, Network File System (NFS), H.323 Versions 1-4, Session Initiation Protocol (SIP), Real-Time Streaming Protocol (RTSP), GPRS Tunneling Protocol (GTP), Internet Locator Service (ILS), Sun Remote Procedure Call (RPC) etc It shall provide a powerful, highly flexible framework for defining flow- or class-based policies, enabling administrators to identify a network flow or class based on a variety of conditions, and then apply a set of customizable services to each flow/class It shall have features to improve control over applications by introducing ability to have flow- or class-specific firewall/inspection policies, QoS policies, connection limits, connection timers etc. It shall be able to deliver per-flow, policy-based QoS services, with support for LLQ and traffic policing for prioritizing latency-sensitive network traffic and limiting bandwidth usage of administrator-specified applications It shall enable businesses to have end-to-end QoS policies for their extended network It shall support deployment of Security Appliance in a secure Layer 2 bridging mode, providing rich Layer 2—7 firewall security services for the protected network while remaining "invisible" to devices on each side of it It shall simplify Security Appliance deployments in existing network environments by not requiring businesses to re-address the protected networks It shall support creation of Layer 2 security perimeters by enforcing administrator defined access control policies for Layer 2 network traffic It shall provide wealth of advanced attack protection services to defend businesses from many popular forms of attacks, including denial-of-service (DoS) attacks, fragmented attacks, replay attacks, and malformed packet attacks It shall deliver advanced TCP stream reassembly and traffic normalization services to assist in detecting hidden application and protocol layer attacks It shall be integrable with Network Intrusion Prevention System (IPS) solutions to identify and dynamically block or shun hostile network nodes Authentication, Authorization, and Accounting (AAA) Support

		It shall be integrable with popular AAA services via TACACS+ and RADIUS, with support for redundant servers for increased AAA services resiliency It shall provide highly flexible user and administrator authentication services, dynamic per-user/per-group policies, and administrator privilege control through tight integration with AAA Server Robust IPSec VPN Services It shall have robust IPSec VPN Services able to deliver feature-rich remote access VPN concentrator services for up to 1500 remote software- or hardware-based VPN clients It shall push VPN policy dynamically to VPN Remote-enabled industry standard solutions upon connection, helping to ensure that the latest corporate VPN security policies are used It shall be able to perform VPN client security posture checks when a VPN connection attempt is received, including enforcing usage of authorized host-based security products and verifying its version number and status prior to letting the remote user access the corporate network OSPF Dynamic Routing It shall provide comprehensive OSPF dynamic routing services It shall offer improved network reliability through fast route convergence and secure, efficient route distribution It shall also support MD5-based OSPF authentication, in addition to plaintext OSPF authentication, to prevent route spoofing and various routing-based DoS attacks. It shall provide route redistribution between OSPF processes, including OSPF, static, and connected routes IT shall support load balancing across equal-cost multipath routes IPv6 Networking It shall provide access control and deep inspection firewall services for native IPv6 network environments and mixed IPv4/IPv6 network environments through dual-stack support. It shall deliver IPv6-enabled inspection services for HTTP, FTP, SMTP, ICMP, TCP, and UDP-based applications. It shall support SSHv2, telnet, HTTP/HTTPS, and ICMP-based management over IPv6

		Security Device Manager It shall have Web-based GUI enables simple, secure remote management of Firewall Security Appliances It shall provide a wide range of informative, real-time, and historical reports which give critical insight into usage trends, performance baselines, and security events Auto Update It shall have feature providing "touchless" secure remote management of Security Appliance configuration and software images via a unique "push/pull" management Model It shall have ability to have Next-generation secure Extensible Markup Language (XML) over HTTPS management interface can be used by any third-party management applications for remote Security Appliance configuration management, inventory, software image management/deployment and monitoring SNMP and Syslog Support It shall provide remote monitoring and logging capabilities, with integration into third party management applications It should support IPSec Flow Monitoring SNMP MIB, providing a wealth of VPN flow statistics including tunnel uptime, bytes/packets transferred etc.