CBS Implementation Project
Technical Specifications for required hardware and virtualization

Brand Servers	Quantity: 3 pcs
Chassis	1U Rack Mountable
CPU	Two (2) Intel Xeon Silver 4216 (2.1GHz/16-core/100W) processors
Motherboard	Intel® C621 Series Chipset
Memory	512 GB (16x32GB) DIMMS should be included scalable up to 1.5 TB using DDR4 (RDIMM) operating at 2666 MHz (depending on processor model) up to 24DIMM slots
Memory Protection	Advanced ECC with multi-bit error protection, Online spare, mirrored memory and fast fault tolerance
HDD Bays	Should be installed 2 x 240GB SATA SSD SFF Should support up to 8+2 SFF HDD/SSD or 10 NVMe PCIe SSD The drive carrier should have intuitive icon based display along with "DO NOT REMOVE" caution indicator that gets activated automatically in order to avoid data loss/downtime due to wrong drive removal.
Hard disk drive	Hot Plug SFF or LFF SATA/SAS/SATA SSD/SAS SSD and NVMe drives
Controller	Server should have included dual port 16Gb HBA for connection to storage and also installed RAID Controller, supporting 12Gb/s SAS and PCIe 3.0
Networking features	Server should have installed 1Gb 4-port network adaptors and support networking cards 10Gb 2-port Ethernet adaptor / 10GBaseT 4-port Ethernet adaptor / 4x25Gb Ethernet adaptor / 10/25Gb 2-port Ethernet adaptor
Interfaces	Serial - 1 Micro SD slot - 1 USB 3.0 support With Up to 5 total: 1 front, 2 internal, 2 rear, 2 internal (secure)
Bus Slots	Three PCI-Express 3.0 slots, at least two x16 PCIe slots
Power Supply	Should have installed 2 x 500W PSU and support hot plug redundant low halogen power supplies with minimum 94% efficiency
Fans	Redundant hot-plug system fans

Industry Standard Compliance	ACPI 6.1 Compliant
	PCIe 3.0 Compliant
	PXE Support
	WOL Support
	Microsoft® Logo certifications
	USB 3.0 Support
	USB 2.0 Support
	Energy Star
	ASHRAE A3/A4
	UEFI (Unified Extensible Firmware Interface Forum)
	SMBIOS
	Redfish API
	IPMI 2.0
	SNMP v3
	TLS 1.2
	DMTF Systems Management Architecture
	Active Directory v1.0
System Security	UEFI Secure Boot and Secure Start support
	Security feature to ensure servers do not execute compromised firmware code
	FIPS 140-2 validation
	Common Criteria certification
	Configurable for PCI DSS compliance
	Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser
	Support for Commercial National Security Algorithms (CNSA) mode to prevent the use of insecure algorithms
	Tamper-free updates - components digitally signed and verified
	Secure Recovery - recover critical firmware to known good state on detection of compromised firmware
	Ability to rollback firmware
	Secure erase of NAND/User data
	TPM (Trusted Platform Module) 1.2
	TPM (Trusted Platform Module) 2.0
	Bezel Locking Kit option
	Chassis Intrusion detection option Support for Commercial National Security Algorithms (CNSA)
	Smart card (PIV/CAC) and Kerberos based 2-factor Authentication
	Configurable for PCI DSS compliance
	Secure erase of NAND
Operating Systems and Virtualization Software Support	Server should support and also support Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Vmware, ClearOS
GPU support	System should support NVIDIA's latest computational accelerators and graphics accelerators
System tuning for performance	1. System should support feature for improved workload throughput for applications sensitive to frequency fluctuations. This feature should allow processor operations in turbo mode without the frequency fluctuations associated with running in turbo

	mode 2. System should support workload Profiles for simple performance optimization
Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.
Warranty	Server Warranty Should include 3-Year Parts, 3-Year Labor, 3-Year Onsite support with next business day response.
Firmware security	1. For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable 2. Should maintain repository for firmware and drivers' recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware
Embedded Remote Management and firmware security	1. 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 2. Server should have dedicated 1Gbps remote management port 3. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware 3. Server should support agentless management using the out-of-band remote management port 4. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 5. Applications to access the server remotely using popular handheld devices based on Android or Apple IOS should be available 6. Remote console sharing up to 6 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128-bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console. 7. Should support RESTful API integration 8. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support
Server Management	Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resource's user is authorized to view.

	The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware • Appliance alerts
	The Systems Management software should provide Role-based access control
	Management software should support integration with popular virtualization platform management software like vCenter, and SCVMM
	Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.
	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 contrats and status. The Portal should also provide a Personalized dashboard to monitor device heath, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud).
	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.
Warranty	3 Years
MAF	Manufacturer Authorization Form – Mandatory

Min.20 TB Brand Storage	Quantity: 1 pcs
Operating System & Clustering Support	1. The storage array should support industry-leading Operating System platforms including: Windows 2012 / 2016, VMWare and Linux. 2. Offered Storage Shall support all above operating systems in Clustering.
Capacity & Scalability	1. The Storage Array shall be offered with 20 TB Raw Capacity Storage using SSD Drives. 2. For effective power saving, Storage subsystem shall be supplied with 2.5" Small form factor SFF drives, however storage subsystem shall also support LFF drives with the addition of required disk enclosures. 3. Storage shall be scalable to minimum of 90 number of drives or greater than 160TB. 4. At least one separate spare drive must be included in the price. This drive must be provided separately and not to be included in the raid array of initial 20TB raw capacity
Front-end Ports	Offered Storage system shall be supplied with minimum of Dual 16Gbps FC ports and Dual 10Gbps ISCSI ports per controller.
Architecture	Offered storage shall have flexibility to use all above ports either as FC or ISCSI by replacing the requisite SFP. Vendors shall provide the additional SFP accordingly. In

	case, vendor doesn't support this feature, then every controller shall be populated upfront with 4 x 16Gbps FC ports and 4 x 10Gbps ISCSI ports.
No Single point of Failure	Offered storage array shall also support self-encrypted SSD, SAS and near line SAS drives.
Disk Drive Support	Storage Array shall support at-least 190 Enterprise SAS SFF drives.
Cache	1. Fibre Channel external storage system with dual Fibre active – active RAID controllers having a minimum of 8GB Cache per controller. 2. Cache shall be backed up (Either through Battery, Capacitors or any other equivalent technologies) for an indefinite time or at-least 5 -7 years of time. 3. Offered storage shall have optional support for SSD / Flash based Cache. Offered Storage shall support at-least 8TB of Flash cache. Vendor shall offer at-least 6TB of flash cache. 4. Offered Flash cache shall be tuned for random read operations and shall remain activated even at less than 70% of random average read workload.
Raid Support	1. Offered storage shall support Raid 1, Raid 1+0, Raid 5 and Raid 6. Thin provisioning shall be supported on all the raid sets as well as with Flash cache. 2. Offered storage shall be offered and configured with virtualization capability so that a given volume can be striped across all spindles of given drive type within a given disk pool. Disk pool shall support all listed raid sets of Raid 1, Raid 5 and Raid 6.
Point in time and clone copy	1. Offered Storage subsystem shall have controller based Snapshot and Clone support. Storage subsystem shall be supplied licenses for 512 Snapshots. 2. Offered Storage system shall support minimum of 512 numbers of snapshots and 128 number of clone copies.
Replication	1. Offered storage subsystem shall support disaster recovery features like replication to DR location. Licenses for the maximum supported capacity of the array shall be supplied. 2. Offered storage subsystem shall support replication to multiple storage array of the same family in fan-out mode. At least 1:4 mode shall be supported.
Thin Provisioning and Data Tiering	1. Offered Storage shall also be licensed for Sub-Lun Data tiering in real time fashion across different type of drives within a given pool like SSD, SAS, NL-SAS etc. License for same shall be offered for maximum supported capacity of the array. 2. Offered Storage shall also be offered with Thin provisioning.
Global and dedicated Hot Spare	1. Storage Array should have the capability of configuring hot swap disks and Global Spare disks as well as dedicated spare disk to raid sets.
Logical Volume & Performance	1. Storage Subsystem shall support minimum of 512 Logical Units. Storage Array shall also support creation of more than 100TB volume at controller level. 2. Offered Storage shall have inbuilt performance management software. Configuration Dashboard shall show overall IOPS and MB/sec performance.
Load Balancing & Muti-path	1. Multi-path and load balancing software shall be provided, if vendor does not support MPIO functionality of Operating system.
Warranty	3 Years
MAF	Manufacturer Authorization Form - Mandatory

Virtual Infrastructure with Management	Quantity: 3 ESXi hosts and 1 vCenter
Mandatory Features	Virtual Infrastructure Solution must provide business continuity and always-available IT, Reduce IT footprint and simplify management, Save on IT hardware costs, improve service levels and application quality, Strengthen security and data protection.
	Virtual Infrastructure Solution must provide robust Hypervisor Architecture, production-proven, high-performance virtualization layer that enables multiple virtual machines to share hardware resources with performance that can match or exceed native throughput.
	Virtual Infrastructure Solution must provide centralized management and performance monitoring for all virtual machines and hosts with built-in physical-to-virtual (P2V) machine conversion and rapid provisioning, using virtual-machine templates.
	Virtual Infrastructure Solution must provide Virtual Machine file system
	Virtual Infrastructure Solution must provide virtual machines to access shared storage devices
	Virtual Infrastructure Solution must provide Thin Provisioning
	Virtual Infrastructure Solution must provide Converter which enables IT administrators to rapidly convert physical servers and third-party virtual machines to virtual machines.
	Virtual Infrastructure Solution must provide Hardware compatibility with the broadest range of 32- and 64-bit servers and OSs, storage and networking equipment and enterprise management tools.
	Virtual Infrastructure Solution must include the following business-continuity features and components for always-available IT:
	High Availability feature which provides cost-effective, automated restart within minutes for all applications in the event of hardware or OS failures.
	Live migration of virtual machines across servers with no disruption to users or service loss, eliminating the need to schedule application downtime for server maintenance.
	Agentless antivirus and antimalware protection to secure your virtual machines.
	Replication Feature which provides low-cost replication for your virtual machine and serves as the foundation for leveraging a cloud-based disaster-recovery solution from a VMware cloud service provider.
	Solution Must be Licenses in bundle Centralized Management
	License kit must include 6 CPU licenses for 3 servers with up to 2 processors each and 1 license for Centralized Management Module
	License Kit must be perpetual with 3 Year Production Support and Subscription
MAF	Manufacturer Authorization Form - Mandatory

Brand name UPS 6000VA	Quantity: 1 pcs
Topology	On-line double conversion with PFC (Power Factor Correction) system
Configuration	Rack/Tower
Rating (VA/Watts)	6000/5400
Rail Kit Included	Yes
Connection	Hardwired
Electrical Input	
Input Voltage Range	176-276V without derating (up to 100–276V with derating)
Nominal Voltage	200/208/220/230/240V
Frequency	50/60 Hz auto selection
Frequency Range	40-70 Hz
Short Circuit Current	90 A
THDI	<5%
Electrical Output	
Voltages	200/208/220/230/240V +/– 1%
Voltage THD	< 2%
Outlets	(8) IEC-320-C13, (2) IEC-320-C19, Hardwired
Overload Capacity	102–110% : 120s, 110–125%: 60s, 125–150%: 10s, >150%: 500ms
Efficiency (Normal Mode)	Up to 94% in Online mode, 98% in Hi-Efficiency mode
Output Frequency	50/60 Hz auto selection, frequency converter as standard
Load Crest Factor	3:1
Battery Management	Temperature compensated charging method, automatic battery test, deep discharge protection, automatic recognition of external battery units.
Communications	
User Interface	Multilingual graphical LCD display
Communication Ports	1 USB port, 1 RS232 serial port, 1 mini terminal block for remote On/Off and 1 for remote power Off
Warranty	1 Year
MAF	Manufacturer Authorization Form - Mandatory

Mandatory Requirement:
1. Complete Installation and Configuration to be performed by an authorized supplier
2. Handover and technical documentation to be provided upon completion of the project
3. On-Site training for min. 2 staff
4. 1 Year Local Support to be included / 4 hours response time on-site