INDEX

SECTION 3

SCOPE OF WORK
SCOPE OF WORK / SERVICE LEVEL AGREEMENT

Haryana State Electronics Development Corporation Ltd. (HARTRON), a State Govt. undertaking invites e-Bids from the manufacturers/their authorized firms of Networking for Selection of System Integrator for Supply, Design, Build, Installation, Commissioning with O&M of Haryana State Data Centre along with NL BCP DR & Far DR for 5 Years as per the minimum technical specifications and other terms and conditions mentioned in this Tender document.

3.1 STATE DATA CENTRE 1.0 RACK LAYOUT

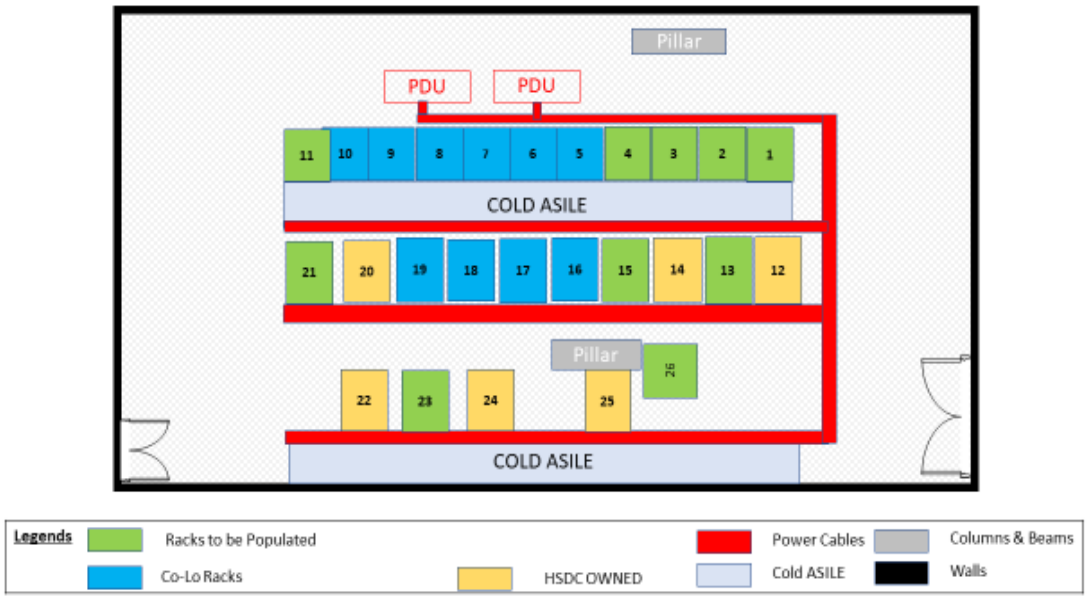
State Data Center (HSDC) is operational since 14-08-2012 and is now managed by CRID, Haryana and MSP RailTel Corporation of India Ltd. ((RAILTEL) a Mini Ratna Category-1 enterprise) Govt. of India undertaking, Ministry of Railways w.e.f. 01.01.2015.Haryana State Data Centre is located in Sector 17F in new Secretariat Building, Chandigarh and comprising of total covered are of 4196 square Feet and Server Racks are installed and commissioned in 2 locations in same Haryana State Data Centre premises as given below:

1. SDC Server FARM Area Size : 942 Square feet 26 Racks
2. SNMC Server FARM Area Size : 461 Square feet 14 Racks

3.2 DETAILS OF IT INFRASTRUCTURE

1) Following is the layout of existing SDC Server farm area:

Proposed SDC Server FARM Floor Plan Layout : 26 Numbers 42 U Racks



2) There are presently provision of 26 Numbers of total Racks comprising 22 numbers of Server Racks, 2 Numbers of Network Racks and 2 numbers of network patch panel Racks in SDC Server Farm Area in which following are the key pointers:

   a) Racks 13 & 15 are Network Racks and all Network and Security equipment are installed and commissioned in these Racks and Racks 12 and 14 are also Network Racks having patch panel for distribution. New Network and Security equipment shall replace old network and security equipment installed and commission in these Racks of Haryana State Data Centre.
   b) Racks 1,2,3,4,11,21,23 & 26 i.e. 8 Racks shall be available to install and commission rest of proposed ICT infrastructure as given below indicative:
      - Compute
      - Network and Security

- Backup & Storage
- Secondary Backup (Tape Library)
- HCI

c) ## Racks 20,22,24 & 25 are completely HSDC owned and having storage, Blade Servers, SLB, HSM etc. Rack 16 is partially in HSDC owned and co-location too. Those work load of these racks will be migrated into the new infrastructure which have obsolete hardware. After migration of the workload more racks will be available for installation of new infrastructure.

d) # Racks i.e. 5,6,9,10,17,18,19 i.e. 7 Racks are in colocation in SDC Server farm area. In these racks some of the work load will also migrate to new infrastructure.

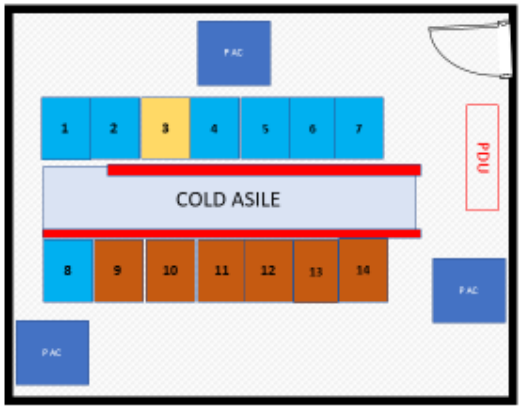
e) * Rest of Racks 7,8 i.e. 2 Racks are in pure colocation in SDC Server farm area.

f) Each Server Rack capacity may have load upto 12KVA.

** Space, power and BMS is provided by HSDC*
 # Space, power, BMS, Network Connectivity & Security provided by HSDC
Space, power, BMS, Network Connectivity, Security, Server & Storage provided by HSDC

3) Following is the layout of existing SNMC server farm area:

Proposed SNMC Server FARM Floor Plan Layout 14 Numbers 42 U Racks



14 Numbers of Rack are installed in State Network Management Server (SNMC) server farm area and following are the key pointers:

a) ## Racks3 are completely HSDC owned in SNMC Server farm are and having Tape Library, Blade Servers & Switches.

b) # Racks1,2,4,5,6,7, & 8 i.e. 7 Racks are in colocation in SNMC Server farm area.

c) * Racks 9,10,11,12,13 & 14 i.e. 6 Racks are SWAN owned in SNMC server farm area

For (a)&(b) above the work load of these racks will be migrated into the new infrastructure which have obsolete hardware. After migration of the workload more racks will be available for installation of new infrastructure.

** Space, power and BMS is provided by HSDC*
 # Space, power, BMS, Network Connectivity & Security provided by HSDC
Space, power, BMS, Network Connectivity, Security, Server & Storage provided by HSDC

Note: After migration (SDC owned applications as well as co-location applications)MSI will be responsible for operation and management of entire new infrastructure including power, BMS, network & Security, backups, compute & storage, HVAC, etc. as well as run these workloads either in active-active or active-passive mode based on the requirement. For active-active or active passive mode Near line BCP site shall be setup by MSI. MSI will also ensure backup and recovery process as per mutually agreed RPO/RTO. It may be noted that there is a separate MSI for O&M of SWAN equipment which are installed and commissioned in SNMC Area. Due to space constraints some HSDC Racks are place in SNMC area which shall be the responsibility of the MSI on boarded through this RFP.

3.3 DISASTER RECOVERY SITE:

HSDC has no DR site but some of critical application which are in colocation, has DR site.

3.4 EXISTING VIRTUAL/BARE METAL MACHINE INFRASTRUCTURE:

Currently the HSDC has a Virtual environment in oVirt or KVM based and some of infrastructure is running on bare metal machine server too.

3.5 DETAILS OF NON-IT INFRASTRUCTURE

Details of Non-IT Infrastructure of HSDC is as follows:

DG Set

HSDC has 3 DG Sets of 320 KVA each make Cummins. All DG Sets are under OEM AMC support up to31.05.2024.

UPS System

Below mentioned UPS systems are running as per the Electrical Architecture shown at **Figure-1:**

Sr. No.	UPS/ Battery Bank Details	Installed on	AMC/ Support By
1	4 Qty of SOCOMEC 160 KVA double conversion IGBT based UPS for Server Farm Note: Fresh UPS procurement is in progress by CRID.	April-2011	SOCOMEC
2	2 Qty of SOCOMEC 30 KVA double conversion IGBT for Other equipment in SDC Note: Fresh UPS procurement is in progress by CRID.	April-2011	SOCOMEC
3	Two Sets of 128 VRLA Batteries of 150 AH, 2V Cell each		
4	Two Sets of 40 VRLA Batteries of 42 AH, 2V Cell each		

Air Conditioning System

HSDC has below mentioned AC Systems

Sr. No.	AC Details	Qty Installed
1	11.4 TR Precision Air Conditioning (PAC) Systems for SNMC Server Farm Area	3
2	11.9 TR In Row Cooling Systems in SDC Server FARM Area(UPS & Electrical Room) - Including one Standby	10

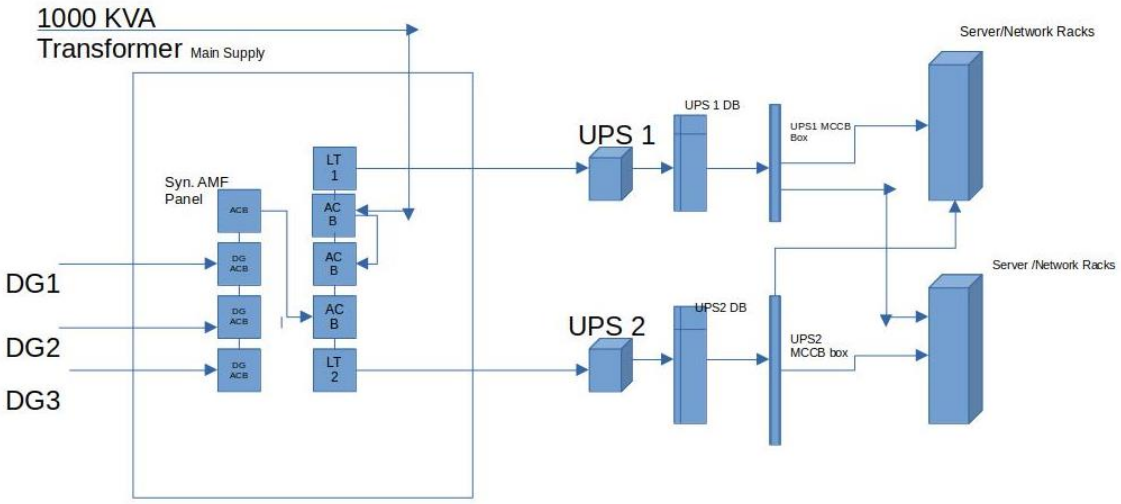


Figure 1: Existing Electrical Architecture of HSDC

Building Management System

Currently, HSDC has BMS from Spectra with below mentioned sub-systems. Details of these sub-systems can be referred at Annexure B

1. Fire Detection & Alarm System
2. Clean agent gas suppression system
3. Water Leak Detection System
4. Very Early Smoke Detection Apparatus (VESDA) solution
5. Access Control System
6. CCTV Surveillance System
7. Public Address System
8. Rodent Repellent System
9. Common alarms (Temperature and Humidity monitoring system)
10. Generator and diesel level monitoring system

3.6 VISION FOR HSDC 2.0

The State Data Centre shall essentially provide Government to Government (G2G) Cloud Services to host Haryana government websites, portal and web applications with the speed and scalability that as per the required SLAs. State Data Centre Cloud Services will be capable to offer variety of service model to meet Government Department's requirements like Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Services (SaaS) as a Cloud Service Provider (CSP).

General

1. Representatives of prospective MSI shall be allowed to visit Haryana State Data Centre for inspection of the Data Center area, available Non-IT Infrastructure, understanding of existing server room setup, discussing the technical requirements, understanding deployment architecture and discussing the implementation plan.
2. The MSI shall supply all necessary Hardware, Software and licenses etc. as per "Bill of Material" / Work Order and in accordance with minimum specifications as provided in "Bill of Material".
3. Requirement of all compute and storage as per BoQ is for CRID usage. Any compute and/ or storage requirement to install and commission any kind of software/ hardware like HIPS, DLP SIEM, etc. should be part of the respective solution offered by respective OEM/MSIincluding

required licenses and should be exclusive of Compute/ Storage required in the BoQ of the RFP.

4. All the supplied equipment & licenses should be in the name of the purchaser "Citizen Resources Information Department (CRID)".
5. The MSI shall be responsible for providing all equipment, software and services, specified or otherwise, which are required to fulfil the intent of ensuring operability, maintainability and reliability of complete solution within the quoted/contract price.
6. The MSI shall provide support and professional services for deployment architecture, installation, configuration, performance tuning, security, acceptance testing and commissioning of the supplied products & implementation of functional / technical requirements as per RFP and carry out required integration of various components offered in overall solution of HSDC.
7. The MSI will deploy the equipment as per the Deployment Architecture of the HSDC solution finalized by the purchaser with no single point of failure and in line with the industry best practices. Integration between various components offered in the overall solution needs to be done as indicated in the proposed deployment architecture in this RFP. However, any minor change in the deployment architecture necessitated to meet the requirements of DC, NL-DR for BCP and Far DR and their integrations will be allowed subject to the approval of the competent authority.
8. Note:- "FAR DR" location shall be in different seismic zone from Haryana State Data Centre location and will be shared with successful bidder. The MSI shall deploy, configure, fine-tune & optimize the supplied infrastructure including hardware, software, network & security components, as per industry best practices and requirements of the RFP
9. MSI shall perform work for Network & Security equipment installation, implementation & integration with existing infrastructure and shall provision (supply, install& commission) the necessary passive components for physical network connectivity of the new infrastructure with existing internet gateway and existing HSDC Infrastructure as per requirement. CRID will upgrade existing NKN link from 1Gbps to 10 Gbps and take one extra internet link of bandwidth of 10Gbps from different ISP(not providing services in existing NKN link).The MSI shall prepare a detailed plan to perform these activities. Planned downtime of appropriate duration shall be allocated for these activities during off peak hours on non-working days.

Note:

a. The MSI will perform all the necessary tasks required for smooth functioning of existing HSDC Infrastructure.
b. The required racks and PDU's in addition to proposed racks/ PDUs for the supplied equipment will be provided by MSI, if existing racks / PDUs are not found suitable for installation of equipment supplied by MSI.
c. All software licenses required for interoperability of various components of the solution are to be provisioned by MSI.

10. MSI will manage all equipment and its respective functionalities (which includes but is not limited to hardware, system software and application platform etc.) of BOM and backup management will also be in scope of MSI.
    Note:- Tape custody shall be joint responsibility of CRID(SDC team) and MSI.
11. MSI shall ensure that:
    a. All equipment must support NTP synchronization with central server and should support logs to centralized syslog server.
    b. All OEMs of security equipment demanded in RFP must have its own threat intelligence analysis Centre.
    c. All OEMs of equipment demanded in RFP must have reporting, monitoring & management platform capable ofrole-based administration.
    d. The configuration/image backup & restore solution for network and cyber security equipment in scheduled/automatic manner are maintained.
    e. All OEMs of equipment demanded in this RFP must have capability to integrate with the SIEM solution offered against this RFP.

Core Services of HSDC 2.0

1. Infrastructure as a Service (IaaS): IaaS provides basic virtual compute infrastructure resources like CPU, Memory, Disk Storage attached to blank VMs with allowing departments to install OS, using ISOs, from scratch and customization. However, Departments have to use their own licenses for OS and Application software (if any).
2. Platform as a Service (PaaS): PaaS provides pre-installed web and database servers so that Departments can publish and run web application without worrying about server setup. The servers are pre-configured ready with basic security hardening. Use PaaS service to quickly deploy servers and publish web applications. The OS & Application Software licenses are provided by us as part of offering.
3. Software as a Service (SaaS): This provides on demand software service. SaaS is a software delivery model where users are not responsible for supporting the application or any of the components. In case, Departments are having SaaS enabled web application and want to distribute it to users, they can use State Data Centre Cloud Services to deliver through Software as a Service.

Total Racks available for MSI for ICT infrastructure at HSDC=12	
Items	**Max Racks Available**
Servers	**6**
Network and Security	**3**
Backup and Storage	**2**
Extra	**1**

Note :-

1. MSI must ensure a secure and resilient design in the data center such that all the assets are protected from - Data loss/leakage, Data exfiltration and ransomware etc. and the desired critical services of the Government are available following applicable ISO 27001 controls, guidelines and compliance requirements as per the IT Act 2000/2008, The Digital Personal Data Protection Act 2023, NCIIPC/ Cert-In/ guidelines and amendments notified by Government of India from time to time.
2. All compute and storage will be exclusively used for application, website, department data store only. Any other solution/equipment desired in RFP requiring compute/storage or any other additional resources shall be supplied as a part of respective solution without any additional cost or overhead to purchaser.

Other Value-Added Services but not limited to:

Vulnerability Assessment Service, Load Balancer as a Service, Public IP Service, Anti-virus Service, Resource Monitoring as a Service, Web Application Firewall (WAF) Service, Backup Service, Storage as a service, APM as a service and SOC will be provided to all the departments of whom the applications are hosted.

1. Vulnerability Assessment Service: This service helps Department to assess Departmental Servers and networks for identifying the security vulnerabilities i.e. threats and risks they pose. A vulnerability assessment process detects and classifies system weaknesses in Servers, networks and communications equipment and predicts the effectiveness of countermeasures.
2. Load Balancer as a Service: Load balancing Service allows Department to efficiently get incoming network traffic requests distributed across a group of back-end servers (e.g. server farm / server pool). This service is available on demand for critical application requiring high availability and easy workload manageability.

3. Public IP Service: A public IP address is an IP address that can be allocated to any of your application on cloud server to make it accessed over the Internet.

4. Anti-virus Service: Virus protection is an important part of keeping the systems, applications and data in your cloud environment safe from viruses, spyware and other malware threats. Antivirus service is made available to cloud users as Managed Service.

5. Resource Monitoring as a Service: This service helps Department to monitor the cloud resources utilization and its availability with allowing Department to analyze the utilization trends for critical server resources like CPU, Memory, Network I/O etc. This helps Department for better capacity planning and provide a better end-user experience.

6. Web Application Firewall (WAF) Service: Web Application Firewall will help Department to give extra protection for HTTP / web-based applications with having applied a set of rules to an HTTP conversation and cover common attacks such as cross-site scripting (XSS) and SQL injection.

7. Backup Service: Allows Department to back up the data and application code lying inside the Cloud Servers based on various parameters like frequency, retention period etc.

8. Storage as a Service: This provides Department on demand storage of various types including file storage and block storage etc. File and Block storage are methods to store data on NAS and SAN storage systems. Each storage volume can be treated as an independent disk drive, and it can be controlled by external server operating system.

9. Application Performance Management (APM) Service: Application Performance Management (APM) provides the monitoring and management of performance, availability, and user experience of software applications. APM strives to detect and diagnose complex application performance problems to maintain an expected level of service.

10. Security Operations Centre: it is proposed to establish Security Operations Centre (SOC) to ensure 24*7 continuous monitoring of the cyber security posture of the Haryana Government by preventing, detecting, analyzing and responding to cyber security threats and incidents. With the increase in number of e-governance applications, web-based G2C services, citizen data and mobile subscribers has resulted in significant growth in cyber activity; therefore, establishing a SOC is a logical step towards a safer cyber space. The primary function would be to detect and contain attacks and intrusions, if any, in the shortest possible time frame, limiting the potential impact and/ or damage that an incident may have by providing near real time monitoring and analysis of suspicious events.

Proposed Setup OF NEAR Line DC Site:

Proposed near line DC site i.e. Business Continuity Site will be established in STPI, Mohali on colocation basis and proposed BOQ items for near line DC site in this RFP shall be installed and commissioned at Data Center of STPI, Mohali with desired SLAs as mentioned in the RFP.

Actual requirement on the no. of racks required at this site shall be determined when the actual hardware is delivered, however, based on the power load estimation, approximately 8 to 10 racks would be required.

Set up of FAR DR SITE:

This site will be established in a different seismic zone which shall be decided in due course. The proposed BOQ items for far DR site in this RFP shall be installed and commissioned with desired SLAs as mentioned in the RFP with approximately 1 or 2 racks.

Component-wise Migration/ Up gradation Plan:

Hosting Infrastructure

HSDC 1.0 has100+Servers,4 x Firewalls, 1 x NIPS, Enterprise Antivirus, switches etc populated 7 Racks with backbone connectivity of 2 * 1Gbps P2P links provisioned under NKN. Most of these items were purchased in 2012 and are under AMC. Details mentioned in the Annexure**-A**

Most of all of this infrastructure are at End of Life and will be replaced with the new infrastructure as mentioned in BOQ with the latest state of the art technology in a below mentioned or better way by ensuring zero or minimal downtime of SDC services:

Note:- All the needful support shall be extended to MSI by the CRID(SDC team) and application owner for smooth migration.

Step 1: Four new Racks to be installed in SDC with full inter & Intra connectivity of racks considering all parameter for High Availability (HA)

Step 2: All network structured cabling and electrical cabling are in place in the HSDC as per the Electrical architecture at Figure-2. MSI must supply and install all required accessories for structured cabling if required to install and commission supplied ICT infrastructure as per BOM. Apart from this, MSI has to maintain the existing cabling and its proper labelling for entire SDC including for Colocation Infrastructure throughout O&M period. In case of any fault in existing passive network components or electrical components, MSI has to replace the same with new one meeting the specifications of latest industry standards & certifications.

Any replacement of passive component should be as per requirements of any TIER 3 data centers in the country .

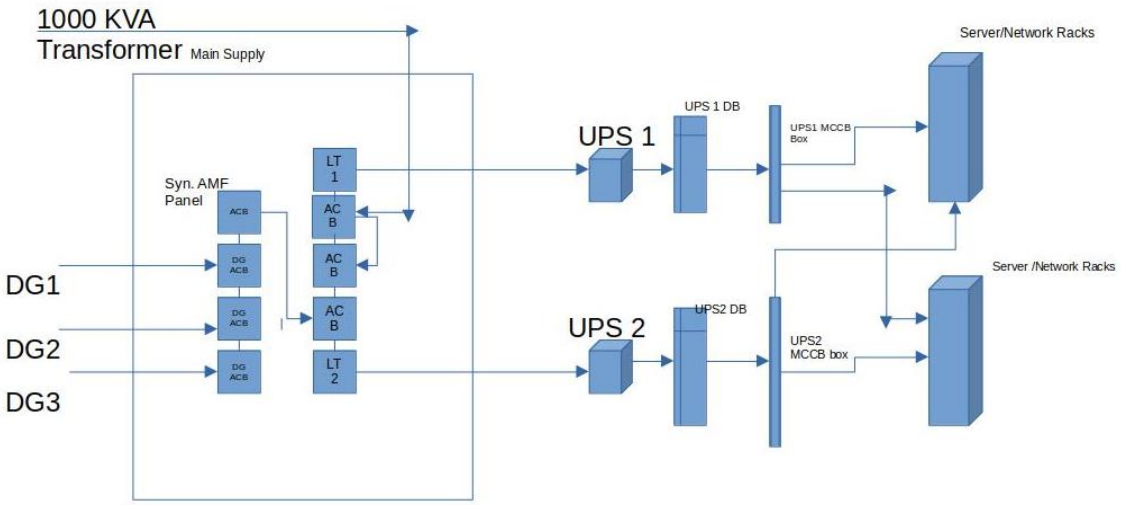


Figure-2 Electrical Architecture for HSDC

Step 3: All the Hosting services will be transferred from old Infrastructure owned by HSDC as well as some of co-location Racks to new Racks by ensuring zero or minimal downtime of SDC services within the Project Implementation Schedule as mentioned at Section Project Implementation Schedule.

Step 4 : List of applications hosted in old VM/Server is placed at Annexure-C. Out of total listed applications, 50 critical applications are marked which have to be migrated to new infrastructure before achieving project Go Live as specified in the implementation schedule in section 8. This shall include Lift Shift Migration(i.e. without or minimal upgrade of OS and Database) however in

case of major upgrade ,the bidder shall support like offering covered under platform as a services etc. to the maximum possible extent and work in close coordination with the developer/technical team(s) of concerned department/CRID to complete the migration. All other remaining applications will be parallelly migrated within 6 months' post Go Live is achieved without any additional cost and as part of O&M. Any kind of installation, commissioning and support for any type of hardware, software, databases etc. required for migration would be in scope of MSI both during GO-LIVE as well as in O&M phase.

Note:- Our existing infrastructure is running on 1Gbps switching backbone. MSI to ensure any additional ICT infrastructure/software required to perform/complete the migration activities as per the scope of work.

Colocation Infrastructure

SDC has 17 Racks as Colocation Infrastructure, populated by servers, storage, etc, provided by different departments of Haryana. This Colocation Infra is of 3 types:

Type: 1 (Pure Co-Lo) – CRID has provided just SDC Space, power and BMS to 2 Racks of various other departments. MSI has to take care of Power and BMS services only.

Type: 2 (Co-Lo with N/w) – Along with SDC Space, Power and BMS, CRID has provided Backbone services like connectivity and network security using SDC's core infrastructure to 15 Racks of various other departments. Rest of all services/management is being taken care by respective departments. MSI has to take care of these services.

Type: 3 (Co-Lo with N/w + H/w) – There is 1 Rack housing multiple applications of other departments, in which apart from services of Type 2, Dedicated Server/Storage is also provided, MSI has to take care of these servers' functionality and coordinate with respective OEMs for AMC support till the scope of the project.

Along with the current ongoing services for Collocation Infrastructure, MSI has to ensure the power distribution to each of these Racks as per the indicative Power Supply Architecture shown at Figure-2:

Step 1: Proper Power distribution need to be done for the racks having dual power strip.

Step 2: All of the single power strip racks has to be replaced with Dual Power Strip Racks, which are going to be vacated out of existing Racks.

Step 3: 4 Racks which will be supplied as part of this bill of material, MSI will install dual power strip as per Rack load.

MSI will also assist the System Integrator/Service Provider of the respective Department for configuration of their hardware as Colocation Infrastructure under the supervision of CRID. MSI will replace and ensure the backbone connectivity upto ToR Switch of respective Racks of Colocation Infra or any other correlated activity to make the system secure and operational benefiting this hardware with new infrastructure.

The security, backup, DR and SOC & NOC services will be applicable for all such collocated infrastructure also as per policies of Haryana Government applicable for respective components. All these services will have to be provisioned by the MSI for collocated infrastructure also.

Up-gradation to Private Hybrid Cloud

MSI has to configure the supplied Hardware and software infrastructure to node servers and Security equipment to provide the services (as mentioned above at Section "**Core Services of HSDC**") to other Departmentswith Software Based Automation and Orchestration on top layer using Single Pane of Glass for management. Solution should be integrated with EMS &NMS for generation of Automated Service Ticketing.

Non-IT Infrastructure

Details of Non-IT Infrastructure of HSDC is as follows:

DG Set

HSDC has 3 DG Sets of 320 KVA each. All DG Sets are under OEM AMC support. Details mentioned at Annexure E. CRID will continue the AMC contract till end of O&M from GoLive and has to refill the diesel as and when required. Re-imbursement of Diesel expenditure will be done on actual at every quarter-end based upon the consumption report verified by officials/Agency authorized byCRID**.**

UPS System

HSDC has 4*160 KVA UPS and 2*30 KVA UPS and appropriate Battery Bank are in place in the existing battery room with Battery performance monitoring system. Currently, four UPS are directly connected to their respective Output Panels. MSI can use the existing LT, UPS Output Panels, RACK PDUs and Floor PDUs. MSI has to ensure High Availability in power source to each Rack with best practices. One of such practice is illustrated at Figure – 2

Air Conditioning System

HSDC has 3*PAC installed and commissioned in SNMC Server farm area and 10 units of "In Row Cooling systems are installed and commissioned/to be installed and commissioned in SDC Server farm area.

If required, MSI need to install appropriate numbers of Relative Humidity (RH) and Temperature Sensors, integrated with existing BMS.

Note:- Installation and commissioning of in row Cooling units are not in the scope of MSI. CRID will provide HSDC Server Farm Area along with proper functioning of 10 numbers of In Row Cooling unit around 11 ton each.

Building Management System

BMS and all of its sub-systems as mentioned at Section 1.2.4are available and CRID will ensure OEM support of all BMS components through AMC/CAMC. MSI will manage, monitor, and coordinate OEM support of all BMS components till O&M.

a) Fire Detection & Alarm System
b) Clean agent gas suppression system
c) Water Leak Detection System
d) Very Early Smoke Detection Apparatus (VESDA) solution
e) Access Control System
f) CCTV Surveillance System
g) Public Address System
h) Rodent Repellent System
i) Temperature and humidity sensor
j) General Alarm System(UPS Voltage, LT Voltage, AMF Voltage, Diesel Level Status)

Design Considerations for Capability building of HSDC

CRID has envisioned a transformation of the current HSDC to a Hybrid Cloud Enabled Data Centre which would offer services to the end customers / line departments on Hosting, Co-location and Cloud model. The motive behind the vision is leveraging the properties of cloud operations that can proactively avoid performance issues and gain deep insights into the health, risk and efficiency of physical, virtual and cloud infrastructure, as well as operating systems and applications. Cloud operations would also allow to manage capacity and usage metering of cloud services. Another key reason to consider the above model is the ability to logically group resources so they can be managed by services, or by groups of services and manage services through the use of policies, which can be set to limit or manage access to cloud services in the catalogue or set alerts for administrators to be notified if services use goes out of pre-set limits.

The desirable capabilities of Haryana State Data Centre (cloud based as well as bare metal configurations) as envisioned by CRID would require but not limited to:

a. Unified life cycle management for the overall cloud solution with enterprise class support.

b. Future ready infrastructure to adopt technology changes and innovation.

c. Enterprise/Open Standards based framework for cloud environment

d. Should have a capability to manage cross platform virtualization with cloud management platform.

e. Complete agent-less automation with life cycle management.

f. Single and Unified run-time environment.

g. The solution should be able to provide IaaS, PaaS and SaaS as per requirements

h. It should have capability to manage hybrid cloud environment.

i. Data Driven & Ready for the unpredictable growth and scale

j. Ready for DevOps & Application Lifecycle Management

The MSI needs to develop and propose a detailed services in the technical proposal and the same would be discussed and finalized between the successful MSI and CRID. A non-exhaustive list of services to be included in-line with the vision of CRID is furnished below for reference. The servicesshould contain (but not limited to following), the details of which shall be incorporated at the time of signing of actual agreement:

a. Contain a set of cloud services that an end user can request (through a web self-service portal).

b. Act as the ordering portal for cloud end users, and service-level commitments and the terms and conditions for service provisioning.

c. Also be used as a demand management mechanism, directing or incentivizing customers toward particular services or service configurations or away from legacy or declining services, as well as making sure of alignment with governance and standards through default configurations and service options.

d. Have a self-service look and feel; that is, it provides the ability to select service offerings from the cloud service catalogue and generate service requests to have instances of those offerings fulfilled.

e. Serve as the provisioning interface to automated service fulfillment using a cloud orchestration subsystem.

The MSI would develop an optimum list of servicesthat maximizes the alignment of infrastructure capabilities with business/application requirements while delivering the best value for the line departments / end customers. The MSI must ensure that the Hybrid cloud service development methodology used by them should be:

a. Repeatable: When a service is built for keeping in mind a set of departments / customers, the process could be taken and repeated for multiple customers.

b. Measurable: Service items should also be measurable in order to track usage of resources department/ VM/ application wise as well as managed for availability and performance.

c. Comprehensive:Service list should encompass all the possible combinations of infrastructure capabilities as well as different deployment requirements.

d. Scalable: To enable services provided to scale up or down according to market and end-user requirements. It should enable horizontal and vertical scaling requirements of the services provided through transparent integrated automation.

e. Flexible: To accommodate new and changing service requirements for end customers and implications on the IT services.

High level ICT infrastructure architecture:

Basic Infrastructure such as Building, server farm area, Raw Power etc. to cater to 34 numbers of racks is available along with the other utility areas. The Data Centre is established in building with pre-fitted Server and Network racks. Telecom racks are also provided by respective ISPs.

The ICT infrastructure for SDC-Chandigarh will require various set of ICT components for running their applications. The MSI is responsible to Supply, Install, Configure, Test, and maintain the entire solution for approx. 34 racks for a period of five years. The MSI should propose only one solution that is in accordance with the tender specifications.

The following is a broad list of categories of components that the MSI is expected to supply, install, configure, and testthe BoQ items

a. Computing Infrastructure such as Servers, Hypervisor etc,.

b. HCI Cloud node server Infrastructure

c. Network Infrastructure such as Backbone Core Switch, Routers and ToR switches, L3/L2 Switches, GSLB, SLB, etc. and ensure implementation of SDN and micro segmentation in Spine Leaf Architecture etc..

d. Security infrastructure such as Firewalls, Anti-APT, WAF, IPS, EDR, HIPS, Anti-virus etc.,

e. Centralized Enterprise Management Solution, Patch Management, Antivirus and Cloud Management – Orchestration layer (On premise Service offering)

f. Enterprise Class Storage Area Network along with Enterprise Class Storage system, SAN switches, Virtual Tape Library, Purpose Built BackupAppliance etc.

g. Operation and maintenance Services for a period of 5 years after go-live

The above list is indicative, though the MSI will be required to provide an infrastructure which is scalable and provides for next generation latest technologies like virtualization, cloud computing, Orchestration etc. The MSI is free to add any additional components that are deemed necessary for providing the overall solution as a whole.

The MSI should also consider the following while proposing the solution:

i. The MSI should ensure that all the peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to the devices, equipment, accessories, software, licenses, tools, etc. should also be provisioned according to the requirements of the solution.

ii. CRID will not be responsible if the MSI has not provisioned for any components, subcomponents, assemblies, sub-assemblies as part of bill of material in the bid. The MSI will have to provision to meet the solution requirements, the same at no additional cost and time implications to CRID.

iii. "The MSI should ensure there is 24 x 7 x 365 comprehensive onsite manpower supports for a period of 2 years in order to perform operation and management for all ICT components as per scope of the RFP after go-live. MSI will provide all warranty/support from all respective OEMs till the scope of project after go-live. The warranty of 5 years of all the equipment/ software shall start from the date of Go-Live of complete solution i.e. after performing SDC, near line BCP & Far DR Drills to check functionality." The MSI shall involve respective OEM for tried and tested global best practices at the time of commissioning and shall involve OEM as and when required in O&M phase.

MSI and OEM shall provide 5 years On-site comprehensive warranty support after Go Live acceptance**.** If the same is de-supported by the OEM for any reason what so ever the MSI shall replace it with an equivalent or better substitute from the same OEM that is acceptable to CRID without any additional cost to the CRID and without impacting the performance of the solution in any manner whatsoever. Any components, sub-components, assemblies, sub-assemblies (i.e., server, storage, OS) required for installation of EMS, Orchestration, backup, patch management, antivirus or any other software/management software needed for Data Centre ICT infrastructure will be provided by MSI without any additional cost.

The Project design should take into consideration following guiding principles:

a. **Transformational Nature of Monitoring**- All monitoring tools should look to fully embrace mobile adoption, online authentication, etc. to transform the processes completely and offer wider choice to interact directly considering the best security practices. It is critical that project design should be aligned to larger trends and designed for next decade rather than past.

b. **Use of Open Standard for evolving Technology:**The entire system would be built to open architecture (standards, open API, plug-n-play capabilities like virtual environments, creating sandbox), components coupled loosely to allow changes in sub- system level without affecting other parts Use of the latest & best available standards to avoid locking in obsolescent technologies simulated services environment can help agencies to save cost, infrastructure and time in testing multiple application integrations. Large integrated systems of SDC operations should be designed to get the best cost and performance advantages of natural technology curve (constant increase of speed and decrease of cost), architecture should be open and vendor neutral, and designed for horizontal as well as vertical scale-out. The technology shall scale linearly and shall have the provision to infuse new technologies without any disruption to running environment. It shall support hardware agnostic and hypervisor agnostic so that we are not bind or dependent on buying a particular hardware of virtualization solution.

c. **Sustainable & Scalable Solution**- Important technical components of the architecture must support scalability to provide continuous growth to meet the growing demand of the SDC without adversely affecting the response time and throughput of the system. Main technology components requiring scalability are storage, bandwidth, computing performance (IT Infrastructure). The architecture should be scalable (cater to increasing load of internal and external users and their

transactions) and capable of delivering high performance till the system is operational. In this context, it is required that the application and deployment architecture should provide for Scale-Up and Scale out on the Application and Web Servers, Database Servers and all other solution components. The expectation is that the system should sustain at least 7 years from GO-Live.

d. **Availability -** Components of the architecture must provide redundancy and ensure that, there are no single point of failures in the key project components. The systems need to be configured to mask and recover with minimum outage. MSI shall make the provision for high availability for all the services of the system. Redundancy has to be considered at the data centre components level and offering system High Availability and failover.

e. **Manageability -** Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the scalability of the system.

f. **Interoperability -** Keeping in view the evolving needs of interoperability, especially the possibility that the solution shall become the focal point of delivery of services, and may also involve cross-functionality with the other projects of other departments / businesses in future, the solution should be built on Open Standards. Operating systems and storage technologies from several vendors must interact well with each other. These systems should also support the open architecture solutions where information/ data can be ported to any system, whenever desired. The standards should be of leading industry and as per standards mentioned at Annexures.

g. **Convergence** - CRID has already initiated many projects which have state of the art infrastructure, hence it is imperative that all infrastructure created under the project shall be leveraged for maximum utilization. MSI is required to ensure that such infrastructure will allow for accommodation of equipment's being procured under other projects. The procedure for utilization of the infrastructure will be mutually agreed between the CRID and MSI.

h. **SLA Monitoring Tools -** The MSI should be able to measure and monitor the performance of the deployed infrastructure and all SLAs set out in this RFP. More importantly, it should be possible to monitor in REALTIME for each day, month, and year, through appropriate tools and MIS reports using tools/appliance procured through this RFP for management, monitoring & maintenance. The infrastructure management and Monitoring System shall be used by MSI as well as CRID team to monitor the infrastructure (both IT and Non-IT) hosted at the Data center, Near line DC and DR site.

i. **Cyber Security -** The Data Centre must provide an end-to-end security blanket to protect applications, services, data and the infrastructure from intentional, unintentional or malicious attacks or theft from external (through internet) and internal (through intranet and or physical) hackers/malicious intent.

    a) Such attacks and theft should be controlled and well supported using next generation cyber security appliances e.g. DDOS, Firewalls, IPS, WAF, Anti-APT HIPS systems and infrastructure protection mechanisms.

    b) Furthermore, all the system logs should be properly stored & achieved for future analysis and forensics whenever desired. It should be note that at different layers of security the make/model of the similar appliances should be different.

j. **SOC**: The Data Centre will operate Cyber Security Operation Centre for all infrastructure installed and commissioned comprising the following:

    i. Ability to protect critical business and customer data/information, demonstrate compliance with relevant internal guidelines, country regulations and laws

    ii. Ability to provide real-time/near-real time information on and insight into the security posture of the Critical Application Hosted in HSDC

    iii. Ability to effectively and efficiently manage security operations by preparing for and responding to cyber risks/threats, facilitate continuity and recovery

iv. Ability to know who did what, when, how and preservation of evidence

v. Integration of various log types and logging options into a Security Information and Event Management (SIEM) system, ticketing/workflow/case management, unstructured data/big data, reporting/dashboard, use cases/rule design (customised based on risk and compliance requirements/drivers, etc.), etc.

vi. C-SOC should be able to monitor the logs of various network activities and should have the capability to escalate any abnormal / undesirable activities.

vii. Key Responsibilities of C-SOC could include:
   a. Monitor, analyse and escalate security incidents
   b. Develop Response - protect, detect, respond, recover
   c. Conduct Incident Management and Forensic Analysis
   d. Co-ordination with all relevant stakeholder of critical application hosted in HSDC/external central agencies like NCIPC etc.

viii. MSI to ensure that there should not be any conflict of interest for any network and security devices with SOC system that are to be installed under scope of this project without affecting the quality & performance of the services.(Refer Annexure-17)

Note:-

1. The preparation of SOC is already mentioned above in which prospective MSI will ensure the following but not limited to:

a. Video wall installation and commissioning along with all required Hardware/Software/cabling, video wall controller required for SOC including any kind of associated equipment/software etc.

b. Requisite structured LAN cabling (UTP as well as FOC) including switching as well as any electrical/cabling work in SOC room to require to make SOC environment visibly professional.

c. Layout and location will be shared to selected MSI

Indicative Logical Schematic of HSDC

Following is an indicative schematic of the Data Centre design architecture (figure-3) showing the major ICT components that are to be provisioned by the MSI. Racks will be loadedwith network, security, compute, storage, hypervisor, virtualization, orchestration etc.

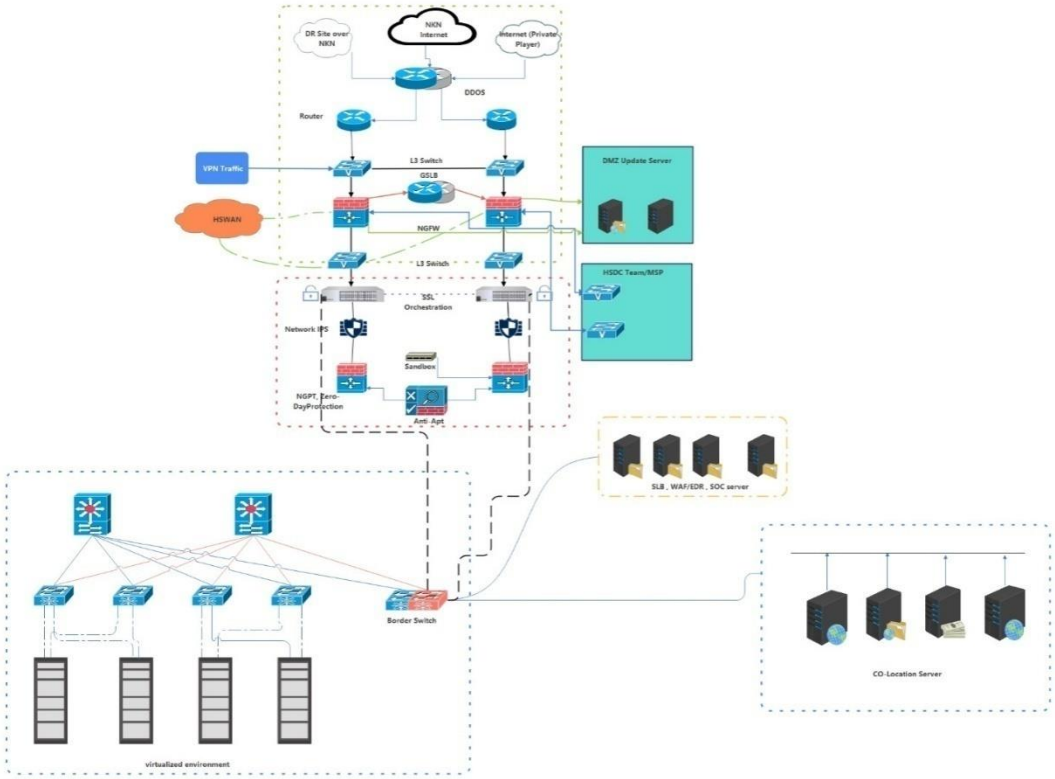


Figure-3 Logical Schematic diagram of transformed HSDC

Detailed functional requirements for HSDC 2.0:

MSI shall adopt Software defined network (SDN) based approach that is designed from the foundation to support emerging industry standards. To allows both traditional enterprise applications and internally developed applications to run side by side on a network infrastructure designed to support them in a dynamic and scalable way. Network policies and logical topologies, to be applied based on the application needs. Next Gen Data Centre should help HSDC 2.0 achieve the following functional requirements:

a. Rapid service provisioning: Services must be available in the shortest time possible.

b. Built-in Security**:** Security is one of the biggest concerns and is required by regulation. Standard tasks like firewall configurations demand a lot of effort. HSDC Architecture should provide secure zero-trust using whitelist policy model in a heterogeneous network environment

c. Consistent services and manageability on physical devices and virtual overlays: Design should support virtualization from one or more vendors. Consistency in terms of manageability, troubleshooting, and security must be present between different virtual networks and the physical network to help minimize the administrative efforts and eliminate errors.

d. Multi-vendor service integration: Data centre should have built on the technologies of multiple OEMs. It must be verified that infrastructure components (like security, load balancing, virtualization, and storage) from various OEMs operate together.

e. Network Architecture: Network should have the Close Architecture defined using Spine & leaf Switches. It must provide REST APIs from the Central management appliance/SDN Controller in

order to integrate with best of breed Management, Monitoring, Hypervisor and Cloud automation & Orchestration software.

f. Visibility: Deeper visibility in terms of latency and packet drop between VM to VM, VM to Physical server and vice versa, switching etc. should be provided. Should provide pervasive visibility of traffic across the entire data centre infrastructure, including servers and extending all the way to processes. Should provide complete visibility into application components, communications, and dependencies to enable implementation of a zero-trust model in the network.

g. Virtualization: HSDC Architecture mustintegrate with minimum of3 Virtual Machine Manager (i.e. vCenter, SCVMM, OpenStack etc.) of different Hypervisors like VMware, HyperV, KVM, and XEN simultaneously.

h. Next-Generation Data Centre Security: HSDC Security architecture should have support for network virtualization and enable Layer 4 through Layer 7 virtual network service chaining for security by using an application-centric, unified, and automated approach to security policies in the data centre infrastructure that is decoupled from the underlying network topology, supports application mobility, offers real-time compliance lifecycle management, and reduces the risk of security breaches. Solution should automate and centrally manage security policies in the context of an application using a unified security policy abstraction model that works across both physical and virtual boundaries. Should Support for dynamic policy creation, deletion, migration, and line-rate enforcement is needed to secure east-west traffic and properly manage application mobility. HSDC architecture should provide threat-focused Next Generation Firewall, IPS with best of breed industry leading state of the art firewall with the best of breed threat capabilities such as nextgeneration intrusion prevention and Advanced Malware Protection, URL filtering (web scanning), application control. Get granular application control. Protect against malware. Gain insight into and control over threats and vulnerabilities.

   I. Next Gen Intrusion Prevention System: Get the visibility, automation, flexibility, and scalability need to defeat the latest threats.

   II. Advance Malware Protection: Discover, track, contain, and block the progression of network-based advanced malware, zero-day attacks, and persistent threats.

   III. URL Filtering: Get alerts and gain control over suspect web traffic. Enforce policies on hundreds of millions of URLs in all major categories as per industry standards.

   IV. Web Application Firewall: Should protect against application layer attacks targeted at web applications. Should provide bi-directional protection against sophisticated threats like SQL injection and cross-site scripting and support OWASP application security Methodology.

i. **SAN Switching:** The SAN solution should offer highly predictable performance, scalability, Intelligence, and ease of management while protecting customer investment.

j. **Storage Infrastructure:** Centralized storage with flexible and secure configuration shall be available in the HSDC including backup facilities. The same shall be leveraged by different line departments for their data storage requirements in shared manner. The following is an indicative list of Components and Software that should be provided as part of this tender scope in DC & near line DC site:

   I. Enterprise Class Storage System (SAN, NAS, Object)

   II. Virtual Tape Library

   III. Purpose Built Backup Appliances

   IV. Backup Software

k. **Structured Cabling:** MSI has to design, lay and test the cabling requirement if any to cater HSDC Racks. Intelligent solution should be provided to manage end to end connectivity (both server rack and backbone/uplink connectivity for DC Backbone) between Backbone and ToR switches, SAN switches and server rack will be on multimode OM3/4 fibre.

l. **Cloud Environment:** MSI has to create an environment for cloud infra as per Technical Specifications. This will be act like converge infrastructure where external SAN storage, NAS storage as well as object storage will be connected in cloud environment to provide service to Haryana government departments/boards/corporation as and when required.

i. Performance: Each node in the cluster should deliver minimum IOPS at 70:30 Read: Write ratio on 8K block size as per specification.

ii. **Scalability:** Any additional node added to the cluster to augment compute or storage capacities, there should not be impact on existing node in terms of the following:

I. Zero downtime for addition of Node in virtualized environment

II. No impact of performance of all available Nodes in cluster

III. Automatic integration of node with NL BCP site

IV. The proposed cloud environment solution independently scalescompute and allocation of available storage as and when needed without any downtime.

m. **On premise Services:** MSI will provide following on premise services.All items supplied to CRID as part of contract shall be the property of CRID from day one.

i. Orchestration layer**:** A strong multi-cloud architecture including support for a range of public and private cloud platforms and to support for VMWare, open Stack, etc., Should support Software Defined Networking, Policy-based orchestration with strong API support, Life Cycle Management workflows Provisioning, Decommissioning , Extensible Capabilities to allow "Self-Management" ,workflows (Reboot/restart, Migrate, Upgrade etc).Should support Multi-Tenancy and User Management On-demand, self-service provisioning portal through which users can access infrastructure services or the infrastructure needed to support platform stacks being provisioned. Automated creation of virtual instances and assignment of virtual infrastructure through appropriate tooling to support end-to end automated provisioning should be provided. Integrated usage-tracking functionality to support departmental utilization. It shouldalso provide REST base APIs and full API-level access to all functional components of the compute service such that any function available through the user interface is available through a REST API. It also should provide Role-based policy management Administer, configure and enforce role-based policies.

ii. Enterprise Management System (EMS): Based on the latest ITIL framework, the EMS system should provide for the regular monitoring, management and reporting of the ICT infrastructure of the Data centre. It should be noted that the activities performed by the MSI will be under the supervision of CRID. The EMS system must have the following features including but not limited to following functionalities are desired by use of such EMS tools:

- Availability Monitoring, Management and Reporting
- Performance Monitoring, Management and Reporting
- Securing critical servers using Server based Access Control & recording user activity through audit logs.

iii. Network Operation Centre (NOC):Based on the latest ITIL framework, the NOC on 24x7x365 basis for the regular monitoring, management and reporting of the ICT infrastructure of the Data centre. It should be noted that the activities performed by the MSI will be under the supervision of CRID. The NOC must enable following features including but not limited to following functionalities are desired:

a. Network monitoring, management and reporting: The Bidder shall be responsible for monitoring and administering the network within the Data Centre up to the integration points with WAN. The bidder will be required to provide network related services for routers, switches, load balancer services etc.

b. Performance monitoring, management and reporting: The Bidder shall be responsible for provisioning & augmentation ports to appropriate applications and segmentation of traffic.

c. Deployment management: The Bidder would also be responsible for the overall SDN solution within the data Centreand its integration with other infrastructure orchestration solutions such as NMS, EMS and Cloud Management etc.

d. Incident management: The bidder shall co-ordinate with the Data Centre Site Preparation vendor in case of break fix maintenance of the LAN cabling or maintenance work requiring civil work.

e. Note:- There is no requirement of Civil work to set up NOC and SOC other than required for basic installation and commissioning. Information security management with backup and restore.

iv. Security Operation Centre**:**

a. Ability to Protect critical business and customer data/information, demonstrate compliance with relevant internal guidelines, country regulations and laws
b. Ability to Provide real-time/near-real time information on and insight into the security posture of the Critical Application Hosted in HSDC
c. Ability to effectively and efficiently manage security operations by preparing for and responding to cyber risks/threats, facilitate continuity and recovery
d. Ability to know who did what, when, how and preservation of evidence
e. Integration of various log types and logging options into a Security Information and Event Management (SIEM) system, ticketing/workflow/case management, unstructured data/big data, reporting/dashboard, use cases/rule design (customised based on risk and compliance requirements/drivers, etc.), etc.
f. C-SOC should be able to monitor the logs of various network activities and should have the capability to escalate any abnormal / undesirable activities.
g. Key Responsibilities of C-SOC could include:
    - Monitor, analyse and escalate security incidents
    - Develop Response - protect, detect, respond, recover
    - Conduct Incident Management and Forensic Analysis
h. Co-ordination with all relevant stakeholder of critical application hosted in HSDC/external central agencies like NCIPC etc.
i. The solution architecture deployed for the above has to address performance and scalability requirements in addition to high availability requirements. Some of the aspects to be considered are:
    - Staffing of C-SOC - is it required to be 24x7x365, in shifts, business hours only, etc.
    - Model used - Finding staff with required skills /managed security service provider with required skill set
    - Metrics to measure performance of C-SOC
    - Ensuring scalability and continuity of staff through appropriate capacity planning initiatives

Installation & Configuration of the Commissioned ICT Infrastructure

The successful MSI along with the Data Centre Site Preparation MSI would be required to undertake pre- installation planning at the Data Centre including but not limited to Rack planning,

structured cabling, SAN cabling, power points, etc. It should be noted that the activities performed by the MSI will be under the supervision of CRID.

a) The MSI shall be responsible for the delivery, installation testing and commissioning of the servers, storage, network, security, cloud orchestration, EMS/NMS, Setup of NOC/SOC and related equipment in the Data Centre.
b) The MSI shall carry out the planning and layout design for the placement of equipment in the provisioned Data Centre. The plan and layout design should be developed in a manner so as to use the resources and facilities optimally and efficiently being provisioned at the Data Centre.
c) The plan and design documents thus developed shall be submitted to CRID for approval and the acceptance would be obtained prior to commencement of installation.
d) The MSI shall carry out installation of equipment in accordance with plans and layout design as approved by the CRID.

Expectation and Consideration from MSI

a) MSI shall engage early in active consultations with the CRID Authority and other key stakeholders to establish a clear and comprehensive project plan in line with the priorities of all project stakeholders and the project objectives.
b) Study the existing IT & Non-IT Infrastructure to understand the existing technology adopted.
c) MSI shall judiciously evaluate the resources and time planned for undertaking the current state assessment, given the overall timelines and milestones of the project.
d) MSI shall be responsible for supply of all the Products/equipment such as optical fiber cables/patches, Network, Hardware, Software, Devices, etc. as required to integrate supplied ICT infrastructure indicated (but not limited to) in the tentative Bill of Materials included in the RFP and their appropriate quantity & capacity.
e) MSI shall be responsible for supply of passive components required to commission the infrastructure enlisted in the Bill of Materials of the RFP viz. Housings, Fiber Patch Cords, Racks etc. associated minorCivil work required for the site shall be undertaken by the MSI.
f) Validate / Assess the re-use of the existing infrastructure if any within Authority site.
g) Supply, Installation, and Commissioning of entire solution at all the locations.
h) MSI has to provide Enterprise version for all Open-source software. No community version will be accepted.
i) MSI shall establish high availability, reliability and redundancy of all equipment and its power supply to meet the Service Level requirements. No equipment will be accepted without redundant power supplies.
j) MSI shall be responsible for up-gradation, enhancement, and provisioning additional supplies of network (including active / passive components), hardware, software, etc. as requisitioned by Authority.
k) MSI shall ensure that the infrastructure provided under the project shall not have an end of Sale within 18 months from the date of bidding.
l) MSI shall ensure that any product supplied under this RFP shall not be declared end of support (EOS) by OEM for at-least 7 years from Go-live (i.e. 5 years under warranty and 2 years post warranty support in case if any product is declared EOS during the mentioned 7 years MSI shall replace the product with similar or better configuration (from the same OEM) no extra cost without compromising on the performance or functionality.
m) MSI will also be responsible for installation and commissioning & support of any additional software/database, being procured by CRID, which is required for successful implementation of the project.
n) MSI shall ensure compliance to all mandatory government regulations as amended from time to time.
o) The MSI shall ensure that all the peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to devices, equipment, accessories, patch cords (fiber), cables, software, licenses, tools, etc. are provided according to the requirements of the solution.
p) Authority shall not be responsible if the MSI has not provisioned some components, sub-

components, assemblies, sub-assemblies as part of Bill of Materials in the RFP. The MSI shall have to provision these & other similar things to meet the solution requirements at no additional cost and time implications to Authority.

q) All the software licenses that the MSI proposes shall be perpetual software licenses along with maintenance, upgrades and updates for the currency of the contract. The software licenses shall not be restricted based on location and Authority shall have the flexibility to use the software licenses for other requirements if required. All licenses should be in name of "CRID, Government of HARYANA"

r) MSI should ensure to implement/provide AD/LDAP and necessary certificate if required without any cost to CRID .CRID will procure separately necessary licenses of operating systems (Windows Data Centre Edition as well as RedHat Linux OS) for compute infrastructure to be installed and commissioned in the scope of this RFP. MSI will ensure installation and commissioning of this OS installation in compute infrastructure to be installed and commissioned at HSDC, NL-BCP site.

s) The MSI shall ensure there is a 24x7X365 comprehensive onsite support for duration of the contract for respective components to meet SLA requirement. MSI is required to provide the necessary MAF (Manufacturer Authorization Form) as per the format provided in the RFP in support of OEMs active support in the project.

t) Considering the criticality of the infrastructure, MSI is expected to design the solution considering the RFP requirement of no single point of failure with high level of redundancy and resilience to meet the network uptime requirements.

u) MSI shall be responsible for periodic updates & upgrades of all equipment, cabling and connectivity provided at all locations during the contract period.

v) Although, CRID will facilitate to provide all Government approvals like, for Pollution Clearance, Fire Audit & Clearance, etc., but MSI has to coordinate with respective department and the cost/fees for the same will be reimbursed on actual to MSI or to respective department (as applicable, if any).

w) MSI is expected to provide following services, including but not limited to:
    i. Provisioning hardware and network components of the solution, in line with the proposed authority's requirements.
    ii. Size and propose for network devices like Switches, security equipment including firewalls, IPS / IDS, etc. as per the SDC requirements with the required components/modules, considering redundancy and load balancing in line with RFP.
    iii. Liaise with service providers for commissioning and maintenance of the links.
    iv. All equipment proposed as part of this RFP shall be rack mountable.
    v. Authority may at its sole discretion evaluate the hardware-sizing document proposed by the MSI. MSI needs to provide necessary explanation for sizing to the Authority.
    vi. Complete hardware sizing for the complete scope with provision for upgrade.
    vii. Specifying the number and configuration of the racks (size, power, etc.) that shall be required at SDC and Near-DR.
    viii. The MSI shall provide for all required features like support for multiple routing protocols, congestion management mechanisms and Quality of Service support.
    ix. MSI shall ensure that all networking active equipment (components) are Simple Network Management Protocol (SNMP) V3 compliant and are available for maintenance/management through SNMP from the date of installation by a Network Monitoring System.

Security Related Design Considerations

The systems implemented for project should be highly secure, considering that it is intended to handle sensitive data relating to the state and residents of the state. The overarching security considerations are described below.

a) The security services used to protect the solution shall include Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols.

b) The solution shall support advanced user authentication mechanisms including digital

certificates and biometric authentication.

c) Security design should provide for a well-designed security of physical and digital assets, data and network security, backup and recovery and disaster recovery system.
d) The solution should provide for maintaining an audit trail of all the transactions and should also ensure the non-repudiation of audit trail without impacting the overall performance of the system.
e) The overarching requirement is the need to comply with ISO 27001 standards of security.
f) A secure solution should be provided at the hardware infrastructure level, software level, and access level.
g) Authentication, Authorization & Access Control:2 factors (User ID Card and Biometric or OTP based) security mechanisms should be implemented to enable secure login and authorized access to SDC.
h) Appropriate mechanisms, protocols, and algorithms necessary to protect sensitive and confirmation data and information both during communication and storage should be implemented.
i) Information security policies and standards to be used as prescribed from Government of India.
j) Role based access for all the stake holders to be implemented to access and use the system.
k) Data alterations etc. through unauthorized channel should be prevented.
l) Build a complete audit trail of all activities and operations using log reports, so that errors in system –intentional or otherwise – can be traced and corrected.
m) Access controls must be provided to ensure that the system is not tampered or modified by the system operators.
n) From a network security perspective all information that flows on the network should be encrypted to ensure safety and privacy of confidential data. The devices at each endpoint of the network should be authenticated (using mechanisms based on attributes one of which could use passwords). The authentication system so used on these endpoint devices should ensure that only authorized users are sending data over the network, and there is no rogue data that is sent to the control systems to generate false alarms or sabotage the systems.
o) Secured Information and Event Management system - monitoring of all networks, devices, and sensors to identify malicious traffic.
p) Activities such as anti-spoofing (no one should be able to masquerade for inappropriate access), anti-sniffing (no one should be able get data and interpret it), anti-tampering (no one should be able to put/change data which was not meant to be put/changed) should be taken care for data in transit, as well as data at rest, from internal and external threats.

ISMS Services and activities

MSI must ensure that each service and activity given below or as identified in due course for different processes under the ISMS should be defined, documented and managed with roles and responsibilities. Also, proper SoPs should be maintained for onboarding of new resources in quick time.

Information protection

Antivirus and Malware Protection

Incidents remediation, Antivirus Infrastructure Management, Endpoint Security, Web and Email Security, External Storage devices, Measures and deployment, Measures Effectiveness

Encryption

Full Disk Encryption, Certificates Management (for websites and systems access), Mobile Device Management (If required)

Networks

Firewall Management, Rules review and recertification, Security Posture Management, Firewall System Acceptance Test, Firewall Penetration Testing (Audit)

Identity and Access Management (Onboarded Applications and Infrastructure)

Certification of Users and Compliance Monitoring for Access controls and Privileged Id transitions. HSDC ensures that the users' matrix to their applications and systems, desired security controls met and User Department ensures that right access is provided to right information.

Applications User Access Control (If required)

Manage access permissions

Infrastructure Access

Manage Administration permissions

Certificates

Administer certificates permission, Users Matrix, access review to applications and systems

Privilege Access

System and security Administration

Monitoring & Response

Security Monitoring

System logs and events, DB Activity Monitoring, Restricted user Access, session activities, Host based Intrusion

Data Leakage Management (Data at rest and Data in motion)

Operates and administers centralized data leakage reporting and 1st level monitoring of activities on behalf of departments. The targets could be Application, File and Database Servers and Network

Incident Response

Handling of cyber security incidents and imminent cyber threats by directing the stakeholder or user department or the owner of the resource to respond within SLA.

Investigations and acquisition

Provide technical expertise and coordination for the acquisition of forensics evidence and investigation of security events.

Risk and Compliance

Asset Risk Assessment, systems acceptance, security scanning (Application and code), Vulnerability Assessment (Application and Infrastructure), Third party System Audits

Policy and Awareness

Policies, procedures and guidelines, policy management, policy assessment, policy compliance

Compliance to Standards & Certifications

a) For a large and complex set up such as the Project, it is imperative that the highest standards applicable are adhered to. In this context, MSI will ensure that the entire Project is developed in compliance with the applicable standards.
b) During project duration, MSI will ensure adherence to all below standards & certifications or latest for compliance as provided below:

Sr.No.	Component/Application/System	Prescribed Standard
1.	Information Security	ISO 27001:2022
2.	Business Continuity Management (Security and Risk resilience)	ISO 22301:2019
3.	Service Management	ISO 20000 latest specifications
4.	Project Documentation	IEEE/ISO/CMMi(wherever applicable) specifications for documentation

c) Apart from the above MSI, need to ensure compliance of the project with Government of India IT security guidelines including provisions of:
   i. The Information Technology Act, 2000 and amendments thereof and
   ii. Guidelines and advisories for information security published by CERT-In/MeitY (Government of India) issued till the date of publishing of tender notice. Periodic changes in these guidelines during project duration need to be complied with.

d) Quality Audits
   i. CRID, at its discretion, may also engage independent auditors or ask PMU to audit any/some/all standards/processes. MSI shall support all such audits as per calendar agreed in advance. The result of the audit shall be shared with MSI who has to provide an effective action plan for mitigations of observations/non-compliances, if any.
   ii. MSI should comply with all the technical and functional specification provided in various sections in this RFP document.

3.7 DETAILED SOW FOR SERVICES/DELIVERABLES

MSI shall ensure the successful implementation of the proposed SDC solutions as per the scope of services described in the RFP. Any functionality not expressly stated in this document but required to meet the needs of the CRID to ensure successful operations of the system shall essentially be under the scope of MSI and no extra charges shall be admissible for this purpose. Any requirement beyond the outlined SOW will be considered after approval of Change Request from CRID on additional cost. MSI shall implement and deliver the systems and components which are described in this RFP. MSI's scope of work shall include but will not be limited to the following broad areas.

#	Title	Expected Outcomes	Actions
1	Handing and Taking Over (HOTO) of HSDC	• Seamless transition of existing operations of HSDC from existing Data Centre Operator to new Operator • Smooth exit of existing Operator	• On boarding of new MSI • Exit management • Takeover of HSDC operations with zero disruptions • O&M • Gap Analysis
2	Infrastructure & Operations rationalization exercise would ensure the refresh of obsolete infrastructure with equivalent or higher product and consolidation of compute and rack space and continuous improvement in delivery capabilities	• Discovery and assessment of current Infrastructure including infrastructure owned by CRID • Efficient usage of rack space and HSDC resources along with resources owned by CRID • Improvement in service delivery approach	• DC Consolidation planning • Technology refresh and Capacity augmentation • EMS/NMS Implementation for HSDC & SWAN • SOC Implementation for SDC and SWAN devices • NOC for SDC devices

3	A mix of Managed Services and Private Cloud offerings	• Alignment with HSDC vision leveraging the flexible rate card based managed services and cloud offerings. • Quick and on-demand service provisioning for Line Departments aligning with the strategic goals of CRID • Gradual migration of Line Department applications and full control in HSDC resources along with resources owned by CRID	• DC Consolidation • Implementation, Integration of Private Cloud and scaling • Implementation of transformed Helpdesk • Consultative migration of Line Department Applications from Co-Lo to Cloud. • Application Deployment and Management Support
4.	Centralized SDC Service Desk & self-service portal	• KPI based operations and management • Transparent and efficient model with visibility to line departments • Quick provisioning	• Helpdesk Transformation • Email, phone, based response and resolution

The minimum specified work to be undertaken by the MSI for setting up and operating the SDC has been categorized as under:

a) Phase I: Handing and Taking Over (HOTO)
b) Phase II: Supply, Installation, testing and commissioning of the ICT Infrastructure of the DC & Far DR sites. Set-up the services and processes as per the desired standards, Centralized SDC Service Desk & Self-service portal Implementation &Management
c) Phase III: Supply, Installation, testing and commissioning of the ICT Infrastructure of the NL DR BCP site.
d) Phase IV: Operations and Maintenance services for the ICT Infrastructure DC, NL DR BCP & Far DR sites for the period of 5 years.

Phases

3.8 PHASE – I: HANDING OVER TAKING OVER (HOTO)

i) MSI should understand, analyse and examine the current state of the HSDC in discussion and knowledge transfer from the current MSI, Composite Team, Project Consultants, CRID and other stakeholders. The process of handover has to be seamless without any disruptions to the existing services following the Exit Management Plan agreed and the Hand-Over Take-Over (HOTO) plan approved by CRID.

ii) The complete handing over taking over (HOTO) activity will be done by the existing operator to the new operator as a transition sub-project. The transition period will be maximum of 30 days or as per the agreed aforementioned HOTO plan. The HOTO activities should be jointly identified by the selected MSI, current MSI and CRID. There will be a team comprising of new and existing service provider for completion of the identified activities.

Note:

It is expected that the team involved in HOTO process must lead the team deployed in the "Operation Man Power required during HOTO shadowing" for NOC and BMS related activities and Project Manager is expected to supervise all activities including Helpdesk. This Shadowing shall continue till confirmation from the MSI or till the delivery of ICT Infrastructure Under the Scope of this RFP, whichever is earlier.

iii) The selected MSI will depute a Transition Team for HSDC to take over the identified activities (knowledge transfer, asset transfer, operations transfer, etc.).

iv) MSI should perform site survey to verify the inventory details provided by current

MSIand Composite Team with the actual on-site inventory. A report on site survey should be submitted to CRID highlighting the discrepancies in the form of GAP report.

v) Site survey should be done for the entire network, inclusive of active (routers, switched, server, storage, security devices etc.) as well as passive (fibre/ copper cables, racks, cabinets, Cooling Systems (HVAC) , BMS etc.) elements. All data must be matched with asset list will be provided to successful bidder.

vi) The site survey report should enlist the details about the assets and their working status (working, not working, end of life, etc.), status of software's (like; license expired, license expiry date, license valid till date etc.) This should include all IT and non-IT equipment.

vii) MSI has to consider the current AMC period of existing Equipment as mentioned at Annexure A. MSI has to coordinate with AMC Providers for smooth operations of SDC as per SLA during the period between HOTO and FAT, in case that equipment is not replaced/upgraded as per this RFP's obligations or for any delay in commissioning due to any reason. MSI has to ensure smooth operations of the SDC till the end of O&M and have to make AMC & support arrangements for all IT & Non-IT equipment provided in this RFP and for pre- existing Non-IT equipment, which are not replaced under this RFP.

Note:-

Operation and management of all Non IT infrastructure (UPS, Air conditioner System, surveillance system, Copper earth and electrical wiring , LAN cabling, VESDA, firefighting system etc. provided at site are responsibility of bidder.

viii) MSI should undertake takeover of equipment and operations from the existing MSI with proper due diligence. The overall facilitation and moderation of the HOTO would be the responsibility of CRID. The current MSI will provide the following to the selected MSI:

a) Current scope of work
b) A detailed documentation of the transfer process that could be used in conjunction with a Selected MSI including details to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer.
c) Proper communication matrix with such like MSI, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on DC project's operation as a result of undertaking the transfer.
d) Details of provisional support of contingent support to SDC project and its selected MSI for a reasonable period after transfer.
e) Entitlement for assets to be used by selected MSI for the duration of the exit management period.
f) Information relating to the current services rendered and performance data relating to the performance of the services; Documentation relating to State Data Centre Project's Intellectual Property Rights; any other State Data Centre project data and confidential information; all current and updated SDC Project data as is reasonably required for purposes of the SDC Project or for transitioning of the services to successful MSI in a readily available format.
g) All other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable the Client and its nominated agencies, or its selected new MSI to carry out due diligence in order to transition the provision of the Services to Client or its nominated agencies, or its replacement Successful MSI (as the case may be).

The MSI should ensure that no downtime of services is attributed due to takeover. The takeover of HSDC should include:

a) Process, Policies & Guidelines
b) Inventory & Assets details (IT, Non-IT and Utilities)
c) Operations, Maintenance and Management of HSDC responsibilities
d) Data Privacy responsibilities

The MSI would be provided with the detailed exit management plan submitted by the Existing MSI to align their activities for HOTO and ensure completion of same within given time days or less.

The deliverable for completion of this phase would be the sign off of HOTO Report from CRID or its nominated agency.

Phase – II & III: Supply, Installation, Testing & Commissioning of ICT Infrastructure at DC , Far DR Site& Near line BCP site

Haryana State Data Centre-Chandigarh, is envisioned as the 'Shared, reliable and secure infrastructure services centre for hosting and managing the e-Governance Applications of the Haryana Government and its constituent departments'. HSDC is envisaged to establish a robust infrastructure to enable the Government to deliver the services quickly and effectively to its stakeholders. The proposed State Data Centre shall provide the access to the e-Governance applications & Services to Government employees through Intranet and to the citizens through public Internet/CSCs etc. Through such a Shared Service Centre implemented and managed by a competent Implementation MSI, the individual departments can focus more on the service delivery rather than on the issues surrounding the Infrastructure.

The objective is to provide logically unified and shared infrastructure flexible enough to rapidly respond to Infrastructure requirements and also accommodate future technology enhancements, Distributed applications, database applications running on bare metal, virtualized applications running in multi-hypervisor environments, and cloud-based applications that are available on demand all impose different demands on infrastructure.

MSI to establish centralized hybrid cloud environment that will be used to host multiple applications with simplified operations and increased application responsiveness to support a new generation of distributed applications while accommodating existing virtualized and non-virtualized environments.

MSI need to design HSDC Architecture as per design considerations mentioned in **Section-2** of this RFP to deliver the following:

a) SDC to deliver IT as a service starting with Hosting, Co-location, IaaS, PaaS and SaaS.
b) Deliver responsive IT based services to CRID customers/ departments on demand at scale
c) Deliver reliable User Experience.

Inception Phase

After signing of contract, the MSI needs to deploy local team (based out of CRID) proposed for the project and ensure that a Project Inception Report is submitted to CRID which should cover following aspects:

a) Names of the Project Team members, their roles & responsibilities and deliverables
b) Approach and methodology to be adopted to implement the Project (which should be in line with what has been proposed during bidding stage, but may have value additions / learning in the interest of the project)
c) Responsibility assignment matrix for all stakeholders
d) Risks that MSI anticipates and the plans they have towards their mitigation
e) Detailed project plan specifying dependencies between various project activities / sub- activities and their timelines
f) MSI shall conduct a comprehensive As-Is study of the existing system and infrastructure. The report shall also include the expected measurable improvements against each KPI in 'As-Is' study after implementation of solutions under this project. The benchmarking data should also be developed to track current situation and desired state.
g) MSI shall study the existing processes, functionalities, existing systems and applications including reporting requirements.
h) MSI will be responsible to propose transition strategy for dismantling of existing hardware, and setting up of new hardware without impacting the services of

HSDC. The proposed strategy should clearly provide approach and plan for implementation while ensuring minimum disturbance to the running services of the SDC with planned downtime during off hours.

Additionally, MSI should provide a detailed To-Be designs specifying the following:

a) High Level Design (including but not limited to) Cloud architecture, Logical and physical infrastructure design for all devices of HSDC.
b) Application component design including component deployment views, control flows, etc.
c) Low Level Design (including but not limited to) hardware connectivity, VM connectivity, Network flow, Application flows and logic including pseudo code, GUI design (screen design, navigation, etc.), Database architecture, including defining data structure, data dictionary for all components including Monitoring software/system to be configured in this project as per standards mentioned in the RFP.
d) Electrical power provisioning.
e) MSI shall also identify the customizations/ workaround that would be required for successful implementation and operation of the project. The MSI would be offering the products and solutions which meet the requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The MSI is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered, if it is required for meeting current & future requirements during the contract period. The MSI is fully responsible for the specified outcome to be achieved.

MSI will be responsible for preparation of detailed project plan. The plan shall address, but not limited to the following:-

a) Define an organized set of activities for the project and identify the interdependence between them
b) Resource planning and loading for each phase/activity. This must also indicate where each resource would be based during that phase, i.e. onsite at the CRID office or off site at MSI premises
c) Establish and measure resource assignments and responsibilities
d) Highlight the milestones and associated risks
e) Communicate the project plan to stakeholders with meaningful reports
f) Measure project deadlines and performance objectives
g) Project Progress Reporting. During the implementation of the project, MSI should present weekly reports. This report will be presented in the Steering Committee meeting to CRID. The report should contain at the minimum the under mentioned:
    i. Results accomplished during the period (weekly)
    ii. Cumulative deviations from the schedule date as specified in the finalized Project Plan
    iii. Corrective actions to be taken to return to planned schedule of progress
    iv. Plan for the next week
    v. Proposed revision to planned schedule provided such revision is necessitated by reasons beyond the control of MSI
    vi. Support needed
    vii. Highlights/lowlights
    viii. Issues/Concerns
    ix. Risks/Show stoppers along with mitigation
    x. Identify the activities that require the participation of client personnel (including CRID, the Program Management Unit etc.) and communicate

their time requirements and schedule early enough to ensure their full participation at the required time.

Requirement Phase

MSI must perform the detailed assessment of the business requirements and IT Solution requirements as mentioned in this RFP. Based on the understanding and its own individual assessment, MSI shall develop & finalize the Implementation plan in consultation with CRID and its representatives. While doing so, MSI at least is expected to do following:

a) MSI shall conduct a detailed survey and prepare a gap analysis report, detailed survey report of the physical and field infrastructure requirements. MSI shall duly assist the department in preparing an action plan to address the gaps.
b) MSI shall study and revalidate the requirements given in the RFP with CRID and submit as an exhaustive Implementation plan cum Design document.
c) MSI shall develop and follow standardized template for requirements capturing and system documentation.
d) MSI must maintain traceability matrix for the entire implementation.
e) MSI must get the sign off from user groups formed by CRID.
f) For all the discussion with CRID team, MSI shall be required to be present at CRID office,Chandigarh with the requisite team members.

Design Phase

MSI shall make a detailed Implementation Plan & Design document within the Time Schedule mentioned at Section- 7 for proposed solution as per the Design Considerations detailed in Section – 2, 3, 4 and all Annexures.

Deployment Phase

a) Inspection of all BOQ Items required for State Data Centre & Far DR
b) MSI shall be responsible for Planning, Designing, Installation till final acceptance by the Purchaser. MSI shall also make sure that proposed solution should work seamlessly as per tender requirement as an integrated solution which has multiple OEMs/ items. Documentation related to Plan, Design and proposed UAT process of the overall solution to be submitted on official letter head along with Bid.
c) MSI to ensure and assure the setup, installation & commissioning of all the BoQ items and integrate them in the total solution as per the best industry practices and/ or recommended by respective OeMs and utilize the support of OeMs on need basis.
d) Purchaser might require OEM enterprise support in order to ensure the quality of work and solution deployed; as such, MSI shall ensure any such support without any additional cost to the purchaser.
e) MSI should provide the overall program management and MSI to ensure that the solution, which may include multiple technologies from various OEM, to work together seamlessly as per the proposed solution design. The seamless integration with all devices with desired performance would be the responsibility of MSI in consultation with OEMs and their respective products offered in the solution.MSI to submit integration document containing details of individual products deployed in the solution.
f) After completion MSI should provide industry best practice document of the deployment to validate the design.
g) After successful commissioning and FAT completions of the project MSI to ensure complete handover and knowledge transfer to CRID for operations and management.

Support Phase

a) The MSI should further ensure that a robust support model is put together along with OEM Certified Engineer (wherever applicable or as per demand by the purchaser) in such a way that the data centre runs with the level of availability it is designed for and with a predictable restoration time in case of any failures.
b) Once deployed, MSI should ensure to complement the support model put together in such a way that MSI will provide optimization services to maintain the data centre & deliver the

desired availability goals.

c) MSI to ensure and assure the operations of the overall solution as per the best industry practices and/ or recommended by respective OeMs and utilize the support of OeMs on need basis.
d) MSI to develop a comprehensive Quarterly Services program that will provide responsive, preventive, and consultative support of all technologies for data centre needs.

Key Services:

a) The MSI shall be responsible for complete Management of the project as per RFP T&C.
b) MSI to ensure the entire infrastructure is supported back to back by OEM support services:
   i. Quality Assurance of the solution: MSI will provide respective OEM best practice document to CRID for review of the solution and methodology being deployed by MSI. In case CRID is not satisfied with offered solution then expert review services of respective OEMs will be required to review same without any additional cost. The aim of the review is to ensure the appropriateness of the Solution as configured, developed and deployed.
   ii. Solution Capability: CRID would choose the system based on what it is capable of offering to meet its business requirements. The experts from the MSI team are expected to support CRID during the project to ensure that capabilities of the DC, Near Line DC and Far DR sites infrastructure are deployed effectively.
   iii. Structured Cabling: MSI has to commission new Structured cabling for all new Racks in SDC from top of the Racks in consultation with CRID team if required.

   The reviews are expected to take place at the following stages of the project implementation.

   a. Technical Solution Preparation
   b. Solution Implementation
   c. Final Preparation for Go-Live
   d. Stabilization period
   e. Final Go Live

Installation &Commissioning of Near Line DCat STPI, Mohali as per RFP

MSI has to install & commission near line BCP site at STPI, Mohali as per RFP BOQ which will be operational either in Active-Active mode or Active Passive mode based on need of application criticality and provide BCP Services. CRID will install and commission their ICT infrastructure at STPI Mohali in Colocation basis where Cooling, Electricity, Physical Security and any other Non IT services like BMS services will be provided but STPI Mohali but MSI need to coordinate in case of problems with these colocation services to STPI Mohali to get the problem rectified.

CRID will take ISP link as well as NKN link at STPI Mohali which will be maintained by MSI in case of any problems or coordination required.

Rest of scope of operation & maintenance service will remain same considering HSDC at primary DC site sand STPI Mohali as Secondary DC site.

MSI need to perform DR Drill to ensure that DR will work as per defined norms in RFP.

AMC of Existing Hardware/Software

Currently, most of the existing hardware and software are under ATS/OEM support. CRID will take care of AMC of all existing Infrastructure till Go-Live of the project. CRID. CRID will ensure to continue AMC/CAMC or ATS of usable infrastructure either Hardware, Software or Non-IT infrastructure but MSI will be responsible to up and running this infrastructure coordinating with respective OEMs/ASP of this Hardware & Software as per defined SLA.

Note:- Operation and management of all Non IT infrastructure (UPS, Air conditioner System, surveillance system, Copper earth and electrical wiring , LAN cabling, VESDA, firefighting system etc. provided at site are responsibility of bidder.

MSI will ensure that Cloud Setup, Network & Cyber Security Implementation including setup of

SOC, EMS/NMS related Installations and Master System Integration (MSI) activities along with the SOPs & Documentation will be performed by certified domain expert of MSI.

Centralized SDC Service Desk & Self-service portal

The selected MSI would be responsible for transforming the existing helpdesk into Centralized SDC Service Desk & self-service portal which would bring in:

- KPI based operations and management
- Transparent and efficient charge-back model with visibility to line departments
- Quick provisioning capabilities

The Centralized SDC Service Desk shall undertake the following activities:

a) Log issues / complaints related to ICT infrastructure at the Data Centre and issue an ID number against the issue / complaint.
b) Assign severity level to each issue / complaint so as to maintain categorization and differentiate the criticality of the incident via the priority levels, severity levels and impact levels
c) Track each issue / complaint to resolution
d) Escalate the issues / complaints, to CRID officials if necessary as per the escalation matrix defined in discussion with CRID.
e) Analyse the issue / complaint statistics and MSI's SLA
f) Should provision for all necessary channels for reporting issues to onsite Technical team. The incident reporting channels will be the following:
    i. Email
    ii. Telephone (mobile phone alerts)
    iii. Web Based
g) Should implement a call logging system in line with the severity levels as mentioned in the SLA
h) The Centralized SDC Service Desk would be driven via Self Service Portal, modern age correlation enabled Service Desk and Email, Phone (2 Lines), and ChatBot based response and resolution.

Self Service Portal Requirements

a) The solution should provide a simple to use intuitive Web experience for SDC Cloud Administrator and User Departments / Customers
b) The solution should have self-service capabilities to allow Users Departments to log service requests to MSI.
c) The solution should use helpdesk for logging call and maintaining escalation.
d) The solution should offer service catalog listing availability of Cloud infrastructure like Virtual Machines, Physical Machines, Applications, Common Services offered by State Private cloud, etc.
e) The solution should provide comprehensive customizable service catalog with capabilities for service design and lifecycle management, a web-based self-service portal for users to order and manage services
f) The solution should provide an on-boarding mechanism for the new tenants (Department) on the cloud infrastructure that automatically creates the tenant, the tenant administrators, allocates specific resources for the tenant like storage pools, server pools, S/W packages, network pools (including VLANs, DNS, IP address spaces, etc.)
g) The solution should offer Registration, Signup, Forgot Password and other standard pages (Profile or Contact information)
h) The solution should enforce password policies and allow to personalize the look & feel and logo on the user- interface panels
i) The solution should be able to offer choice of various hardware profiles, custom hardware profile, selection of operating systems, VLAN, Storage, etc
j) The solution should automate provisioning of new and changes to existing infrastructure

(Virtual, Physical, Application or Common Services) with approvals

k) The solution should allow for implementing workflows for provisioning, deployment, decommissioning all virtual and physical assets in the cloud
l) The solution should allow easy inventory tracking all the physical & virtual assets of the SDC, and DR on Cloud. It should provide capabilities to track usage and non-compliance situations.
m) The solution should allow the ability to identify non-compliant systems (both Virtual and Physical) in terms of desired configuration (e.g. file system policy on a VM etc.) and automatically remediate the same wherever possible.
n) The solution should have Show-Back functionality (to check the usage patterns and reporting for the user department)
o) The solution should allow the users to schedule a service creation request in a future date/time; the solution should check if a request scheduled for a future time can be fulfilled and reject the request in case of projected resources shortage or accept the request and reserve the resources for that request
p) The solution should have the ability to generate customized report as well as the native ability to export to common formats
q) The solution should provide service catalog with capabilities for service offering design and lifecycle management, a self-service portal for users to order and manage services

The Help Desk services should:

a) be 24x7x365 services
b) Helpdesk Number (2 Lines) Managed by MSI, all expenses will be bear by MSI.
c) log all events or disruption of services with a ticket/docket number which will be informed to the caller/requester
d) The requests marked as a closed should be reopened by the requester within 24 hours of closing if the closure is not satisfactory.
e) follow the guidelines as per the ITIL framework
f) have a periodic feedback survey through a mail or recorded over voice on random sampled basis
g) Provide Pro-active and re-active monitoring and support. The Pro-active monitoring will include L1 and L2 support which will be from the NOC (24x7) and L3 will be the reactive support and will be provided during the normal business hours and on call basis for 24x7 support.

Commissioning & Acceptance of the Equipment

Commissioning of System

a) The MSI in coordination with OEM/OEM's Authorised System Integrator should describe in advance the tests and details of the process that will be adopted to demonstrate the correct working of the equipment supplied both individually and as an integrated system.
b) System testing schedules, formats for testing and commissioning reports and dissemination mechanism for such reports shall be drawn by the MSI in consultation with CRID.
c) It shall be the responsibility of The MSI to get pre-dispatch inspection of the goods as part of factory tests and furnish necessary certificate to CRID certifying that the goods conform to the specifications in the proposed bill of material and are in line with the mandatory technical specifications as specified in **Section- – Technical Specifications of this Tender.**
d) Commissioning of the solution shall be considered to be complete only after the following conditions have been met successfully to the satisfaction of CRID.
    i. Successful completion of Final Acceptance Tests and submission of necessary reports and certificates to CRID.
    ii. Delivery of all the items under the proposed bill of material at the designated locations of installation. Short shipment of goods will not be acceptable.
    iii. Installation and Configuration of all the components of the solutions including, but not limited to, hardware, software, devices, accessories, etc. to the satisfaction of CRID.
    iv. Successful completion of Commissioning would need to be certified by CRID and

operations shall commence only after approval of CRID.

Testing and Acceptance Criteria

a) MSI shall demonstrate the following mentioned acceptance criteria prior to acceptance of the solution as well as during project operations phase, in respect of scalability and performance etc. MSI may propose further detailed Acceptance criteria which the CRID will review. Once CRID provides its approval, the Acceptance criteria can be finalized. In case required, parameters might be revised by CRID in mutual agreement with bidder and the revised parameters shall be considered for acceptance criteria. A comprehensive system should be set up that would have the capability to log & track the testing results, upload & maintain the test cases and log & track issues/bugs identified. Solution should demonstrate the compliance with security requirements as mentioned in the RFP including but not limited to security controls in the application, at the network layer, datacenter, security monitoring system deployed by MSI.
b) Solution shall pass vulnerability and penetration testing for roll out of each phase. The solution should pass web application security testing for the portal, mobile app and other systems and security configuration review of the infrastructure.
c) MSI should carry out security and vulnerability testing on the developed solution.
d) Security testing to be carried out in the exact same environment/architecture that would be setup for production.
e) Security test report and test cases should be shared with CRID
f) Testing tools if required, to be provided by MSI.
g) During O&M phase, penetration testing and vulnerability assessment to be conducted on quarterly basis.
h) CRID will also involve third party auditors to perform the audit/review/monitor the security testing carried out by MSI. Cost for such auditors to be paid by CRID.
i) Bidder needs to provide the details of the testing strategy and approach including details of intended tools/environment to be used by MSI for testing in its technical proposal. CRID does not intend to own the tools.
j) MSI shall work in a manner to satisfy all the testing requirements and adhere to the testing strategy outlined. MSI must ensure deployment of necessary resources and tools during the testing phases. MSI shall perform the testing of the solution based on the approved test plan, document the results and shall fix the bugs found during the testing. It is the responsibility of MSI to ensure that the end product delivered by MSI meets all the requirements specified in the RFP. MSI shall take remedial action based on outcome of the tests.
k) MSI shall arrange for environments and tools for testing and for training as envisaged. Post Go-Live; the production environment should not be used for testing and training purpose. Detailed process in this regard including security requirement should be provided by MSI in its technical proposal. The process will be finalized with the selected bidder.
l) All the Third Party Auditors (TPA) as mentioned above will be appointed and paid by CRID directly. All tools/environment required for testing shall be provided by MSI.
m) STQC/Other agencies appointed by CRID shall perform the role of TPA. MSI needs to engage with the TPA at the requirement formulation stage itself. This is important so that unnecessary re-work is avoided, and the audit is completed in time. The audit needs to be completed before Go-Live. MSI needs to prepare and provide all requisite information/documents to third party auditor and ensure that there is no delay in overall schedule.
n) The cost of rectification of non-compliances shall be borne by MSI.

Final Acceptance Testing (FAT)

CRID shall review the detailed acceptance test plan (FAT). CRID would also conduct audit of the process, plan and results of the Acceptance Test carried out by the MSI. MSI would request for FAT against which CRID shall verify availability of all the defined services as per the conditions enumerated in RFP.

Commissioning shall involve the completion of the supply and installation of the required IT components / subcomponents and making the HSDC available to CRID for carrying out live Operations. Testing and Commissioning shall be carried out before the commencement of Operations.

The final acceptance shall cover 100% of the State Date Centre, after successful testing by CRID or its third- party monitoring agency; a Final Acceptance Test Certificate (FAT) shall be issued by CRID.

The date on which the Final Acceptance certificate is issued shall be the deemed date of the successful commissioning of the Project. Any delay by the successful MSI in the performance of its contracted obligations shall render the successful MSI liable to the imposition of appropriate liquidated damages, unless agreed otherwise by the CRID.

Successful implementation of SDC Applications including EMS, NMS, BMS and SOC:

Detailed test plan shall be developed by MSI and approved by CRID. This shall be submitted by MSI before FAT activity to be carried out.

a) All documentation related to SDC Project and relevant acceptance test document (including IT Components, Non IT Components etc.) should be completed & submitted before the final acceptance test to the CRID.
b) The training requirements as mentioned should be completed before the final acceptance test.
c) Successful hosting of at least two departmental applications. Details for the same shall be shared at a later date before the commencement of FAT.
d) Successful implementation of SDC Applications including EMS, BMS and NMS.
e) For both IT & Non-IT equipment's / software manuals / brochures / Data Sheets / CD / DVD / media for all the Project's supplied components should be hand over to CRID.

The FAT shall include the following:

a) All the IT hardware and software items must be installed at SDC site as per the specification.
b) Availability of all the defined services shall be verified.
c) The MSI shall be required to demonstrate all the features / facilities / functionalities as mentioned in the RFP.
d) MSI shall arrange the test equipment required for performance verification, and will also provide documented test results.
e) MSI shall be responsible for the security audit of the established system to be carried out by a certified third party as agreed by CRID.

Any delay by MSI in the Final Acceptance Testing shall render him liable to the imposition of appropriate Penalties. However, delays identified beyond the control of MSI shall be considered appropriately and as per mutual agreement between CRID and MSI.

Acceptance schedules, detailed acceptance tests, formats for acceptance reports and dissemination mechanism for such reports shall be drawn by the MSI in consultation with CRID.

The Acceptance of the solution shall be provided by CRID only after the following conditions have been met successfully to the satisfaction of CRID.

a) Successful operation of the system for 24 x 7 x 365 working.
b) Completion of all the documentation required as part of this tender and as desired by CRID to the satisfaction of CRID.

Go-Live Preparedness and Go-Live

MSI shall prepare and agree with CRID, the detailed plan for Go-Live (in-line with CRID implementationplan as mentioned in RFP).

a) MSI shall define and agree with CRID, the criteria for Go-Live.

b) MSI shall ensure that all the data migration is done from existing systems for all applications.
c) MSI shall ensure that all existing applications as annexed in the document is done from existing systems
d) MSI shall submit signed-off issue closure report ensuring all issues raised during User Acceptance Testing (UAT) are being resolved prior to Go-Live.
e) MSI shall ensure that Go –Live criteria as mentioned in User acceptance testing of Project is met and MSI needs to take approval from CRID team on the same.
f) Go-live of the application shall be done as per the finalized and agreed upon Go-Live plan.

3.9 PHASE – IV: OPERATION AND MAINTENANCE SERVICES

MSI will operate and maintain all the components of the HSDC **with 5 years On-site comprehensive warranty support after Go Live acceptance. O&M of manpower support is for first 2 years.** During O&M phase, MSI shall ensure that service levels are monitored on continuous basis; service levels are met and are reported to CRID. After Go-Live, if any system/sub-system/appliance that is deployed during the O&M phase must be added in the System only after proper induction procedures are followed including hardening and security testing. MSI needs to implement suitable Performance Improvement Process (PIP) in the project.

PIP program applies to all the processes of HSDC project. MSI need to submit its detailed approach for PIP in its technical proposal. Every process and procedure implemented in this project must be reviewed and updated by MSI at least on annual basis from the Go-Live Date. All the manpower engaged for O&M support of the project should be citizens of India. MSI will ensure that at no time shall any data of HSDC be ported outside the geographical limits of the country.

Following is the summary of operations and maintenance services to be provided by the MSI: It should be noted that the activities performed by the MSI will be under the supervision of CRID.

a) The MSI shall provide comprehensive onsite support to CRID on a 24 x 7 x 365 basis to ensure uptime for the ICT infrastructure solution at the Data Centre in accordance with the Service Level Agreement mentioned as part of this RFP.
b) The MSI shall commit to provide all necessary manpower resources onsite (CRID) to resolve any issues/incidents and carry out required changes, optimizations and modification.
c) The MSI shall assign onsite manpower resources on a 24 x 7 x 365 basis to diagnose, troubleshoot and resolve issues related to the Data Centre services. The onsite support staff should possess capability for supporting the equipment and components proposed, but not limited to undertaking preventive and break-fix maintenance, troubleshooting, resolving problems, tuning, etc. The MSI shall also provision for necessary offsite support to ensure continuity of operations for CRID, if required. Cost of such support will be borne by MSI.
d) The MSI shall provide comprehensive onsite warranty on a 24 x 7 x 365 basis for a period of 5 (Five) years from the date of Go Live. The warranty period shall commence from the date of acceptance (FAT) of the entire system.
e) Besides the ICT infrastructure procured for HSDC Chandigarh as part of this RFP/Tender, The MSI shall also provide Installation and Configuration and on-going maintenance services for the infrastructure hosted by other government agencies. The government agencies can either collocate their infrastructure or host it under the managed services arrangement with their respective vendor. The MSI shall provide 24x7x365 onsite support to such infrastructure also.
f) During the scope of work of this RFP, any additional IT infra (apart from this RFP BOQ) or software etc. procured by CRID in order to enhance the productivity of the project (like Database Server licenses, BMS enhancement, UPS, additional servers etc.) shall also be under the scope of MSI.
g) The MSI shall provide all necessary training to the CRID officials for successful functioning of the Data Centre operation and management.

ICT Infrastructure Support and Maintenance

ICT infrastructure includes servers, storages, back up, networking, load balancers, security equipment, operating systems, database, enterprise management system, help desk system and other related ICT infrastructure in the RFP required for running and operating the envisaged system. MSI shall define, design, develop, implement and adhere to all stages IT Service Management (ITSM) processes aligned to ITIL framework for all the IT Services defined and managed as part of this project.

Onsite support

The MSI should ensure that the entire ICT Infrastructure solution is operational in accordance with the stipulated service standards in Service Level Agreement.

a) The MSI along with all the associated OEMs should commit to provide all necessary resources and expertise to resolve any issues and carry out required changes, optimizations and modification to ensure that the ICT infrastructure is operational in accordance with the stipulated service standards in Service Level Agreement.
b) The MSI should provide comprehensive onsite warranty on a 24 x 7 x 365 basis for a period of 5 (Five) years from the date of acceptance on all ICT infrastructure solution provided as part of scope of work. The warranty period shall commence from the date of acceptance of the entire system as described in RFP

Warranty support

a) MSI shall provide comprehensive and on-site warranty for 5 years from the date of Go-Live for the infrastructure deployed on the project. MSI need to have OEM support for these components and documentation in this regard need to be submitted to CRID on annual basis.
b) MSI shall provide the comprehensive & onsite manufacturer's warranty in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. covered by the RFP. MSI must warrant all hardware, equipment, accessories, spare parts, software etc. procured and implemented as per this RFP against any manufacturing defects during the warranty period.
c) MSI is responsible for sizing and procuring the necessary hardware and software licenses as per the performance requirements provided in the RFP. During the warranty period, CRID can ask MSI to replace or augment or procure higher-level new equipment or additional licenses/hardware at the Unit rate quoted in Commercial Bid or at agreed rates, whichever would be lesser in case the procured hardware or software is not enough or is undersized to meet the service levels and the project requirements.
d) During the warranty period MSI shall maintain the systems and repair/replace all the supplied equipment's at the installed site including all consumables, at no charge to CRID, all defective components that are brought to the MSI's notice.
e) The MSI shall carry out Preventive Maintenance (PM) of all hardware and should maintain proper records for such PM. The PM should be carried out at least once in six months as per checklist and for components agreed with CRID.
f) The MSI shall carry out Corrective Maintenance for maintenance/troubleshooting of supplied hardware/software and support infrastructure problem including network (active/passive) equipment, security and rectification of the same. The MSI shall also maintain complete documentation of problems, isolation, cause and rectification procedures for building knowledge base for the known problems in centralized repository, accessible to CRID team as well.
g) MSI shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.
h) The MSI shall ensure that the warranty complies with the agreed technical standards, security requirements, operating procedures, and recovery procedures.
i) MSI shall have to stock and provide adequate onsite and offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met.
j) Any component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated

in the Service Level Agreement (SLA).

k) The MSI shall introduce a comprehensive Assets Management process & appropriate tool to manage the entire lifecycle of every component of SDC system.

Ongoing Operations and Maintenance Services

The MSI would be responsible for managing and maintaining the Data Centre operations on a 24x7x365 basis. It should be noted that the activities performed by the MSI will be under the supervision of CRID. Ongoing operations and maintenance of the Data Centre shall comprise of the following activities in conjunction with the indicative features required by the centralized management system as specified:

Management of SDC

MSI need to deploy requisite mix of L1, L2 and L3 resources (on 24X7 basis) for management of entire ICT & Non- IT infrastructure deployed at SDC as per the requirement mentioned at Section – 3.3.12.

During operations phase the MSI needs to submit proof of renewal of support for all IT infrastructure products and other system software's for whom it is mandated to have OEM support.

This needs to be submitted on an annual basis and needs to be verified before release of 2nd quarter payment of each O&M year.

Data Centre Certifications

MSI to get following certifications within 3 months from Go-Live and all related cost for the certification will be borne by MSI:

i. ISO 27001
ii. ISO 9001
iii. ISO 20000

Cost of sustenance audit for above certification shall be responsibility of the MSI for the entire contract period.

System Maintenance and Management

Certain minimum deliverables sought from the MSI with regards to System Maintenance and Management are provided below: -

a) The MSI shall be responsible for tasks including but not limited to setting up servers, configuring and provisioning storage space, account management, performing periodic backup of data and automating reporting tasks, and executing hardware and software updates when necessary with approval of CRID. It should be noted that the activities performed by the MSI may also be reviewed by CRID.
b) The MSI shall provision skilled and experienced manpower resources to administer and manage the entire ICT Infrastructure solution at the CRID Data Centre.
c) On an ongoing basis, the MSI shall be responsible for troubleshooting issues in the ICT infrastructure solution and coordinate with OEM if required to determine the areas where fixes are required and ensuring resolution of the same.
d) The MSI shall be responsible for identification, diagnosis and resolution of problem areas pertaining to the ICT Infrastructure and maintaining the defined SLA levels.
e) The MSI shall implement and maintain standard operating procedures for the maintenance of the ICT infrastructure based on the policies formulated in discussion with CRID and based on the industry best practices / frameworks. The MSI shall also create and maintain adequate documentation / checklists for the same.
f) The MSI shall be responsible for managing the user names, roles and passwords of all the relevant subsystems, including, but not limited to servers, other devices, etc.
g) The MSI shall be responsible for management of passwords for all relevant components and devices under his purview and implement a password change mechanism in accordance with the security policy formulated in discussion with CRID and based on

the industry best practices / frameworks like ISO 27001, ISO 20000, ISO 22301, ISO 27017, ISO 27018 etc.

h) The administrators will also be required to have experience in latest technologies like Orchestration, virtualization, and cloud computing so as to provision the existing and applicable infrastructure on a requirement-based scenario

i) The MSI shall also provide operation & maintenance services for Security Operation Centre (SOC) and will be responsible for incident management and response as per Policy & Guidelines and directions from State Government/ Government of India

j) The MSI would be to provide centralized capabilities to detect, identify, and respond to security incidents + service availability that may impact as per Government of Haryana IT infrastructure, services, and customers. The primary function would be to detect and contain attacks and intrusions in the shortest possible timeframe, limiting the potential impact and/ or damage that an incident may have by providing near real-time monitoring and analysis of suspicious events.

System Software Support and Maintenance

Application support includes, but not limited to, monitoring, troubleshooting and addressing the functionality, availability and performance issues, implementing the system change requests etc. of System Software installed in HSDC. The MSI shall keep all the system software in good working order; perform release upgrades on timely basis in consultation with CRID team. All tickets related to any issue/complaint/observation about the system shall be maintained in an ITIL compliant comprehensive ticketing solution. Key activities to be performed by MSI in the system software support phase are as follows:

1. Compliance to SLA

   MSI shall ensure compliance to SLAs as indicated in this RFP and any upgrades/major changes to the system software shall be accordingly planned by MSI ensuring the SLA requirements are met at no additional cost to the CRID.

2. Annual Technology Support

   MSI shall be responsible for arranging for annual technology support for the OEM products to CRID provided by respective OEMs during the entire O&M phase.

3. System Software Maintenance

   a) MSI shall provide unlimited support through onsite team/telephone/Fax/E-mail/Video Conferencing/installation visit as required

   b) MSI shall address all the errors/bugs/gaps in the functionality in the solution implemented by the MSI (vis-à- vis the Design Document signed off) at no additional cost during the O&M phase.

   c) All patches and upgrades from OEMs shall be implemented by the MSI ensuring customization done in the solution as per the CRID requirements are applied. Technical upgrade of the installation to the new version, as and when required, shall be done by the MSI. Any version upgrade of the software / tool / appliance by MSI to be done after taking prior approval of CRID and after submitting impact assessment of such upgrade.

   d) Any changes/upgrades to the software performed during the support phase shall subject to the comprehensive and integrated testing by the MSI to ensure that the changes implemented in the system meets the specified requirements and doesn't impact any other function of the SDC. Release management for system software will also require CRID approval. A detailed process in this regard will be finalized by MSI in consultation with CRID.

   e) Issue log for the errors and bugs identified in the solution and any change done in the solution shall be maintained by the MSI and periodically submitted to the CRID.

   f) MSI, at least on a monthly basis, will inform CRID about any new updates/upgrades available for all software components of the solution along with a detailed action report.

   g) In case of critical security patches/alerts, the MSI shall inform about the same

immediately along with his recommendations. The report shall contain MSI's recommendations on update/upgrade, benefits, impact analysis etc. The MSI shall need to execute updates/upgrades though formal change management process and update all documentations and Knowledge databases etc. For updates and upgrades, MSI will carry it out free of cost by following defined process.

i. Problem identification and Resolution

a) Errors and bugs that persist for a long time, impact a wider range of users and is difficult to resolve becomes a problem. MSI shall identify and resolve all the problems in the identified solution (e.g. system malfunctions, performance problems and data corruption etc.).
b) Monthly report on problem identified and resolved would be submitted to CRID along with the recommended resolution.

ii. Change and Version Control

All planned or emergency changes to any component of the system shall be through the approved Change Management process. The MSI needs to follow all such processes (based on industry ITSM framework). For any change, MSI shall ensure:

a) Detailed impact analysis
b) Change plan with Roll back plan
c) Appropriate communication on change required has taken place
d) Proper approvals have been received
e) Schedules have been adjusted to minimize impact on the production environment
f) All associated documentations are updated post stabilization of the change
g) Version control maintained for software changes

The MSI shall define the Software Change Management and Version control process. For any changes to the solution, MSI has to prepare detailed documentation including proposed changes, impact to the system in terms of functional outcomes/additional features added to the system etc. MSI shall ensure that software and hardware version control is done for entire duration of MSI's contract.

iii. Maintain configuration information

a) MSI shall maintain version control and configuration information for application software and any system documentation.

iv. Training

a) MSI shall provide training to CRID personnel whenever there is any change in the functionality. Training plan has to be mutually decided with CRID.

v. Maintain System documentation MSI shall maintain at least the following minimum documents with respect to the SDC System:
a) High level design of whole system
b) Low Level design for whole system / Module design level
c) Any other explanatory notes about system
d) Traceability matrix
e) Compilation environment

vi. MSI shall also ensure updation of documentation of software system ensuring that:
a) Functional specifications are documented
b) Documentation is updated to reflect on-going maintenance
c) User manuals and training manuals are updated to reflect on-going changes/enhancements
d) Standard practices are adopted and followed in respect of version control and

management.

All the project documents need to follow version control mechanism. MSI will be required to keep all project documentation updated and should ensure in case of any change, the project documents are updated and submitted to CRID by the end of next quarter.

System Administration

Certain minimum deliverables sought from the MSI with regards to System Administration are provided below:-

a) 24*7*365 monitoring and management of the servers in the Data Centre.
b) The MSI shall ensure proper configuration of server parameters. The MSI shall be the single point of accountability for all hardware maintenance and support the ICT infrastructure at the Data Centre. It should be noted that the activities performed by the MSI will be under the supervision of CRID
c) The MSI shall be responsible for Operating system administration, including but not limited to management of users, processes, preventive maintenance and management of upgrades including updates, upgrades and patches to ensure that the system is properly updated.
d) The MSI shall also be responsible for installation and re-installation in the event of system crash/failures.
e) The MSI shall appoint system administrators to regularly monitor and maintain a log of the monitored servers to ensure their availability to CRID at all times.
f) The MSI shall undertake regular analysis of events and logs generated in all the sub systems including but not limited to servers, operating systems etc. The system administrators shall undertake actions in accordance with the results of the log analysis. The system administrators should also ensure that the logs are backed up and truncated at regular intervals. The MSIs are advised to refer CERT-In Guidelines so as to ensure their alignment with the practices followed.
g) The system administrators should adopt a defined process for change and configuration management in the areas including, but not limited to, changes in servers, operating system, applying patches, etc.
h) The system administrators should provide hardening of servers in line with the defined security policies
i) The system administrators should provide integration and user support on all supported servers, data storage systems etc.
j) The system administrators should provide & maintain directory services such as local LDAP/AD services and DNS services and user support on all supported servers, data storage systems etc.
k) The system administrators will be required to trouble shoot problems with web services, application software, desktop/server relationship issues and overall aspects of a server environment like managing and monitoring server configuration, performance and activity of all servers.
l) Documentation with version control regarding configuration, hardening parameters, polices implemented on all servers, IT Infrastructure etc.
m) The system administrators shall be responsible for managing the trouble tickets, diagnosis of the problems, reporting, managing escalation, and ensuring rectification of server problems as prescribed in Service Level Agreement.
n) The administrators will also be required to have experience in latest technologies like Orchestration, virtualization and cloud computing so as to provision the existing and applicable infrastructure on a requirement-based scenario

Storage Administration

Certain minimum deliverables sought from the MSI about Storage Administration are provided below:-

a) The MSI shall be responsible for the management of the storage solution including, but not limited to, storage management policy, configuration and management of disk array, SAN switches, Virtual tape library, PBBA, Backup Software etc. It should be

noted that the activities performed by the MSI will be under the supervision of CRID

b) The MSI shall be responsible for storage management, including but not limited to management of space, SAN volumes, RAID configuration, LUN, replication, zone, security, business continuity volumes, performance, etc.
c) CRID would additionally remotely manage the storage system and components and appropriate setup should be provided by the MSI
d) The storage administrator will be required to identify parameters including but not limited to key resources in the storage solution, interconnects between key resources in the storage solution, health of key resources, connectivity and access rights to storage volumes and the zones being enforced in the storage solution.
e) The storage administrator will be required to create/delete, enable/disable zones in the storage solution
f) The storage administrator will be required to create/delete/modify storage volumes in the storage solution
g) The storage administrator will be required to create/delete, enable/disable connectivity and access rights to storage volumes in the storage solution
h) To facilitate scalability of solution wherever required.
i) The administrators will also be required to have experience in latest technologies like virtualization and cloud computing so as to provision the existing and applicable infrastructure on a requirement based scenario

Database Administration

Under the supervision/ guidance of CRID officials, the MSI shall be responsible for monitoring database activity and performance, changing the database logical structure to embody the requirements of new and changed programs.

a) MSI responsible for Database Administration, Installation & Configuration, Log analysis, Backup, Restoration, Disaster Recovery, Performance tuning, Patching, Upgradation, Cluster implementation, Scalability, High Availability, Load balancing, Mirroring, Replication, Resource governance, Testing and related services etc. for databases not limiting to MS-SQL, Oracle, MySQL, DB2, Postgresql, MongoDB etc.,
b) The MSI shall be responsible to perform physical administrative functions such as re-organizing the database to improve performance.
c) The MSI shall be responsible for tuning of all database, ensuring the integrity of the data and configuring the data dictionary.
d) The MSI shall be responsible for testing and installing new database software releases and patches if any.
e) The MSI shall be responsible for Data protection and Encryption of Database and EMS database.
f) The MSI shall support Transparent Data Encryption (TDE), database activity monitoring and blocking, consolidated auditing and reporting, masking.
g) MSI will follow guidelines issued by CRID in this regard from time to time including access of data base by system administrators and guidelines relating to security of database.
h) Database administration should follow the principle of segregation of duties to ensure no single DBA can update production tables/data singularly.
i) In addition to restrictions on any direct change in Data by any administrator, the Databases shall have Auditing features enabled to capture all activities of administrators.

Backup / Restore

The MSI shall be responsible for backup of storage as per the SDC Standards approved by CRID. These policies would be discussed with The MSI at the time of installation and configuration. It should be noted that the activities performed by the MSI will be under the supervision of CRID

a) The MSI shall be responsible for monitoring and enhancing the performance of scheduled

backups, schedule regular testing of backups and ensuring adherence to related retention policies

The MSI shall be responsible for prompt execution of on-demand backups of volumes and files whenever required by CRID or in case of upgrades and configuration changes to the system.

b) The MSI shall be responsible for real-time monitoring, log maintenance and reporting of backup status on a regular basis. The MSI shall appoint administrators to ensure prompt problem resolution in case of failures in the backup processes.
c) The administrators shall undertake media management tasks, including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fireproof cabinets (onsite and offsite).
d) The MSI shall also provide a 24x7 support for file and volume restoration requests at the Data Centre.

Network Administration

The MSI shall provide services for management of network environment to maintain performance at optimum levels on a 24 x 7 basis. It should be noted that the activities performed by the MSI will be under the supervision of CRID.

a) The MSI shall be responsible for monitoring and administering the network within the Data Centre up to the integration points with WAN. The MSI will be required to provide network related services for switches, load balancer services etc.
b) The MSI shall be responsible for creating and modifying VLAN, assignment of ports to appropriate applications and segmentation of traffic.
c) The MSI shall co-ordinate with the Data Centre Site Preparation MSI in case of break fix maintenance of the LAN cabling or maintenance work requiring civil work.
d) MSIshallalsoberesponsibleforbreakfixmaintenanceoftheLANcablingwithinDC,etc.
e) MSIshallalsoprovidenetworkrelatedsupportandwillcoordinatewithconnectivityserviceprovider sof CRID other agencies who are terminating their network at the DC for access of system.

Information Security Monitoring and Management

The MSI shall provide services (monitoring and management) for the following infrastructure systems related to information security. Management of this environment in order to ensure confidentiality, integrity, availability, and non-repudiation of the services on a 24 x 7 basis. It should be noted that the activities performed by the MSI will be under the supervision of CRID. The team will be required to provide monitoring and management of activities including but not limited to the following: -

Firewall Monitoring and Management

a) Installation and maintenance of the firewall
b) Firewall Hardening with initial configuration
c) Performance Monitoring
d) Regular Monitoring of the LAN errors
e) Firewall Rule based policy changes
f) Security Policy Configuration
g) Create and maintain Network Access Policy (NAP) document (the access specification) agreed between the parties from time to time.
h) Log File review and analysis of information on traffic flow
i) Log File trend upgrade and analysis
j) Compliance Testing
k) Design, configure and maintain all Network Address Translation (NAT) services.
l) Access control management through creation of the Network Access Policy and firewall rules.
m) Implementation and maintenance.

n) Manage access to F/W logs policies and performance statistics for viewing through secure web portals in conjunction with monitoring tools
o) Manage the functioning of Regular Reports in conjunction with monitoring tools so as to provide detailed auditing of configuration history and change of journals. Alerts include critical configuration changes, potential malicious activity and operational alarms
p) Incidence response
q) Lifecycle Management of all Hardware and Software components
r) Firewall Policy & Configuration Backup
s) Coordination with SOC and fixing of issues reported by SOC

Network Based Intrusion Prevention System - Monitoring and Management

a) Traffic Profiling
b) Define Alert levels and Incident response level
c) Root cause analysis
d) Technical support
e) Monitor NIPS for 24*7 availability
f) Restore NIPS availability
g) Determine Intrusion occurrence
h) Upgrade of vendor provided intrusion signatures
i) Provide security event correlation
j) Regular Monitoring of the attack logging rules' logs
k) Regular Monitoring of the generic deny rules' logs
l) Regular Monitoring of the attack bandwidth utilization
m) Network attacks and serious attack attempts analysis
n) Uncovered new vulnerabilities assessment
o) Propose corrective and preventive actions.
p) Monitoring and subscribing to external network security information in order to evaluate new attacks and propose preventive steps.
q) Installation and configuration of NIPS Software and Hardware
r) Provide maintenance and upgrade of service component Software
s) Provide reporting of intrusions and actions, web-based access
t) Regular Reports
u) Incidence response
v) Prevent all known network-based attacks
w) Filter out IP and TCP illegal packet type
x) Design and Configuring IPS services in response to Flooding limits (per source, destination, and intensity)
y) Technical Support desk Support
z) Lifecycle Management of all Hardware and Software components aa) 24*7Real time Monitoring and Response

Vulnerability Assessment

This section provides an outline of the various items to be investigated during our Vulnerability Assessment phase. The said activities should follow the various guidelines for cyber security like ISMO, CRID guidelines and Cert- In Guidelines. The activities performed should be included but not limited to the following:

a) Web Application based vulnerability assessment:

To provide proper evaluation of security vulnerabilities associated with web applications– Apache, IIS, Tomcat, etc., thereby, recommend solutions to problems.

b) OS level vulnerability assessment:

To provide proper evaluation of security vulnerabilities associated with operating systems – Unix, Linux, Sun OS, Windows, etc., thereby, recommend solutions to problems.

c) Database Vulnerability assessment:

To provide proper evaluation of security vulnerabilities associated with database –Microsoft SQL Server, MySQL, Oracle, DB2, etc., thereby, recommend solutions to problems.

d) Network level Vulnerability Assessment

To provide proper evaluation of security vulnerabilities associated with Network components – Firewall, NIPS, HIPS, LLB, etc.,

Vulnerability Assessment will include checks like Port scan, unnecessary or vulnerable services, file permission, user access control, password protection, system vulnerability Firmware vulnerabilities, etc.

OS Hardening

OS Hardening will include activities but not limited to the removal of all non-essential tools, utilities, and services with other system administration by activating & configuring all appropriate security features. The entire scope of this service will differ on different Operating System basis. Most of the Windows based Operating Systems will include following activities in conjunction to CRID OS hardening guidelines:

Broad category:

a) User Account Management
b) Access Control Management
c) Configuration and supporting processes
d) System logging and auditing.
e) Network and environmental variables.

A preview on the activities associated with Broad categories:

a) Identifying unused or unnecessary ports
b) Disable/Shutdown/remove unused and unnecessary services and daemons.
c) Removing rogue connections: wireless and dial-up.
d) Setting up filters for malicious content for each OS.
e) Test Backup and restoring procedures.
f) Account Policies: Password policy, Account lockout policy etc.
g) Local server Policies: Audit policies, User rights assignments, security options etc.
h) Event logs settings
i) System services
j) Registry settings
k) File & Folder permissions

Penetration Testing

The Penetration Testing will include activities but not limited to the test should simulate activities in conjunction to ISMO, CRID cyber security and Cert-In guidelines. These activities should identify specific exploitable vulnerabilities and expose potential entryways to vital or sensitive data. The results should clearly articulate security issues and recommendations and create a compelling event for the entire management team to support a security program.

A complete project-based approach should be followed that covers areas including but not limited to the following:

a) Network Security
b) Network Surveying
c) Port Scanning
d) System Identification
e) Services Identification
f) Vulnerability Research & Verification
g) Application Testing & Code Review
h) Router Testing

i) Firewall Testing
j) Intrusion Detection System Testing
k) Trusted Systems Testing
l) Password Cracking
m) Denial of Service Testing
n) Containment Measures Testing

Disaster Recovery & Business Continuity

The MSI is responsible for Disaster Recovery Services so as to ensure continuity of operations in the event of failure of CRIDHSDC. DR services will be provided through near line BCP site at STPI, Mohali to be installed and commissioned by MSI as part of this RFP. MSI shall be responsible for operation & maintenance and implementation of DR. RPO should be less than or equal to 5 minute or in some critical application near real time and RTO shall be less than or equal to 15 minutes. The key transaction data shall have RPO of 5 minutes. However, during the change from CRID SDC to DRC or vice-versa (regular planned changes), there should not be any data loss. There shall be asynchronous replication of data between CRID SDC and DRC and the CRID will provide DC & near line DC P2P connectivity through dark fibre as well as through 10Gbps internet link(possibly NKN) and latency less than 5 millisecond so that some critical application can be run on active-active or active passive mode considering 0 data loss and RTO less than 5 min.

1. The proposed bandwidth of Dark Fiber connectivity between HSDC and NL-BCP site may be 10 Gbps and proposed MPLS connection in Far DR site may be 1 Gbps considering backup of minimum of 400 GB per hour.

2. HSDC is considering hourly incremental data size will be between 200GB to 250 GB maximum in next 5 year and maximum 1.5 TB to 2 TB per day during business days in next 5 years.

3. Considering this RPO and RTO between HSDC and NL BCP site may be set to maximum 5 minutes for all critical application in case of failover.

4. In any case RPO should not be more than 30 minutes between HSDC and Far DR site for all critical application and RTO will be decided with mutually agreed condition between CRID and MSI

MSI can suggest better solution to integrate HSDC and NL DC site Mohali to run application in active-active as well as active passive mode. To achieve automatic failover, MSI will bring required hardware/software with no extra cost to deliver desired SLA other than BOQ.

However, during the change from CRISHSDC to Near line DC site or vice-versa (regular planned changes), there should not be any data loss. There shall be asynchronous/synchronous replication of data between CRID SDC and Near line DC site

a) During normal operations, the CRID HSDC will serve the requests other than if any critical application running on active-active mode. The Disaster Recovery Site will not be performing any work but will remain on standby. During this period, the compute environment for the application in DR shall be available but with minimum possible compute resources required for a functional DR as per the solution offered. The application environment shall be installed and ready for use. DR Database Storage shall be replicated on an ongoing basis and shall be available in full (100% of the CRID HSDC) as per designed RTO/RPO and replication strategy. The storage should be 100% of the capacity of the Primary Data Centre site.
b) In the event of a site failover or switchover, DR site will take over the active role, and all requests will be routed through that site. Application data and application states will be replicated between data centre so that when an outage occurs, failover to the surviving data centre can be accomplished within the specified RTO. This is the period during which the Compute environment for the application shall be equivalent to DC. The installed application instance and the database shall be usable and the same SLAs as DC shall be provided. The use of this Full Compute DR environment can be for specific periods during a year for the purposes of DC failure or DR Drills or DC maintenance. The Database and storage shall be of full capacity and the licenses and security shall be for full infrastructure. The bandwidth at the DR

shall be scaled to the level of Data centre. Users of application should be routed seamlessly from DC site to DR site. The MSI shall conduct DR drill for two days at the interval of every six months of operation wherein the HSDC has to be deactivated and complete operations shall be carried out from the DR Site. However, during the change from DC to DRC or vice-versa (regular planned changes), there should not be any data loss.

c) The MSI shall clearly define the procedure for announcing DR based on the proposed DR solution. The MSI shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to DR. The MSI shall plan all the activities to be carried out during the Disaster Drill and issue a notice to the Department at least two weeks before such drill.
d) The MSI should offer switchover and switchback of individual applications instead of entire system.

Service Level Management

MSI shall ensure compliance to uptime and performance requirements of project solution as indicated in the SLA (as per section 8 of the RFP) table of RFP and any upgrades/major changes to the SDC System shall be accordingly planned by MSI for ensuring the SLA requirements. MSI shall be responsible for measurement of the SLAs at the SDC System level as well as at the user level with the help of the enterprise monitoring tool on a periodic basis. Reports for SLA measurement must be produced to CRID officials as per the project requirements.

Monitoring and Management

a) The proposed service management system should provide a detailed service dashboard view indicating the health of each of the departments / offices in the organization and the health of the services they rely on as well as the SLAs.
b) The system should provide an outage summary that gives a high level health indication for each service as well as the details and root cause of any outage.
c) The system must be capable of managing IT resources in terms of the business services they support, specify and monitor service obligations, and associate users/Departments/ Organizations with the services they rely on and related Service/Operational Level Agreements. Presently, services shall include E-mail, Internet Access, Intranet and other services hosted.
d) The Service Level Agreements (SLAs) definition facility must support defining a set of one or more service that specify the Service obligations stipulated in an SLA contract for a particular time period (weekly, monthly, and so on).
e) SLA violation alarms must be generated to notify whenever an agreement is violated or is in danger of being violated.
f) The system must provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In addition the capability to exempt any service outage from impacting an SLA must be available.

Reporting

a) The reports supported must include one that monitors service availability (including Mean Time to Repair (MTTR), Mean Time between Failure (MTBF), and Maximum Outage Time thresholds) and the other that monitors service transaction response time.
b) The system must provide a historical reporting facility that will allow for the generation of on-demand and scheduled reports of Service related metrics with capabilities for customization of the report presentation.
c) The system should provide for defining service policies like Service Condition High\Low Sensitivity, Port Status High\Low Sensitivity should be provided out of the box.
d) The system should display option on Services, Customer, SLA's, SLA templates. The customer definition option should allow to associate a service or an SLA with a customer.

Performance-Monitoring, Management and Reporting

The proposed performance management system shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network components. The proposed performance management system must integrate network, server & database performance reporting information and alarms in a single console in order to provide a unified reporting interface.

Onsite Support to ICT Infrastructure hosted by other Government Agencies: Co-location

a) CRID shall provide the Data Centre Rack space to other Government agencies and user departments to host their ICT Infrastructure.
b) The MSI shall provide onsite support to such Government Agencies and user departments. The MSI shall be responsible for providing all the onsite support services as mentioned in this section.

Other Support Services

a) Hardware support for the ICT infrastructure solution which will include diagnosing the problem and getting the same resolved through coordination with the respective vendors as per the severity level assigned to it to ensure uptime of all ICT infrastructure of CRID as per the SLAs defined in Service Level Agreement.
b) Maintain a record of all the hardware changes made in the ICT infrastructure solution.
c) Onsite Support to ICT Infrastructure hosted by other Government Agencies: Colocation
d) Schedule maintenance of the ICT infrastructure solution under the scope of work at the periodicity defined by the OEM and also as per the schedule defined in discussion with CRID.
e) Installation, upgrade, update and management of all the patches including but not limited to the servers, switches etc.
f) Maintain the inventory of the entire hardware and software assets installed at the Data Centre.
g) The MSI shall maintain all documentation related to material movement such as new hardware, spare parts or equipment going out of premises for repairing etc.
h) The MSI shall also maintain other site specific documentation such as network diagrams, manuals, license copies in hard and soft formats.
i) The MSI shall also update changes to documents like changes in IP addresses, changes to layout of machines, addition to network, change in network layout, etc.
j) The MSI shall ensure implementation and enforcement of procedures, policies and guidelines like Security policy, Network access policy, Anti-virus policy, etc. as formulated in discussion with CRID.
k) The MSI shall be responsible for Liaison with the data centre teams for utilities such as Power, UPS, Air Conditioning, etc. as and when required.

MIS Reports and deliverables

The MSI shall be required to submit the reports as specified hereunder on a regular basis in a format decided by CRID. The following is only an indicative list of MIS reports which should be in conjunction to the reporting features highlighted in RFP. The MSI should submit 2 hard copies and 2 soft copies of each of the reports.

Dailyreports

a) Summary of issues / complaints logged at the Technical Support desk
b) Summary of resolved, unresolved and escalated issues / complaints
c) Summary of resolved, unresolved and escalated issues / complaints to vendors.
d) Log of backup and restoration undertaken.

Weekly Reports

a) Issues / Complaints Analysis report for virus calls, call trend, call history, etc.
b) Summary of systems rebooted.
c) Summary of issues / complaints logged with the OEMs.
d) Inventory of spare parts in the Data Centre.

e) Database Report in DB wise Resource utilization report.
f) Summary of changes undertaken in the Data Centre including major changes like configuration changes, patch upgrades, database reorganization, storage reorganization, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.

Monthly reports

a) Component wise ICT infrastructure availability and resource utilization.
b) Consolidated SLA / (non)-conformance report.
c) Summary of component wise Data Centre uptime.
d) Summary of changes in the Data Centre.
e) Log of preventive / scheduled maintenance undertaken
f) Log of break-fix maintenance undertaken
g) Summary of attendance of MSI's staff at the Data Centre.

Quarterly Reports

Consolidated component-wise ICT infrastructure availability and resource utilization

Half-yearly Reports

a) Data Centre Security Audit Report
b) ICT infrastructure Upgrade / Obsolescence Report

Software license violations

a) CRID shall get the ICT infrastructure solution audited by a third-party on yearly basis. The third-party shall undertake the audit of the entire ICT infrastructure solution. The audit shall ensure installation of proper versions of software including, but not limited to, Firmware, OS patches, etc.
b) The audit report shall make recommendations to CRID regarding issues including but not limited to upgrade of infrastructure components, reallocation of unused infrastructure components, etc.
c) The audit shall also cover obsolescence of the ICT infrastructure as per the policy defined by the MSI in discussion with CRID. The audit report shall provide details of the infrastructure components that are due for obsolescence and provide recommendations for upgrade / refresh of infrastructure components and plan for disposal of obsolete infrastructure components.
d) CRID may also get a half-yearly security audit done by a third-party for the security practices, implementation of security policy and vulnerability assessment at the Data Centre. The security audit report shall rate the security implementation in three grades viz. Satisfactory, Requires Improvement and Unsatisfactory.
e) MSI shall provide necessary support and co-operation for these audits.
f) The MSI shall implement all the audit recommendations in time as per the service levels defined in section 8 of the RFP.
g) There shall be an Internal Audit Team constituted by CRID, who will perform the internal audit of HSDC ISO processes (ISMS Policy, ISO 27001 and ISO 20000) on half yearly basis.

Documentation

a) The MSI shall be required to submit documentation in the format, media and number of copies as decided mutually with CRID. The documentation shall be kept updated throughout the contract period with appropriate change management procedures and version control. It is advisable to follow international standards and best practices like ISO standards while creating the documentation
b) The selected MSI shall provide documentation, which follows the ITIL (Information Technology Infrastructure Library) standards. This documentation should be submitted as the project undergoes various stages of implementation.
c) Indicative list of documents includes:
   - Project Commencement: Project Plan in MS Project giving out micro level activities with milestones & deadlines

- Delivery of Material: Original Manuals from OEMs.
- Training: Training Material will be provided which will include the presentations used for trainings and also the required relevant documents for the topics being covered.
- Process Documentation: The MSI shall be responsible for preparing process documentation related to the operation and maintenance of each and every IT component of the SDC. The prepared process document shall be formally signed off by CRID before completion of final acceptance test.
- The selected MSI shall document all the installation and commissioning procedures and provide the same to the CRID within one week of the commissioning of the SDC.
- Manuals for configuring of switches, firewall, IPS etc shall be provided by the selected MSI.
- The selected MSI shall be responsible for documenting configuration of all devices and keeping back up of all configuration files, so as to enable quick recovery in case of failure of devices.
- The selected MSI shall submit the report on best security practices & further improvement & enhancement of the Data Centres to the CRID
- Data Centre, being a property of CRID, it reserves the right to verify the process and documentation submitted, at any given point of time
- The MSI shall be responsible for creation and maintenance of all the documentation including but not limited to configuration documents, network diagram, Data Centre operation manual, system administration manual, security administration manual, password management manual, etc. The servicing manual should cover all the procedures and information necessary for the diagnosis and repair of faulty units or components of every type.
- These MSI shall get all these documents approved by CRID.
- The MSI shall be also responsible for maintenance and updation of all the policy documents including but not limited to security policy, backup policy, archival policy, backup policy, anti-virus policy, etc.
- The MSI shall make changes to the documents as and when there is change in the ICT infrastructure components or policies or as and when required by CRID.
- The MSI should maintain a library of various art effects including, but not limited to, documents, manuals, knowledge bases, CD / DVDs, etc. pertaining to all the components supplied by various OEMs. The MSI should keep a track of all the art effects and manage the issue and return of the arteffects into the library.
- All the documents would be solely owned by CRID.

Handholding & Training for Information Security and BCP

In order to strengthen the staff, structured capacity building programmes shall be undertaken for identified resources of CRID. It is important to understand the training needs to be provided to each and every staff personnel of HSDC. These officers shall be handling emergency situations with very minimal turnaround time. The actual number of trainees will be provided at design stage.

a) MSI shall prepare and submit detailed Training Plan and solution specific Training Manuals to CRID for review and approval. Training Manuals, operation procedures, visual help-kit etc. shall be provided in English/Hindi language.
b) MSI shall ensure that the training module holistically covers all the details around hardware and system applications expected to be used on a daily basis to run the system covering functional, technical aspects, usage and implementation of the products and solutions.
c) Appropriate training shall be carried out as per the User Training Plan prepared in detail stating the number of training sessions to be held, course work for the training program, coursework delivery methodologies and evaluation methodologies in detail.
d) MSI shall also be responsible for full capacity building. Training and capacity building shall be provided for all individual modules along with their respective integrations.
e) MSI shall be responsible for necessary demonstration environment setup including setup of cameras, sensors and application solutions to conduct end user training. End user training shall include all the equipment installed at HSDC.

f) MSI shall impart operational and technical training to internal users on solutions being implemented to allow them to effectively and efficiently use & monitor the SDC system.
g) MSI shall ensure that all concerned personnel receive regular training sessions, from time to time, as and when required. Refresher training sessions shall be conducted on a regular basis.
h) An annual training calendar shall be clearly chalked out and shared with the CRID along with complete details of content of training, target audience for each year etc.
i) MSI shall update training manuals, procedures, manuals, deployment/installation guidelines etc. on a regular basis (Quarterly/ Biannual) to reflect the latest changes to the solutions implemented and new developments.
j) MSI shall ensure that training is a continuous process for the users. Basic intermediate and advanced application usage modules shall be identified by the MSI.
k) Systematic training shall be imparted to the designated trainees that shall help them to understand the concept of solution, the day-to-day operations of overall solution and maintenance and updating of the system to some extent. This shall be done under complete guidance of the trainers provided by the MSI.
l) Time Schedule and detailed program shall be prepared in consultation with CRID and respective authorized entity. In addition to the above, while designing the training courses and manuals, MSI shall take care to impart training on the key system components that are best suited for enabling the personnel to start working on the system in the shortest possible time.
m) MSI is required to deploy a Master Trainer who shall be responsible for planning, designing and conducting continuous training sessions.
n) The master trainer shall demonstrate a thorough knowledge of the material covered in the courses, familiarity with the training materials used in the courses, and the ability to effectively lead the staff in a classroom setting. If at any stage of training, the CRID feels that on-field (SDC-Server Farm) sessions are required, the same shall be conducted by the MSI.
o) If any trainer is considered unsuitable by CRID, either before or during the training, MSI shall provide a suitable replacement without disrupting the training plan.
p) Training sessions and workshops shall comprise of presentations, demonstrations and hands-on mandatorily for the application modules.
q) CRID shall be responsible for identifying and nominating users for the training. However, MSI shall be responsible for facilitating and coordinating this entire process.

MSI has to ensure that training sessions are effective, and the attendees shall be able to carry on with their work efficiently. For this purpose, it is necessary that effectiveness of the training session is measured through a comprehensive feedback mechanism. MSI shall be responsible for making the feedback available for the CRID/authorized entity to review and track the progress, In case, after feedback, more than 40% of the respondents suggest that the training provided to them was unsatisfactory or less than satisfactory then the MSI shall re-conduct the same training at no extra cost. Following training needs is identified for all the project stakeholders:

i. Operational & Functional training

a) The MSI shall impart operational training to all the primarily the designated resources CRID. This training should cover a session on below mentioned key areas:
   - Security Awareness,
   - practices and operations for the information security,
   - Centralized & System Administration Helpdesk including handling helpdesk requests,
   - BMS Administration & Incident Management,
   - Master trainer assistance and etc
   - Feed monitoring and
   - BCP components installed at the Data Centre.

b) The standard contents of such training should be documented and made available to all the users. Two copies in hard and soft format should be made available to the in-charge. Changes to the same should be updated periodically as mentioned above.

ii. Technical training

a) The MSI should also provide OEM specific Technical training on all equipment to officials as designated by CRID. This training should include, but not limited to the training on Usage of all the proposed systems for monitoring, tracking and reporting (Including MIS reports & accessing various exception reports) particularly for Senior Management.

b) The contents of such training would need to be documented and made available to all the attendees. Two copies in hard and soft format should be made available to the office of CRID.

   i. Post-Implementation Training
   Apart from above, MSI has to impart below mentioned trainings as and when required during O&M phase:
      i. Refresher Trainings for senior officials
      ii. Functional/Operational training for new operators/officers of CRID
      iii. Refresher courses on System Administration
      iv. Change Management programs

Manpower Deployment

a) The MSI shall provision for adequate onsite support to provide 24x7x365 onsite operations and maintenance services to CRID as defined in the scope of work.

b) The MSI shall provide adequate number of administrators, each responsible for its respective specific role at the Data Centre. The MSI must provide clear definition of the role and responsibility of each manpower resource as part of the Technical Bid in the format specified in Contents of the Bid.

c) Onsite resources will follow six working days per week cycle, and will be entitled for all national holidays. Required resources can be called on Holiday/odd hours, in such case they will be entitled for compensatory leaves.

d) All the critical (L3 & above) onsite resources deployed at SDC Chandigarh have to be on MSI's payroll. All other onsite resources deployed at SDC Chandigarh should ideally be on MSI's payroll however in case resources are not available, third party services may be taken where in the full responsibility of the man power shall lie with the MSI with regard to confidentiality of information, their technical skill set, their SLA's etc. in order to meet the scope of work as per RFP."In case, MSI is a PSU, All the critical (L3 & above) onsite resources may also be deployed in third party rolls with prior consent of CRID. This shall additionally required fulltime onsite supervisor /senior officer on the payrolls of the PSU.

e) Onsite resources for Network, Security and Technical support will work in shifts to provide 24x7x365 onsite operations and maintenance services to CRID.

f) All the concerned onsite staff shall log an attendance on a daily basis. The MSI shall maintain a database of attendance of his staff at the Data Centre. The attendance database should have facility to track attendance and draw out MIS reports as desired by CRID. The MSI shall submit the attendance records in a format and as per schedule desired by CRID.

g) The MSI should ensure that all the personnel identified for this project have high level of integrity. The MSI should undertake necessary due diligence to ensure that the personnel have high standard of trustworthiness. The MSI should obtain an undertaking from each of the personnel assigned and the same should be submitted to CRID as and when demanded by CRID.

h) The MSI shall be responsible for any mishaps or security breaches that happen due to MSI's personnel / personnel

i) appointed by MSI for execution of services.

j) A Project In-charge should be appointed on a full-time basis. The Project In-charge shall be responsible for the overall project and shall be a single point of contact for CRID.

k) The MSI should estimate and propose the personnel required during the Installation, Commissioning and Maintenance phase and provide the estimation as part of the Technical Bid in the format specified in Contents of the Bid.

l) The following clause defines the skill sets and qualification requirement for Project in Charge. However, criteria mentioned in manpower eligibility requirements for L3 and L4

in this document will be binding.

m) Project In-charge
    i. Should be resident at the Data Centre site on a full-time basis.
    ii. Should be responsible for the overall contract performance and should not serve in any other capacity under this contract.
    iii. Should be responsible for organizing, planning, directing, and coordinating the overall program effort and managing the team.
    iv. Should have extensive experience and proven expertise in managing infrastructure project of similar type and complexity.
    v. Should have a thorough understanding and knowledge of the principles and methodologies associated with program management, vendor management, quality assurance metrics and techniques, and configuration management tools.
    vi. Should have a graduation degree in Computer Engineering or Masters Degree in Computer Applications with PMP certification.
    vii. Should have an IT experience of 10 years with minimum 5 years of relevant experience in Data Centre with PMI Certification and complying to Eligibility criteria
    viii. ITIL certification would be preferable.

PROJECT GOVERNANCE AND CHANGE MANAGEMENT

Project Management and Governance

Project Management Office (PMO)

A Project Management office will be set up during the start of the project. The PMO will, at the minimum, include a designated full time Project Manager from MSI. It will also include key persons from other relevant stakeholders including members of CRID and other officials/representatives by invitation. The operational aspects of the PMO need to be handled by MSI including maintaining weekly statuses, minutes of the meetings, weekly/monthly/project plans, etc. PMO will meet formally on a weekly basis covering, at a minimum, the following agenda items:

a) Project Progress including HOTO
b) Delays, if any – Reasons thereof and ways to make-up lost time
c) Issues and concerns
d) Performance and SLA compliance reports
e) Unresolved and escalated issues
f) Project risks and their proposed mitigation plan
g) Discussion on submitted deliverable
h) Timelines and anticipated delay in deliverable if any
i) Any other issues that either party wishes to add to the agenda

During the implementation phase, there may be a need for more frequent meetings and the agenda would also include:

a. Phase wise Implementation status
b. Testing results
c. IT infrastructure procurement and deployment status
d. Status of setting up of Helpdesk, DC, DR on Cloud
e. Any other issues that either party wishes to add to the agenda

Bidder shall recommend PMO structure for the project implementation phase and operations and maintenance phase.

Help desk and Facilities Management Services

a) MSI shall be required to establish the helpdesk and provide facilities management services to support the CRID and stakeholder department officials in performing their day- to-day functions related to this system.

b) MSI shall setup a central helpdesk dedicated (i.e. on premise) for the Project. This helpdesk would be operational upon implementation of the Project. Providing helpdesk/support services from a shared facility of any other party/provider is not permitted.
c) Functional requirements of the helpdesk management system, fully integrated with the enterprise monitoring and network management system. The system will be accessed by the stakeholder department officials for raising their incidents and logging calls for support. The detailed service levels and response time, which MSI is required to maintain for provisioning of the FMS services are described in the Service Level Agreement of this Tender.
d) Helpdesk System should be part of Workflow management system with facilities like Auto-Routing, Auto- Escalation, User Management, Password Management, In-Built Form Builder & Process Designer etc.

Steering Committee

a) The Steering Committee will consist of senior stakeholders from CRID, its nominated agencies and MSI. MSI will nominate its Director/ Vertical head to be a part of the Project Steering Committee.
b) MSI shall participate in Monthly Steering Committee meetings and update Steering Committee on Project progress, Risk parameters (if any), Resource deployment and plan, immediate tasks, and any obstacles in project. The Steering committee meeting will be a forum for seeking and getting approval for project decisions on major changes etc.
c) All relevant records of proceedings of Steering Committee should be maintained, updated, tracked and shared with the Steering Committee and Project Management Office by MSI.
d) During the development and implementation phase of the project, it is expected that there will be at least fortnightly Steering Committee meetings. During the O&M phase, the meetings will be held at least once a quarter.
e) Other than the planned meetings, in exceptional cases, CRID may call for a Steering Committee meeting with prior notice to MSI.

Project Monitoring and Reporting

a) MSI shall circulate written progress reports at agreed intervals to CRID and other stakeholders. Project status report shall include Progress against the Project Management Plan, status of all risks and issues, exceptions and issues along with recommended resolution etc.
b) Other than the planned meetings, in exceptional cases, project status meeting may be called with prior notice to the MSI. CRID reserves the right to ask the MSI for the project review reports other than the standard weekly review reports.

Risk and Issue management

a) MSI shall develop a Risk Management Plan and shall identify, analyze and evaluate the project risks, and shall develop cost effective strategies and action plans to mitigate those risks.
b) MSI shall carry out a Risk Assessment and document the Risk profile of CRID based on the risk appetite and shall prepare and share the CRID Enterprise Risk Register. MSI shall develop an issues management procedure to identify, track, and resolve all issues confronting the project. The risk management plan and issue management procedure shall be done in consultation with CRID.
c) MSI shall monitor, report, and update the project risk profile. The risks should be discussed with CRID and a mitigation plan be identified during the project review/status meetings. The Risk and Issue management should form an agenda for the Project Steering Committee meetings as and when required.

Governance procedures

MSI shall document the agreed structures in a procedure's manual.

Planning and Scheduling

MSI will prepare a detailed schedule and plan for the entire project covering all tasks and sub tasks required for successful execution of the project. MSI has to get the plan approved from CRID at the start of the project and it should be updated every week to ensure tracking of the progress of the project. The project plan should include the following:

a) The project break up into logical phases and sub-phases;
b) Activities making up the sub-phases and phases;
c) Components in each phase with milestones;
d) The milestone dates are decided by CRID in this RFP. MSI cannot change any of the milestone completion dates. MSI can only propose the internal task deadlines while keeping the overall end dates the same. MSI may suggest improvement in project dates without changing the end dates of each activity.
e) Key milestones and deliverables along with their dates including those related to delivery and installation of hardware and software;
f) Start date and end date for each activity;
g) The dependencies among activities;
h) Resources to be assigned to each activity;
i) Dependency on CRID

License Metering/Management

MSI shall track software usage throughout the IT setup so as to effectively manage the risk of unauthorized usage or under-licensing of software installed at the HSDC. This may be carried out through the use of standard license metering tools.

Manpower Deployment

MSI need to deploy requisite mix of L1, L2 and L3 resources (on 24X7 basis) for management of entire ICT & Non-IT infrastructure deployed at HSDC.

i. All resources deployed in the project should be employees of MSI and be Indian citizens.
ii. All the L1 and L2 resources proposed for the project need to be dedicated for the project.
iii. Any change in the team once deployed will require approval from CRID. It is expected that resources have proven track record and reliability.
iv. Considering the criticality of the project, CRID may ask for security verification (Police verification) of every resource deployed on the project and MSI need to comply the same before deployment of the resource at the project.
v. At all times, the MSI need to maintain the details of resources deployed for the project to CRID and keep the same updated.
vi. Detailed process in this regard will be finalized between CRID and MSI.
vii. The MSI shall maintain an attendance register for the resources deployed.
viii. Attendance details of the resources deployed also need to be shared with CRID on monthly basis.
ix. CRID reserves the right to interview resources deployed for Operations and maintenance and assess the suitability of the resource for the role. In case a resource is not found suitable, MSI will change the resource on request of CRID. MSI shall comply with this.

MSI shall deploy below Manpower during implementation and O&M phases. The deployed resource shall report to CRID and work closely with Program Management Office of the project. Following are the minimum resources required to be deployed in the Project, however MSI may deploy additional resources based on the need of the Project to meet the Go-Live milestone and to meet the defined SLAs in this RFP:

Resources Required during the HOTO & Implementation Phase

Sr. No.	Role	Expertise Level (with qty)	Minimum Qty	Minimum Deployment during HOTO & Implementation Phase	Shift Timings	No. of Shifts
1	Project Manager	L4	1	100%	8x6	1
2	Network and Security Expert	L3	2	100%	8x6	1
3	DC-DR Cloud Solution Expert	L3	1	100%	8x6	1
4	Solution Architect cum-DBA	L3	1	100%	8x6	1
5	Storage and Backup Expert	L3	1	100%	8x6	1
6	Server Expert/ System Administrator	L3	1	100%	8x6	1
7	BMS Expert	L3	1	100%	8x6	1

Operation Manpower required during HOTO shadowing

Sr. No.	Role	Expertise Level (with qty)	Minimum Qty	Minimum Deployment during O&M Phase (24x7x365)	Shift Timings	No. of Shifts
1	NOC Engineer	L1	4	100%	24x7	3
2	HelpDesk Engineer	L1	4	100%	24x7	3
3	BMS Expert	L2-(2) L1-(2)	4	100%	24x7	3

Resources Required during the O&M Phase for DC

Sr. No	Role	Expertise Level (with qty)	Minimum Qty	Minimum Deployment during O&M Phase(24x7x365)	Shift Timings	No. of Shifts
1.	Project Manager	L4	1	100%	8x6	1
2.	Network and Security Expert	L3-(2) L2-(3)	5	100%	24x7	4
3.	DC-DR Cloud solution Expert including HCI	L3(1) L2(2)	3	100%	8x6	2
4.	DBA	L3(1) L2(2)	3	100%	16x6	2
5.	Storage and Backup Expert	L2	2	100%	16x6	2
6.	Server Expert/System Administrator	L3-(1) L2-(2) L1-(2)	5	100%	24x7	4
7.	NOC Engineer	L1	5	100%	24x7	3
8.	HelpDesk Engineer	L1	7	100%	24x7	4
9.	BMS Expert	L3-(1) L2-(2) L1-(2)	5	100%	24x7	3

Resources Required during the O&M Phase for BCP

Sr. No.	Role	Expertise Level (with qty)	Minimum Qty	Minimum Deployment during O&M Phase (24x7x365)	Shift Timings	No. of Shifts
1.	Network and	L3-(1)	6	100%	24x7	3

	Security Expert	L2-(5)				
2.	DBA	L3(1)	1	100%	16x6	1
3.	Storage and Backup Expert	L2(5)	5	100%	16x6	3
4.	Server Expert/System Administrator	L3-(1) L2-(2) L1-(2)	5	100%	24x7	3
5.	BMS Expert	L2(2)	2	100%	24x7	2

The above proposed manpower in Information Security should be well capable of managing all equipment in DC and DR with demonstrable experience in 1 or more domains of security. It is envisaged that the experienced manpower required for the SOC will be deployed during the implementation and O&M phase sufficiently to maintain the mentioned SLAs in the RFP. The desired roles and responsibilities for SOC manpower is as below.

Note: It is expected that the members involved in this team must lead the team deployed in the "Operation Man power required during HOTO shadowing" for NOC and BMS related activities and Project manager is expected to supervise all activities including Helpdesk. The Shadowing shall continue till confirmation from the MSI or till the delivery of ICT infrastructure under the scope of this RFP, whichever is earlier.

Furthermore, it is expected that the same set of resources as in above phases shall be involved in next phase i.e. "Resources Required during the O&M Phase for DC" in order to take over the operations; and thereafter, for the next phase i.e. "Resources Required during the O&M Phase for BCP"

In case, there is an additional requirement from CRID or some resources are not required in the O&M phase, not compromising the overall SLAs of the RFP and/ or meeting the additional requirements of the Department, the specific manpower rate discovered in the RFP shall be applicable and payments shall be made accordingly till the validity of the contract period.

Sl. No.	**Manpower requirements**	**Job Description**
1	Analyst Tier1 –5 in nos. (24X7) Edu and Experience B.E./ B.Tech/ MCA/ M.Sc. in Computer Science or IT w/ 2+ years of relevant experience	Real-time monitoring of all security appliance(s) like Secure Web/ Email Gateways, Proxy, IPS/ IDS, NGFW, DLP, APT, WAF, Network Forensics, SIEM, NAC etc. in HSDC for security events · Endpoint Threat Detection · Reporting the security events/ incidents to relevant/designated stakeholders (HSDC/ SecLAN/ SWAN/WiFietc. FMS Teams etc.) · Communicating Emergency Alerts & Warnings to relevant/ designatedStakeholders
2	**Analyst** **Tier2 – Required 2 in nos** **1 shift (week days)**	**Incident Analysis** · Incident co-ordination & Response · Remote Incident Response · Forensics Artifact handling & Analysis · Malware Analysis · Insider Threat Case Support · Sensor Tuning & Maintenance

	Edu and Experience B.E./ B.Tech/ MCA/ M.Sc. in Computer Science or IT w/ 3+ years of relevant experience	· Custom Signature/ Rules Creation Scripting & Automation • Audit Collection & Storage • Product Assessment & Deployment • Risk Assessment • Response Planning • Mitigation • Recovery Planning • Communicating Emergency Alerts & Warnings to relevant/ designated stakeholders
3	**Lead Analyst** **Tier 3 : Required 1 in no. 1 shift (week days)** Edu and Experience B.E./ B.Tech/ MCA/ M.Sc. in Computer Science or IT w/ 3+ years of relevant experience	Cyber News Collection & Analysis, Distribution, Creation, Fusion • Local/ Global Threat Feed Tools • Security Trends • SOC Automation • Tradecraft Analysis • Security Consulting & Training • Communicating Emergency Alerts & Warnings to relevant/ designated stakeholders
4	**SOC Manager** **Tier 3 : Required 1 in no. 1 shift (week days)** Edu and Experience B.E./ B.Tech/ MCA/ M.Sc. in Computer Science + CEH + (CISSP/ GCIH/ GSEC/ PMP) or IT w/ 5+ years of relevant experience	Provide the first line supervision to HSDC and to Lead and manage the Security Operations Center • Develop and administer SOC processes and review their application to ensure that SOC's controls, policies, and procedures are operating effectively • Ensure SOC operations are compliant with standards released at time to time by various agencies like CERT-IN, NCIIPC etc. and maintain necessary documentation • Primarily responsible for overall security event monitoring, management and response • Ensure incident identification, assessment, quantification, reporting, communication, mitigation and monitoring • Ensure compliance to SLA, process adherence and process improvisation to achieve operational objectives • Revise and develop processes to strengthen the current Security Operations Framework, Review policies and highlight the challenges in managing SLAs • Responsible for team & vendor management, overall use of resources and initiation of corrective action where required for Security Operations Center • Management, administration & maintenance of security devices under the purview of HSDC which consists of state-of-the art technologies • Perform threat management, threat modeling, identify threat vectors and develop use cases for security monitoring • Creation of reports, dashboards, metrics for SOC operations and presentation to Sr. Mgmt. • Co-ordination with stakeholders, build and maintain positive working relationships with them • Produce and review aggregated performance metrics Manage and increase the effectiveness and efficiency of the SOC, through improvements to each function as well as coordination and communication between support and business functions • Play a significant role in long-term SOC strategy and planning, including initiatives geared toward operational excellence
5	**Application Security Support**	Understanding the overall technical capabilities of any application, typical deployment scenarios- Partner with Help SI/ Department/ Application teams to perform threat

	Required 1 in no. **1 shift (week days)** Edu and Experience B.E./ B.Tech/ MCA/ M.Sc. in Computer Science + CEH/OSCP or IT w/ 4+ years of relevant experience	modeling and drive the associated security requirements. Work closely with SI/ Department teams in assessing the risks, mitigations and preparing responses. – Perform manual and automated application security testing for complex Desktop, Web and Mobile applications to identify vulnerabilities and support the application team in application security audit.

Note:

1. The desired manpower should be CISSP or CISA or equivalent
2. It is to clarify that for posts like "Analyst" where it is mentioned that Tier1 –5 in no.s are required for (24X7) operations, it is implied that minimum ONE Analyst position is required/ stationed onsite for handling 24x7 operations managed in shifts which can be achieved by a minimum of 5 resources.
3. Tier 1, Tier 2, resource must be as per RFP and should be able to perform activities of SOC and adhere on defined SLAs as per RFP.

Apart from the above-mentioned manpower, CRID reserves the right to increase or decrease the number of manpower. The exact role of these personnel and their responsibilities would be defined and monitored by CRID.

The bidders should propose on-site resources to be deployed based on the proposed technical solution. It is expected that there should be minimal human intervention on day-to-day management operations. The minimum experience and certifications for on-site L1 & L2 resources is given below, minimum qualification for L3 & L4 resources is mentioned at Section 6:

Sl. No.	Role	Min. Qualification & Experience
1.	DBA(L3/L2)	BE/B.Tech/MCA with minimum 7 Years of Experience in Database Administration. a. SQL Server related Certification (Mid/ Professional level) b. Cluster management and DC/DR and Failover experience of minimum 3 years c. Must be able to handle Databases like Postgre SQL ,MySQL and Mango DB (No SQL) d. Database Administration Experience of Project value>INR 7 Crores
2.	Network and Security Expert(L2)	BE/B.Tech/MCA with minimum 7Years of Experience in network system provisioning, configuration, and management a. Relevant Firewall OEM related Certification (Mid/Professional Level) as per Bidder's Solution b. Network Security Implementation & Management Experience of Project value > INR 5 Crores
3.	Storage and Backup Expert (L2)	BE/B.Tech/MCA with minimum 5 Years of Experience in Storage Implementation & Management. a. Relevant Storage OEM related Certification (Mid/Professional Level) as per Bidder's Solution b. Storage Implementation & Management Experience of Project value> INR 7 Crores
4.	Server Expert /System Administrator(L2)	BE/B.Tech/MCA with minimum 7 Years of Experience in Server Administration. a. Windows/Linux Server related Certification (Mid/ Professional Level)

		b. Server Administration Experience of Project value > INR 7 Crores
5.	Server Expert /System Administrator(L1)	BE/B.Tech/MCA with minimum 5 Years of Experience in Server Administration / Configuration. a. Windows/Linux Server related Certification (Entry/Associate Level) b. Server Administration/ Configuration Experience of Project value> INR 5 Crores
6.	BMS Expert (L2)	BE/B.Tech/MCA with minimum 5 Years of Experience in BMS Solution Implementation & Management a. Relevant BMS OEM related Certification (Mid/Professional Level) as per Bidder's Solution b. BMS Implementation & Management Experience of Project value> INR 7 Crores
7.	BMS Expert (L1)	a. BE/B.Tech/MCA with minimum 3 Years of Experience in BMS Solution Implementation/Monitoring a. Relevant BMS OEM related Certification (Entry/Associate Level) as per Bidder's Solution b. BMS Implementation/ Monitoring Experience of Project value>INR5Crores
8.	NOC Engineer (L1)	BE/B.Tech/MCA/Polytechnic Diploma (IT) with minimum 3 Years of Experience in Network/Server Configuration/Performance Monitoring.
9.	Help Desk Engineer (L1)	BE/B.Tech/MCA/Polytechnic Diploma (IT) with minimum 2 Years of Experience in IT Infra Helpdesk handling.

i. MSI shall be required to provide such manpower meeting following requirements: i. All such manpower shall be minimum graduates.
ii. All such manpower shall be without any criminal background/record.
iii. CRID reserves the right to carry out background check of the personnel proposed on the Project for verification of criminal record, at the beginning of deployment or during deployment.
iv. MSI shall have to replace any person, if not found suitable for the job.
v. All the manpower shall have to under go training from MSI for atleast 15 working days on the working of project. Training should also cover dos & don'ts.
vi. NOC Manpower shall working shifts, with no person being made to see the NOC Screen for more than 8 hours at a stretch.

Detail operational guideline document, standard operating procedure, governance, and oversight plan shall be repaired by MSI during implementation which shall specify detail responsibilities of these resources and their do's & don'ts.

The supervisors required for operationalization of the project will be provided by CRID, as per requirements.

Change Management & Control

Change Orders/Alterations/Variations

a) MSI agrees that the requirements given in the Bidding Documents are minimum requirements and are only indicative. The vendor would need to fetch out the details at the time of preparing the design document prior to actual implementation. It shall be the responsibility of MSI to meet all the requirements of technical specifications contained in the RFP and any upward revisions and/or additions of quantities, specifications sizes given in the Bidding Documents required to be made during execution of the works, shall not constitute a change order and shall be carried out without a change order and shall be carried out without any time and cost effect to Purchaser.

b) Further upward revisions and or additions required to make MSI's selected equipment and installation procedures to meet Bidding Documents requirements expressed and to make entire facilities safe, operable and as per specified codes and standards shall not constitute a change order and shall be carried out without any time and cost effect to Purchaser.
c) Any upward revision and/or additions consequent to errors, omissions, ambiguities, discrepancies in the Bidding Documents which MSI had not brought out to the Purchaser's notice in his bid shall not constitute a change order and such upward revisions and/or addition shall be carried out by MSI without any time and cost effect to Purchaser.
d) The Change Order will be initiated only in case(i) the Purchaser directs MSI in writing to include any addition to the scope of work covered under this Contract or delete any part of the scope of the work under the Contract, (ii) MSI requests to delete any part of the work which will not adversely affect the operational capabilities of the facilities and if the deletions proposed are agreed to by the Purchaser and for which cost and time benefits shall be passed on to the Purchaser,(iii) the Purchaser directs in writing MSI to incorporate changes or additions to the technical specifications already covered in the Contract.
e) Any changes required by the Purchaser over and above the minimum requirements given in the specifications and drawings etc. included in the Bidding Documents before giving its approval to detailed design or Engineering requirements for complying with technical specifications and changes required to ensure systems compatibility and reliability for safe operation (As per codes, standards and recommended practices referred in the Bidding Documents)and trouble free operation shall not be construed to be change in the Scope of work under the Contract.
f) Any change order comprising an alteration which involves change in the cost of the works (which sort of alteration is here in after called a "Variation")shall be the Subject of an amendment to the Contract by way of an increase or decrease in the schedule of Contract Prices and adjustment of the implementation schedule if any.
g) If parties agree that the Contract does not contain applicable rates or that the said rates are in appropriate or the said rates are not precisely applicable to the variation in question, then the parties shall negotiate a revision of the Contract Price which shall represent the change in cost of the works caused by the Variations. Any change order shall be duly approved by the Purchaser in writing.
h) Within ten (10) working days of receiving the comments from the Purchaser or the drawings, specification, purchase requisitions and other documents submitted by MSI for approval, MSI shall respond in writing, which item(s) of the Comments is/are potential changes(s) in the Scope of work of the RFP document covered in the Contract and shall advise a date by which change order(if applicable)will be submitted to the Purchaser.
i) The successful bidder will not be allowed to provide equipment/solution different from the proposed in the BOM at the time of proposal submission. However, if for reasons beyond the control of the bidder, the proposed line items in the BOM are untenable during the project term, the MSI may be allowed (subject to the approval of State) to provide a similar or higher equipment /solutions which must meet all RFP requirements, without any cost escalation subject to following restrictions:
    - OEM of respective products shall remain the same;
    - Product should meet all functionalities listed in the RFP.
    - OEM must provide a representation that the product proposed as a replacement is similar or of higher version/configuration than the previously proposed product.

Roles and Responsibilities

MSI is responsible for executing this contract and delivering the services, while maintaining the specified performance targets.

Below is the table of the responsibility matrix, providing roles and responsibilities of various stakeholders (CRID, Master System Integrator, PMU and Independent Third-Party Auditor (TPA),etc.) for this engagement during various stages of the engagement. Responsibilities of the Systems Integrator must be complied to and any deviation will mean disqualification of the MSI For the table given below, following is the terminology which is being used:

R–Responsible: who is responsible for carrying out the entrusted task

A–Approval: who is responsible for the approving the engagement tasks/activities

S–Support: who provides support during implementation of activity/process/service

C–Consulted: who can provide valuable advice or consultation for the task

I–Informed: who should be informed about the progress or the decisions in the task

Sl. No.	Activities	CRID	PMC	Present MSI	MSI	Line Department
	Handover Takeover					
1	Project Kick Off Presentation	C	C	I	R	
2	Share the Exit Management Plan of Current MSI To MSI	A	C	I	R	
3	Study of Exit Management Plan	I		R	R	
4	Preparation of road map for HOTO	I	S	C	R	
5	Presentation of Roadmap to CRID	I	I	I	R	I
6	Approval of Roadmap	A	C	I	R	C
7	Knowledge transfer sessions	I	C	R	R	
8	Documentation of Knowledge Transfer and Sign off	I	S	R	R	
9	Shadowing of Operations by MSI	I		R	R	
10	Weekly progress reporting	I		I	R	
11	Operations take over by selected MSI from Existing MSI	C	C	I	R	
12	Sign off on HOTO Report	A	C	C	R	I
13	Exit of existing MSI	A	I	R	I	I
	Gap Analysis and Requirements Study					
14	Resource mobilization for the Gap assessment Study	C	C	I	R	I
15	Detailed study of the Infrastructure and Application Landscape (MS)	C	C		R	
16	Detailed study of the Infrastructure and Application Landscape(Co-Lo)	C	C		R	C
17	Preparation of the inventory detailing the EoL and EoS of active equipment	C			R	C
18	Preparation of the report detailing the usage of the active equipment				R	C
19	Preparation of Upgradation, DC Consolidation& Capacity Augmentation Plan for next 12 months	A	S		R	C
20	Draft Implementation Roadmap Highlighting the dependencies	A			R	C
21	Assist CRID in detailing procurement requirements	A			R	
	Phase-II Supply, Installation, Testing and Commissioning ICT of the ICT Infrastructure for HSDC Chandigarh					
22	Discussion with CRID for drafting the Cloud Vision Roadmap & FRS	A	C		R	C

Sl. No.	Activities	CRID	PMC	Present MSI	MSI	Line Department
23	Consultative discussion with Line Departments to visualize the Cloud Adoption trend /scalability requirement	A	I		R	R
24	Presentation of Hybrid Cloud Vision Roadmap & FRS	I	I		R	I
25	Vetting of Design document by CRID	A	S		R	C
26	Installing and Commissioning of Hardware & Software including network, storage, compute, EMS and other ICT infra as per RFP	C	C		A	I
27	Integration of the implemented cloud with the existing cloud	A	C		R	
28	Implementation of Self Service Portal	A	C		R	I
29	Planning and Implementation of EMS	A	C		R	
30	UAT&FAT	A	I		R	I
31	Migration support for Compute and Application & dB Stack	A	I		R	R,A,C
32	Go-Live and O&M by MSI	A	C		R	
	Phase-II Operations and Maintenance Phase					
31	Operations & Management of the Data Centre infrastructure as per SLA (Managed Hosting, Co-Location and Cloud Infrastructure)	A			R	
32	Responsibility for all backup of the data stored on the SAN as well as servers, bought under this RFP.	A			R	
33	Media responsibility for any other backup activity related to line Department	A			R	
34	Recurring expenditure like bandwidth charges, electricity, diesel ,etc.	A				
35	Provisioning of Rack Space for Hosting of Co- Located Infrastructure	A	I		R	C
36	Provisioning of IaaS and PaaS services as Requested	A	I		R	C
37	24*7single point technical support to CRID and Line Departments	A	I		R	
38	ISO20000,ISO27001,ISO22301,ISO 27017 and ISO27018 Compliance	A	C		R	I
39	Provisioning of IaaS and PaaS Services	A	I		R	C
40	Closing of open issues post Infra and Security Audit	C	I		A	C
41	Migration support for Compute and Application & dB Stack	A	I		R	R,A,C
42	Infrastructure & Operations Rationalization Study	I	C		R,A	

Other Roles and Responsibilities:

4.1.1.1. Responsibilities of the MSI

a) MSI shall prepare and then seek approval from CRID on all the ICT infrastructure solution architecture, diagrams and plans before commencement of installation.
b) MSI shall follow Change Management Procedures, Information Security Policies as suggested by CRID.

c) MSI shall ensure proper handover /takeover of documents & other relevant materials in the event of change in personnel.
d) The MSI shall share and review all internal documents/ reports used to monitor & execute the project with CRID as and when desired.
e) MSI shall proactively interact with other vendors / third parties / OEMs to ensure that the equipment is upgraded and maintained at a periodic interval. CRID would only pay the services charges applicable for operations and maintenance of the Data Centre.
f) The MSI would manage all aspects of Vendor management

Responsibilities of CRID

CRID shall provide approvals & sign-offs to the deliverables with in the stipulated time period. CRID shalldirect and monitor the activities performed by the MSI as per the Tender Document and in turn validate the service levels attained as per the SLA document. CRID will also be responsible for the following activities:

i. Internet Bandwidth at HSDC
ii. P2P Connectivity link from HSDC to DR on Cloud
iii. Power supply from multiple grid at HSDC
iv. AMC for servers/storage provided for Co-Lo rack
v. AMC of all equipment upto Go-Live of project.
vi. AMC of existing HCI.

Project Team Requirement

Sl. No.	Role	Min. Qualification & Experience
1.	Project Manager (L4)	Mandatory: Educational Qualification in BE / B. Tech / M.Tech / MCA from recognised Institute, with PGDM/ MBA from recognised Institute. a. Certification in PMP/ Prince2 Practitioner b. Minimum 15 Years' Experience, out of which, 5 years in the capacity of Project/Program Manager in ICT implementation projects c. Minimum 2 Years' Experience of Project of Data Centre Implementation / O&M : d. Minimum 2 Years' Experience in managing Cloud Service Project
2.	Solution Architect – Cum-DBA (L3)	Mandatory: Educational Qualification in BE / B. Tech / MCA with minimum 10 Years of Experience in Database Administration. a. SQL Server related Certification (Expert level): 1 mark b. Database Administration Experience of Project value > Rs. 10 Crores: 1 mark
3.	DC-DR Cloud Solution Expert (L3)	Mandatory: Educational Qualification in BE / B. Tech / MCA and 7+ Years of Experience in Cloud Solution Implementation, Management and Operations a. Two Years' Experience in Cloud Migration: b. Certification (Expert Level) of Relevant Cloud OEM as per Bidder's Solution: 1 mark
4.	Network and Security Expert (L3)	Mandatory: Educational Qualification in BE / B. Tech / MCA with minimum 7 Years of Experience in network system provisioning, configuration, and management a. Relevant Firewall OEM related Certification (Expert Level) as per Bidder's Solution, such as CCNA/ CCNP/ComTIA/JNCIA: 0.5 Mark b. Network Security Implementation & Management Experience of Project value > Rs. 10 Crores:
5.	Storage and Back up Expert (L3)	Mandatory: Educational Qualification in BE / B. Tech / MCA with minimum 7 Years of Experience in Storage Implementation & Management. a. Relevant Storage OEM related Certification (Expert Level) as per Bidder's Solution: 1 mark b. Storage Implementation & Management Experience of Project value > Rs. 10 Crores:
6.	Server Expert	Mandatory: Educational Qualification in BE / B. Tech / MCA with minimum

Sl. No.	Role	Min. Qualification & Experience
	/System Administrator (L3)	10 Years of Experience in Server Solution & Management. a. Windows/Linux Server related Certification (Expert Level): 1 mark b. Server Administration Experience of Project value > Rs. 10 Crores:
7.	BMS Expert (L3)	Mandatory: Educational Qualification in BE / B. Tech / MCA with minimum 7 Years of Experience in BMS Solution Implementation & Management a. Relevant BMS OEM related Certification (Expert Level) as per Bidder's Solution : b. BMS Implementation & Management Experience of Project value > Rs. 10 Crores : 1 mark

Key Personnel Criteria

MSI shall provide adequate number of personnel, each responsible for a specific role within the project. MSI shall provide clear definition of the role and responsibility of each individual personnel.

MSI shall have a defined hierarchy and reporting structure for various teams that shall be part of the project. MSI must provide the list of proposed Manpower for the Project. Any changes in Manpower deployment post submission of the proposal will have to be approved by the CRID.

However, beside these mandatory deployments, MSI shall independently estimate the teams size required to meet the requirements of Service Levels as specified as part of this tender.

All other proposed positions shall be Onsite throughout the entire project implementation phase.

Project Plan

Within 15 calendar days of the Effective Date of the contract/Issuance of LoI, MSI shall submit a project plan to the designated authority for its approval a detailed Project Plan with details of the project showing the sequence, procedure, and method in which it proposes to carry out the works. The Plan so submitted by MSI shall conform to the requirements and timelines specified in the Contract. The designated authority and MSI shall discuss and agree upon the work procedures to be followed for effective execution of the works, which MSI intends to deploy and shall be specified. The Project Plan shall include but not be limited to project organization, communication structure, proposed staffing, roles and responsibilities, processes, and toolsets to be used for quality assurance, security, and confidentiality practices by industry best practices, project plan, and delivery schedule by the Contract. Approval by the designated authority's Representative of the Project Plan shall not relieve MSI of any of his duties or responsibilities under the Contract.

If MSI's work plans necessitate a disruption/ shutdown in the designated authority's operation, the plan shall be mutually discussed and developed to keep such disruption/shutdown to the barest unavoidable minimum. Any time and cost arising due to the failure of MSI to develop/adhere to such a work plan shall be to his account.

A Detailed Project Plan covering the break-up of each phase into the key activities, along with the start and end dates must be provided as per the format given below.

Activity-Wise Timelines											
Sl. No.	Item of Activity	Month wise Program									
1	Project Plan										
1.1	Activity1										

1.2	Sub-Activity1										

Note: The above activity chart is just for illustration. Bidders are requested to provide detailed activity &phase-wise timelines for executing the project with details of deliverables &milestones as per their bid.

Manpower Plan

Manpower distribution								
S. No.	**Name**	**Role**	**Month wise time to be spent by each personnel (in days)Total**					
			Month1	Month2	Month3	- -	- -	-- -
1		Project Manager (L4)						
2		Solution Architect–Cum-DBA(L3)						
3		DC-DR Cloud Solution Expert (L3)						
4		Network and Security Expert (L3)						
5		Storage and Backup Expert (L3)						
6		Server Expert /System Administrator (L3)						
7		BMS Expert (L3)						

Name					
1.	**Proposed position or role**	(Only one candidate shall be nominated for each position)			
2.	**Date of Birth**		**Nationality**		
3.	**Education**	**Qualification**	**Name of School or College or University**	**Degree Obtained**	**Year of Passing**
4.	**Years of Experience**				
5.	**Areas of Expertise and no. of years of experience in this area**	(as required for the Profile)			
6.	**Certifications and Training at tended**				
7.	**Employment Record**	**Employer**	**Position**	**From**	**To**
		[Starting with present position and last 2 firms, list in reverse order, giving for each employment : dates of employment, name of employing organization, positions held.]			
8.	**Detailed Tasks Assigned**	(List all tasks to be performed under this project)			

Curriculum Vitae (CV) of Team Members

Name		
1.	**Proposed position or role**	(Only one candidate shall be nominated for each position)

2.	**Date of Birth**		**Nationality**		
3.	**Education**	**Qualification**	**Name of School or College or University**	**Degree Obtained**	**Year of Passing**
4.	**Years of Experience**				
5.	**Areas of Expertise and no. of years of experience in this area**	(as required for the Profile)			
6.	**Certifications and Training attended**				
7.	**Employment Record**	**Employer**	**Position**	**From**	**To**
		[Starting with present position and last 2 firms, list in reverse order, giving for each employment : dates of employment, name of employing organization ,positions held.]			
8.	**Detailed Tasks Assigned**	(List all tasks to be performed under this project)			

3.10 EXIT MANAGEMENT

a) This sets out the provisions, which will apply on expiry or termination of the Master Service Agreement, the Project Implementation, Operation and Management SLA.
b) In the case of termination of the Project Implementation and/or Operation and Management, the Parties shall agree at that time whether, and if so during what period, the provisions of this Schedule shall apply.
c) The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Schedule.

Purpose

This clause sets out the provisions, which will apply during Exit Management period. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Clause.

The exit management period starts, in case of expiry of contract, at least 3 months prior to the date when the contract comes to an end or in case of termination of contract, on the date when the notice of termination is sent to the MSI. The exit management period ends on the date agreed upon by CRID or Three months after the beginning of the exit management period, whichever is earlier.

Exit Management Plan

MSI shall provide the CRID or its nominated agency with a recommended exit management plan ("Exit Management Plan") which shall deal with at least the following aspects of exit management in relation to the MSA as a whole and in relation to the Project Implementation, and the Operation and Management SLA.

- A detailed program of the transfer process that could be used in conjunction with a Replacement MSI including details of the means to be used to ensure continuing

provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;

- Plans for the communication with such of MSI's sub-contractors, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on the CRID's operations as a result of undertaking the transfer;
- Proposed arrangements for the segregation of MSI's networks from the networks employed by CRID and identification of specific security tasks necessary at termination(if applicable);
- Plans for provision of contingent support to CRID, and Replacement MSI for a reasonable period after transfer.

a) MSI shall re-draft the Exit Management Plan annually there after to ensure that it is kept relevant and up to date.
b) Each Exit Management Plan shall be presented by MSI to and approved by the CRID or its nominated agencies.
c) The terms of payment as stated in the Terms of Payment Schedule include the costs of MSI complying with its obligations under this Schedule.
d) In the event of termination or expiry of MSA, and Project Implementation, each Party shall comply with the Exit Management Plan.
e) During the exit management period, MSI shall use its best efforts to deliver the services.
f) PaymentsduringtheExitManagementperiodshallbemadeinaccordancewiththeTermsofPaymentSchedule.In Case the exit management due to termination, the payment shall be made for the deliverables after deducting applicable penalties and/or SLAs.
g) This Exit Management plan shall be furnished in writing to the CRID or its nominated agencies within 90 days from the Effective Date of this Agreement.

Cooperation and Provision of Information

During the exit management period:

- MSI will allow the CRID or its nominated agency access to information reasonably required to define the then current mode of operation associated with the provision of the services to enable the CRID to assess the existing services being delivered;
- Promptly on reasonable request by the CRID,MSI shall provide access to and copies of all information held or controlled by them which they have prepared or maintained in accordance with this agreement relating to any material aspect of the services (whether provided by MSI or sub-contractors appointed by MSI). The CRID shall be entitled to copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. MSI shall permit the CRID or its nominated agencies to have reasonable access to its employees and facilities, to understand the methods of delivery of the services employed by MSI and to assist appropriate knowledge transfer.

Confidential Information, Security and Data

MSI will promptly on the commencement of the exit management period supply to the CRID or its nominated agency the following:

- Information relating to the current services rendered and customer and performance data relating to the performance of sub-contractors in relation to the services.
- Documentation relating to Intellectual Property Rights.
- Documentation relating to sub-contractors.
- All current and updated data as is reasonably required for purposes of CRID or its nominated agencies transitioning the services to its Replacement MSI in a readily available format nominated by the CRID, its nominated agency.
- All other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable CRID or its nominated agencies ,or its Replacement MSI to carry out due diligence in order to transition the provision of the Services to CRID or its nominated agencies, or its Replacement MSI (as the case may be).

Before the expiry of the exit management period, MSI shall deliver to the CRID or its nominated agency all new or up-dated materials from the categories set out in Schedule above and shall not retain any copies thereof, except that MSI shall be permitted to retain one copy of such materials for archival purposes only.

Transfer of Certain Agreements

On request by the CRID or its nominated agency MSI shall effect such assignments, transfers, licenses and sub- licenses CRID, or its Replacement MSI in relation to any equipment lease, maintenance or service provision agreement between MSI and third party lessors, vendors, and which are related to the services and reasonably necessary for the carrying out of replacement services by the CRID or its nominated agency or its Replacement MSI. SPLA licenses under DR environment will be provided as a service to CRID.

Employees

Promptly on reasonable request at any time during the exit management period, the MSI shall, subject to applicable laws, restraints and regulations (including in particular those relating to privacy) provide to CRID a list of all employees (with job titles and communication address) of the Successful MSI, dedicated to providing the services at the commencement of the exit management period; To the extent that any Transfer Regulation does not apply to any employee of the Successful MSI, CRID or Replacing

Vendor may make an offer of contract for services to such employee of the Successful MSI and the Successful MSI shall not enforce or impose any contractual provision that would prevent any such employee from being hired by CRID or any Replacing Vendor.

General Obligations of MSI

a) General Obligations of MSI a) MSI shall provide all such information as may reasonably be necessary to effect as seamless a handover as practicable in the circumstances to the CRID or its nominated agency or its Replacement MSI and which MSI has in its possession or control at any time during the exit management period.
b) For the purposes of this Schedule, anything in the possession or control of any MSI, associated entity, or sub- contractor is deemed to be in the possession or control of MSI.
c) MSI shall commit adequate resources to comply with its obligations under this Exit Management Schedule.

3.11 SERVICE LEVELS

a. The MSI shall be submitting monthly SLA reports to CRID. CRID may appoint a Third Party Agency to audit the performance, accuracy and integrity of the tools generating SLA data and also review the monthly SLA reports for SLA penalty computation.
b. If the MSI is getting penalized on two or more parameters because of one incident, then the MSI may seek exemption from getting penalized on the parameters resulting in the least amount of penalty. CRID may exercise its discretion in granting such exemptions.
c. Severity of services are given below. CRID reserve the right to define Severity/Priority levels of services not mentioned below. The Severity level of each service defines by its importance in the infrastructure and its impact in case of failure as detailed below.
d. For certain incidents, RCA may be carried out by CRID.
e. **In case of Penalty reached the maximum limit as per the limit mentioned in respective clause,** then the performance of the MSI will be reviewed and then CRID may take appropriate action including termination of the contract and invoking the Performance Bank Guarantee.
f. If SLA penalty calculations (during O&M phase) exceed 15% of the quarterly payment **for three consecutive quarters** or 25% in any quarter, then CRID may take appropriate action including termination of the contract and invoking the Performance Bank Guarantee**.**
g. The MSI shall bring the necessary tools required to measure the SLA parameters mentioned in this Agreement.

h. The MSI must comply to the Government policies and requirements as per guidelines and orders.

Table : Definitions of Severity Levels

Severity Level	Priority Type	Definition
Severity1	Critical	Denial of data centre services/ standard compliance due to Total breakdown/failure of any one of the equipment/components installed in HSDC. Apart from this hacking of website/data/virus attacks (malicious code)effecting database system, system software, data etc.
Severity2	Major	Denial of Services/standard compliance due to partial break down/failure of any one of the equipment/ components installed in the HSDC
Severity3	Minor	Partial/ breakdown of any equipment/ component installed in the HSDC without disrupting any services and failure/delay in undertaking and completing activities.

Denial of services due to failure of any device/Equipment/ services/ users supplied under this RFP shall be treated as per respective Severity Level mentioned in table below (indicative list only and is non exhaustive)

Severity1	Severity2	Severity3
• Access Control Server Failure • Anti-virus server Failure • Active Directory Failure • BMS Service Failure • Backup Server Failure • Cluster Service Failure • Controller Failure • DNS Service Failure • Directory Service Failure • Database Failure • Database Node/ Instance Failure • Firewall Failure • Genset Failure • IPS Failure • Load Balancer Failure • LT Panel Failure • Power Failure to Rack(s) • PAC Failure • Router Failure • RAID Controller Failure • Switch Failure • SAN Switch Failure • Storage Failure • Server/ System Failure • Storage System Related Issues • Security Component failure of Server Farm Area. • Sync Panel Failure • Tape Library Failure • UPS Failure	• Agent- Installation, Configuration, Modification, Un-installation • Backup- New Backup request, New Policy, Change in Policy etc. • Failure of physical infrastructure components related to humidity control and comfort air conditioning other than server farm area • Fibre Optic cable failure • Failure of Modules/ Slot • Firmware Upgrade • HBA Failure • IOS- Update, Upgrade, Downgrade • IDS/IPS Policy updating as per new requirement • InfoSec Incidents (IT-Critical) • InfoSec Incidents (Non-IT-Critical) • Tape Drive Failure • LUN's /Storage Volumes-Allocation, add to Existing, Delete, Issue, etc. • Port Failure • PSU /Cooling Fan Failure • Passive Cable	• Adding new devices to fabric • OS installation, Un-installation • Patch- Update, Remove • Threshold Alarm (Major) • H/W up-gradation • Anti-virus updates • Printer- Cartridge Change • Coolant for genset • Desk Phone- New Allotment, Shifting • Data- Archival, Restoration • Database- New User Request, Modify user access rights, removal/ disable user • Planned Maintenance • User Management- New user, Removal of User • Access Card- New card request, Issue, Removal/ Assigning rights, etc. • Backup Policy • FTP service- New User, Password Reset, Access Modification, Removal of User, etc. • Power Failure to PDU • PDU requirement • Patch Cord Request • RCA Report

• VTL Failure • Virtualisation Network Failure • Virtualisation Infrastructure Failure • Threshold Alarm (Critical)	component connecting the above equipment's • Signature Update • Server Reboot Request • User Account Locked • VM Provisioning Failure	• IP Address- New request, Removal • InfoSec Incidents (IT-Critical) • InfoSec Incidents (Non-IT-Critical) • Security Incident Report • VPN Service- New Request, Issue • VNC/ Remote Login- New Request, Issue • Printer Issue

Table: Service level details

Severity Level	Priority type	Response time	Service Window	Resolution Time
Severity1	Critical	15 Minute of call logged	24*7	Within 4 hours of call logged or a workaround is in place
Severity2	Major	30 Minute of call logged	24*7	Within 8 hours of call logged
Severity3	Minor	30 Minute of call logged	7 AM to 7 PM (Monday to Friday)	Within 2 days of call logged

Penalty Clauses

Service Level parameters defined in this section shall be monitored on a periodic basis, as per the individual parameter requirements. MSI shall be responsible for providing appropriate web based online SLA measurement and monitoring tools and it is also proposed to have an independent technical auditor, third party appointed by the authority for monitoring the Service levels. MSI shall be expected to take immediate corrective action for any breach in SLA. In case issues are not rectified to the complete satisfaction of Authority, within a reasonable periodof time defined in this RFP, then the Authority shall have the right to impose penalty as per the terms of the RFP, or termination of the contract.

Penalties for Non-Performance

a) Performance Penalty for not meeting a measurement parameter for any two months in consecutive quarters shall result in twice the penalty percentage of that respective measurement parameter in the third quarter for all the three months.

b) The payment to the agency shall be on Quarterly basis however the penalty shall be calculated on monthly basis as per the SLAs stated in the RFP.

The Service Level agreements have been logically segregated in the following categories:

1) HOTO Phase SLAs
2) Manpower deployment SLAs
3) Implementation Phase SLAs
   a) Delivery of all ICT components (Hardware + Software) SLAs
   b) Private Cloud Implementation & Integration SLAs
   c) Centralized SDC Service Desk & Self-service portal SLAs
   d) Infrastructure Consolidation and Rationalization Study SLAs
4) Operations & Maintenance Phase SLAs
   a) Equipment/ Application uptime SLAs
   b) Technical Support desk SLAs
   c) Compliance and Reporting Procedures SLAs
   d) Security anagement SLAs on-IT Infrastructure related SLA

Note: O&M SLAs will be applicable for all applications hosted at DC and DR whether in active – active or active-passive mode

Hand Over Takeover (HOTO) SLAs

Measurement	Target	Penalty
Milestone-Submission of documents: Hand Over and Take Over completion report Sign-off. **T→ WO Date/Agreement Date**	T+4Weeks	Nil
	>T+4Weeksto <=T+6Weeks	Penalty at **0.10%** shall be imposed on the CAPEX value quoted by the MSI
	>T+6weeks	Penalty at **0.2%** per week shall be imposed on the CAPEX value quoted by the MSI

Manpower deployment SLAs

Measurement	Target	Penalty
Milestone – Submission of documents, HOTO Manpower	T+4 Week	Nil
	>T+4Weekto<=T+6 Weeks	Penalty at **0.2%** shall be imposed on the total CAPEX value quoted by the MSI
	>T+6 Week	Penalty at **0.2%** per week shall be imposed on the total CAPEX value for non deployment of 100% of required manpower
Milestone-Commissioning, UAT, Go-Live with hands-on training/ hand-holding. Declaration of start of O&M: O&M Manpower	**T+47 Weeks**	Nil
	>T+47 Weeks	Inability of MSI to deploy manpower resource/resource as per Manpower requirements specified in RFP, will attract a penalty of double the amount payable to MSI for the resource/resources during that period as per manpower payment terms

Measurement	Target	Penalty
Milestone-Commissioning, UAT, Go-Live with hands-on training/ hand-holding. Declaration of start of Centralized SDC Service Desk & Self-service portal	T+ 4 weeks	Nil
	>T+4Weekto <=T+6weeks	Penalty at **0.05%** shall be imposed on the total CAPEX value quoted by the MSI
	>T+6Week	Penalty at **0.1%** per week shall be imposed On the Total CAPEX value for every subsequent week thereof

Implementation Phase SLAs

The following measurements and targets shall be used to track and report performance during implementation phase

Delivery of all ICT components (Hardware + Software) SLA

Measurement	Target	Penalty
Milestone- Delivery of all BoQ items required for State Data Center and Far DR: Delivery of all ICT components (Hardware + Software)	**T+20 Weeks**	Nil
	>T+20 Weeks to <=T+24 Weeks	Penalty at 0.5% shall be imposed on the respective CAPEX value for State Data Center and Far DR
	>T+24Weeks	Penalty at 0.25% per week shall be imposed on the respective CAPEX value for State Data Center and Far DR for every subsequent week Thereof

Measurement	Target	Penalty
Milestone Delivery of all BoQ items required for Near Line BCP Site: Delivery of all ICT components (Hardware + Software)	**T+31 Weeks**	Nil
	>T+31Weeks to <=T+35 Weeks	Penaltyat0.5%shallbeimposedonthere spective CAPEX value for Near Line BCP Site
	>T+35 Weeks	Penalty at 0.25% per week shall be imposed on the respective CAPEX value for Near Line BCP Site for every subsequent week Thereof

Go-Live & Integration SLAs

Measurement	Target	Penalty
Milestone- Commissioning, UAT, Go-Live with hands-on training/ hand-holding. Declaration of start of O&M: FAT of DC Site & Far DR site	**T+47 Weeks**	Nil
	>T+47Weeks to <=T+50 Weeks	Penaltyat0.5%shallbeimposedonthe respective CAPEX value for DC Site & Far DR site
	>T+50 Weeks	Penalty at 0.25% per week shall be imposed on the respective CAPEX value for DC Site & Far DR sitefor every subsequent week thereof

Measurement	Target	Penalty
Milestone- Commissioning, UAT, Go-Live with hands-on training/ hand-holding. Declaration of start of O&M: FATof Near Line BCP Site	**T+56 weeks**	Nil
	>T+56 Weeks to<=T+60 Weeks	Penalty at 0.5% shall be imposed on the respective CAPEX value for Near line BCP site
	>T+60 Weeks	Penalty at 0.25% per week shall be imposed on the respective CAPEX value for Near line BCP site for every subsequent week thereof

Infrastructure Consolidation and Rationalization Study SLAs

Measurement	Target	Penalty
Milestone -Perform SDC, near line BCP and Far DR Drills to check functionality: Sign-off of consolidation and capacity augmentation plan	**T+ 60 Weeks**	Nil
	>T+ 60 Weeks to <=T+64 Weeks	Penalty at 0.5% shall be imposed on the Total CAPEX value
	>T+ 64 Weeks	Penalty at 0.25% per week shall be imposed on the Total CAPEX value for every subsequent week thereof

Measurement Matrix

a. **Response Time:** Response time is the total time taken registering the complaint at Helpdesk or through web telephone to reach the user.

Response time %= [(Calls Responded Time – Call Logged Time)/ Total Quarterly Calls] * 100

b. **Resolution Time:** The total time taken registering the complaint at Helpdesk or through web telephone at respective location and rectifying the fault. This time includes time taken to reach the site, diagnose, installation, configuration and repair of operating systems and all other applicable software including anti-virus software; escalation of call or other applicable third party for resolution of the call as per requirement; installation, shifting/ reinstallation of systems along with applicable software; and any other applicable FMS services etc. to make the system functional as per requirement.

Resolution time %= [(Calls Resolution Time – Call Logged Time)/ Total Quarterly Calls] * 100

Penalty Calculation

a. Actual vs Target Compliance Level for each of the respective service are as will be measured separately I n every quarter.
b. Short fall in achieving SLA Compliance, if any will be calculated on the quarterly basis.
c. Penalty amount will be calculated as per the criteria mentioned in penalty clause, maximum penalty amount would not exceed more than 10% of CAPEX.
d. Incidents will be logged and the MSI will have to resolve the incident and provide necessary update through the helpdesk portal and coordinate with the stake holders. Root Cause should be identified for all incidents; if root cause is not identified the additional penalties will be levied.
e. The breach of SLA compliance with direct impact to the performance of the manpower deployed by MSI will result in computing the penalty towards Manpower service provided instead here.
f. Quality of Services (QoS) is the overall performance of Helpdesk response and resolution time taken from incidents along with responsibilities of manpower deployed by MSI for the resolution of incidents raised through helpdesk service particularly the performance experienced by CRID. Based on the same, penalty may be deducted on the manpower deployed for critical services by server expert, storage expert, security expert, database expert, EMS & BMS expert etc. Other than the absence of resource, replacement etc. will be computed based upon the manpower resource service levels.

IMPLEMENTATION AND OPERATIONS & MAINTENANCE PHASE SLAS

The following measurements and targets shall be used to track and report performance during operation and maintenance phase and after HOTO till FAT (wherever applicable, as mentioned specifically in sub-sections). The targets shown in the following table are applicable for the duration of the contract:

Data Centre, Near Line DC and FAR DR Overall UPTIME SLA

Penalty for Service and Equipment Failure (for the Data Centre, Near Line BCP and Far DR site ICT infrastructure components supplied and installed under this project) shall be calculated on the basis of total Service failure and individual Equipment / Part.

Sl. No	Measurement	Target uptime (Quarterly)	Penalty
1.	Over All Uptime for Data Center and Near Line BCP Site and Far DR site: calculated for Site individually	99.982%	No Penalty
		>=99.5% to <99.982%	1% of the total PBG value
		>=99.0%to<99.5%	2% of the total PBG value
		<99.0%	0.1% of the total PBG for every 3 hours of down time at stretch in parts upto total downtime in addition to the penalty mentioned above.

Note: Over all Data Centre uptime related penalties shall be governed by the following conditions:

a) T=Date of acceptance of LOI.
b) Uptime will be measured on quarterly basis as specified Uptime %= (((Overall Total Uptime - Overall Planned downtime) - Overall Downtime) *100)/(Overall Total Uptime - Overall Planned downtime)

c) The Penalty shall be calculated on quarterly basis as per the target specified.
d) Maintenance may include scheduled maintenance or any other maintenance required to ensure continuity of Data Centre operations. Any downtime for maintenance shall be with prior written intimation to CRID.
e) If downtime of system or subsystem affects the operation of other systems, then vendor has to pay penalty for the affected systems also.

Equipment/Application uptime SLAs

Penalty for Service and Equipment Failure (for the Data Centre, Near Line BCP and Far DR site ICT infrastructure components supplied and installed under this project) shall be calculated on the basis of total Service failure and individual Equipment/Part. In case when both total Service failure and individual Equipment/Part failure are applicable, the higher one shall be charged. Penalty for Service and Equipment Failure **as per SLA period** shall be deducted from **Annual O&M Cost** or any payment to be released to MSI or from the Performance Bank Guarantee.

IT/Non-IT Equipment are divided into two broad categories

Type-I**:** All Critical Equipment such as Core Switch, Core Router, All Security equipment, TOR Switch, EMS, Service portal, Spine and Leaf Switch, PAC,UPS, DG, Virtual Machines and Server, Storage ,Backup devices etc.

Type-II: Desktops, Monitors, Access switches not used for Type-I equipment connectivity

Sl. No	Measurement	Target uptime (Monthly)	Penalty
1.	Uptime for Data Center and Near Line BCP Site: calculated for each IT equipment (Type-I)	99.982%	No Penalty
		>=99.5% to <99.982%	1% of the yearly PBG value
		>=99.0%to<99.5%	2% of the yearly PBG value
		<99.0%	0.1% of the yearly PBG for every 3 hours of down time at a stretch or in parts upto total downtime in addition to the penalty mentioned above.

			This downtime should be calculated over and above the total hours of downtime permissible till 99.00% availability
2.	Uptime for Data Center and Near Line BCP Site: calculated for each IT equipment (Type-II)	99.982%	No Penalty
		>=99.5%to<99.982%	Rs. 5000
		>=99.0%to<99.5%	Rs. 10000
		<99.0%	Rs. 2000 every 3 hours of down time at a stretch or in parts upto total downtime in addition to the penalty mentioned above. This downtime should be calculated over and above the total hours of downtime permissible till 99.00% availability
3.	EMS/OS/Portal Uptime calculated for each component.	99.982%	No Penalty
		>=99.5%to< 99.982%	1% of the yearly PBG value
		>=99.0%to< 99.5%	2% of the yearly PBG value
		<99.0%	0.1% of the yearly PBG for every 3 hours of down time at a stretch or in parts upto total downtime in addition to the penalty mentioned above. This downtime should be calculated over and above the total hours of downtime permissible till 99.00% availability
4.	Uptime of Co-Located Devices, calculated for each IT equipment supplied by MSI	99.982%	No Penalty
		>=99.5%to< 99.982%	1% of the yearly PBG value
		>=99.0%to< 99.5%	2%of the yearly PBG value
		<99.0%	0.1% of the yearly PBG for every 3 hours of down time at a stretch or in parts upto total downtime in addition to the penalty mentioned above. This downtime should be calculated over and above the total hours of downtime permissible till 99.00% availability

Note:

- **Yearly PBG value is the Value applicable that year as per PBG Release schedule. For example**
    - **Total PBG Value = Rs 21 C**
    - **For First to2nd year (as per Schedule) : 16% of PBG value = Rs 3.36 Cr.**
    - **If Penalty = 1% of Yearly PBG Value then the Penalty = Rs 3.36 Lakh**
    - **For 3rd year (as per Schedule) : 20% of PBG value = Rs 4.2 Cr.**
    - **If Penalty = 1% of Yearly PBG Value then the Penalty = Rs 4.2 Lakh**
- **Similarly**
    - **For 4th & 5th Year (as per Schedule) = 24% of PBG value = Rs 5.04 Cr**
    - **If Penalty = 1% of Yearly PBG Value then the Penalty = Rs 5.04 Lakh**

:: Equipment Availability Related penalties shall be governed by the following conditions:

a) T=Date of acceptance of LOI.

b) Any malfunction reported (Service failure or performance degradation) for equipment installed in High availability may invoke penalty defined for warranty support but if this malfunction impact over all services of data centre, above SLA will be applicable regarding

uptime calculation.

c) Uptime will be measured on monthly and quarterly basis as specified Uptime % = (((Total Uptime-Planned downtime) - Downtime) * 100)/ (Total Uptime-Planned downtime)

d) The Penalty shall be calculated on weekly, monthly and quarterly basis as per the target specified. The Penalty would be calculated on an incremental basis for each component of the entire ICT Infrastructure affected. For example, if the total number of Leaf Switch affected is 3, the Penalty would be multiplied by 3.

e) Maintenance may include scheduled maintenance or any other maintenance required to ensure continuity of Data Centre operations. Any downtime for maintenance shall be with prior written intimation to CRID.

f) If downtime of system or subsystem affects the operation of other systems, then vendor has to pay penalty for the affected systems also.

g) The downtime shall be the time from the point the respective equipment becomes unavailable (due to any reason attributable to the MSI) till the time the same becomes fully available for carrying out intended operations (including reinstallation, configuration, restoration, boot-uptime, etc.) OR till the time a stand by equipment is made available for carrying out intended operations (including installation, configuration, restoration, boot-uptime, etc.)

h) MSI's SLA will not be affected by any downtime due to network connectivity at HSDC, Near DR and Far DR site, which is not provided by MSI.

i) MSI's SLA will not be affected by any downtime due to power related issues at Near DR & Far DR site.

Technical Support desk SLAs (L1 Support): (From date of HOTO till end of O&M period)

Sl. No	Measurement	Definition	Measurement Interval	Target	Penalty
1.	Response Time	Average Time taken to acknowledge and respond once a ticket/incident is logged through one of the agreed channels. This is calculated for all tickets/incidents reported within the reporting month (24x7x365).	Monthly	15 Minutes	No Penalty
				>15Min	Rs.100 for every 30 minutes of delay on an incremental basis for every Non response Tickets
2.	Resolution Time	"Resolution Time", means time taken by the MSI staff to troubleshoot and fix the problem from the time the ticket has been logged through one of the agreed channels and till the time the problem has been fixed.	Monthly	60 minutes	No Penalty
				>60min	Rs.1000 for every 60 minutes of delay on an incremental basis for every unresolved call.

Compliance and Reporting Procedures SLAs (From date of HOTO till end of O&M period)

Sl. No.	Measurement	Definition	Measurement Interval	Target	Pen alty
1.	Submission of MIS Reports	The MSI shall submit the MIS reports as defined in Scope of Work	Monthly	All MIS Reports for the previous quarter shall be submitted by the 5th of the next quarter	No Penalty
				Delay beyond The date of submission	Rs.10000 for every day's delay on an incremental basis.
2.	Incident Reporting	Any failure/ incident on any part of the Data	Monthly	100% Incidents to be	No Penalty

		Centre infrastructure or its facilities shall Be communicated Immediately to CRID as an Exceptional report Giving details of Downtime, if any.		reported to CRID within 1 hour with the cause, action, and remedy for the incident	
				Delay beyond An hour	Rs.1000 for every hour's delay on an Incremental basis.
3.	Change Management	Measurement of quality and time lines of Changes to the Data Centre facilities	Monthly	100% of changes should follow formal change control procedures. All changes need to be approved by CRID.	Rs. 50000 for every non compliance.
				All changes should be implemented on time and as per schedule & without any disruption to business.	Rs.10000 for every non compliance .
4.	Scheduled Maintenance	Measures timely maintenance of the ICT Infrastructure equipment installed at the Data Centre. The MSI shall provide a detailed ICT Infrastructure maintenance Plan on the commencement Of the project.	Monthly	100 % of scheduled maintenance should be carried out as per maintenance plan submitted by the MSI. Any scheduled maintenance Needs to be Planned and Intimated to CRID at least 2 Working days in advance.	Rs.10000 for every non compliance
5	Certifications of SDC ISO 27001 ISO 9001 and ISO 20000	MSI has to get the SDC certified within 3 Months of FAT	3 Months	100%Certified for all required Certifications within 3 Months of FAT	Rs.20000 per week of delay.
	Implementation of SDCISO 27001, ISO 9001 and ISO 20000 Recommendations	Implementation of audit recommendation by CRID or its auditor, which have been agreed by MSI & CRID to be implemented.	3 Months	100% on time to be implemented as per time lines agreed upon with CRID.	Rs.10000 for every non-compliance
	Implementation of Audit Recommendations	Repeat Observations (same observations that Has been reported earlier)	Monthly		Rs.50000 for every non-compliance
6.	Maintenance of Spares	The MSI should maintain an inventory of spare components of ICT infrastructure as mutually agreed with	Monthly	100% as per the inventory log committed and maintained by MSI.	Rs.10000f oreveryno n-complianc e

		CRID. For e.g. Switch, Servers etc.			
7.	Manpower	Absence of resource	Monthly	100% on site deployment	Inability of MSI to deploy manpower resource/resources as per Manpower requirement specified in RFP, will attract a penalty of double the amount payable to MSI **for the particular** resource/resources during that period as per manpower payment Terms. **The same shall apply for absence of resource as well**

Security Management SLAs (From date of HOTO Completion)

S. No	Service description	Measurement parameter(Monthly)	Target	Penalty
1.	Data Centre shall be kept free from virus attack	Resolution time for each virus attack	12 – 36 hours, as may be decided depending upon the severity of the attack	Rs.10000 for delay of every 24 hours or it's part
2.	There shall be no Data loss or compromise of any Data hosted at SDC	Number of such incidents	Zero	Rs.50000 per such incident
3.	There shall be no intrusion	Number of such Incidents	Zero	Rs.20000 per such incident

Security Management SLAs (From date of Commissioning till end of O&M period)

S. No	Service description	Measurement parameter (Monthly)	Target	Penalty
1.	Data Centre shall be kept free from virus attack	Resolution time for each virus attack	12 – 36 hours, as may be decided depending upon the severity of the attack	Rs.10,000 for delay of every 24 hours or it's part
2.	Data center shall be kept free from denial of service (DoS) attack which can impact overall data centre services.	Number of DoS attacks	Zero	Rs.5,00,000 per DoS attack

3.	There shall be no Data loss or compromise of any Data hosted at SDC	Number of such incidents	Zero	Rs.5,00,000 per such incident
4.	There shall be no intrusion	Number of such Incidents	Zero	Rs.200000 per such incident
5.	SOC Overall Uptime	99.982%	No Penalty	
		>=99.5%to<99.982%		0.5 % of the yearly PBG value
		>=99.0%to<99.5%		1 % of the yearly PBG value
		<99.0%		0.5% of the yearly PBG for every 3 hours of down time at a stretch or in parts upto total downtime in addition to the penalty mentioned above. This downtime should be calculated over and above the total hours of downtime permissible till 99.00% availability

Note : In case of identification of zero day attack either reported by Cert-in, ISMO or Security OEM's or any other authorized source, will require immediate remediation to mitigate risk.

Non-IT Infrastructure related SLA

Sr	Measurement	Severity	Penalty
1	Power Availability (UPS output)	Critical	Operation and management of all Non IT infrastructure (UPS, Air conditioning systems, Surveillance Systems, copper earth and electrical wiring, LAN cabling , Very Early Smoke Detection System(VESDA) and fire fighting system etc. provided at site are responsibility of the bidder. Clause "Data Centre, Near Line DC and **FAR DR Overall UPTIME SLA" and "Equipment/Application uptime SLAs" penalty clauses respectively** will be invoked in case downtime occurred other than scheduled maintenance of Non IT infrastructure. Bidder has to adhere on SLA resolution time of Severity 1 if failed to resolve snag in Non IT infrastructure additional penalty of Rs.1 Lakh shall be imposed even in case no impact on DC uptime. **Though the Non IT infra as above will be procured by CRID however O&M of this infrastructure will be**
2	PAC System Availability PAC System availability would mean (all PAC's including the standby) temperature and the humidity at the rack level. Temperature to be maintained 20°± 2° at all times Relative humidity to bemaintained50°± 5° at all times	Critical	
3	Surveillance: CCTV Availability would include DVR system availability, availability of CCTV recording –180 days of backup data from the present date	Critical	
4	Complete BMS, system. This parameter applies to any individual component of BMS system, i.e., VESDA, Fire detection, fire suppression, water leak detection,, Rodent repellant etc. For any component downtime, the penalty will be applicable	Critical	
5	Data Centre Infrastructure Management (Measure all the components at the end terminal level)	Critical	

6	Rack Inlet Temperature	Major	**the responsibility of MSI including but not limited to following :** a. Informing CRID on CAMC/AMC renewal time to time b. MSI on behalf of CRID shall coordinate with respective OEM/their Authorized Service Provider to resolve issues/snags in order to keep infrastructure operation as per desired SLAs , as MSI SLA would also be dependent on this infrastructure. c. MSI shall carry out these activities keeping the HSDC team/ CRID in loop
7	Fire Suppression: System Refilling of fire Suppression cylinders in case of discharge during any incident	Critical	

Note: In case of the fire suppression system installed in the Server Farm Area gets discharged / leaked / any accident caused due to the negligence of the MSI; the cost of refilling the cylinders would be borne by the MSI. During the time the fire suppression system installed in the Server Farm Area gets discharged /leaked; the MSI would make provision for hand-held fire suppression system in the required area.

Warranty related SLA

Sl. No	Measurement	Target (Support Response & Resolution time)	Penalty
1	Warranty support for 5 years with all the OEM for respective ICT components after go-live	<= 8 hours	No Penalty
		> 8 Hours to =< 16 hour	0.1% of yearly PBG value
		> 16 hours to =< 24 Hours	0.2% of yearly PBG value
		> 24 hours	0.1% of the yearly PBG for every 1 hours of down time (due to not meeting warranty support) at a stretch or in parts up to total down time
* If there is downtime/denial of services due to delay in warranty support, the respective downtime SLA will also be applicable in addition to above warranty SLA. * The Bidder has to provide resolution/replacement within above timeline for 24*7*365 basis (All Days)			
* The Bidder is required to give Escalation Matrix for Response & Resolution time			

ANNEXURE -A – STATE DATA CENTER EXISTING SYSTEMS AND NETWORK INFRASTRUCTURE

I. HSDC Network Devices

Sr #	Asset Type	Make	Model	Serial Number(s)	Qty	Warranty/ AMC	AMC/ Support End Date
1	Internet Router	H3C	3Com,H3CMSR50-40Router	CN12BDJ05T	1	AMC-Renewal Under Process	14-02-2023
2	Internet Router	H3C	3Com,H3CMSR50-40Router	CN12BDJ00N	1		
3	Core Switch	H3C	H3CS7500E	CN0BD5602D	1		
4	Core Switch	H3C	H3CS7500E	CN0BD56021	1		
5	Application Switch	H3C	3Com,H3CS5500-52C-EI	CN11B9S07D	1		
6	Application Switch	H3C	3Com,H3CS5500-52C-EI	CN11B9S06S	1		
7	Application Switch	H3C	3Com,H3CS5500-52C-EI	CN11B9S07G	1		
8	Application Switch	H3C	3Com,H3CS5500-52C-EI	CN11B9S07Q	1		
9	Application Switch	H3C	3Com,H3CS5500-52C-EI	CN0BB9S05W	1		
10	Firewall	H3C	3Com,SecPathF1000-EFirewall	CN09B7H00D	1	No	EoL
11	Firewall	H3C	3Com,SecPathF1000-EFirewall	CN09B7H00G	1	No	EoL
12	Firewall	H3C	3Com,SecPathF1000-EFirewall	CN09B7H00H	1	No	EoL
13	Firewall	H3C	3Com,SecPathF1000-EFirewall	CN09B7H008	1	No	EoL
14	Firewall, IPS, URL Filtering, Malware	Cisco	CISCO 2130		1	Warranty	

II. HSDC Server & Storage Devices

Sr #	Asset Type	Make	Model	Serial Number (s)	Qty	Warranty/ AMC	AMC/ Support End Date
A	**CHASSISE(1)**	**IBM**	**8677-4TA**	**99AFL47**	**1**	AMC	04-05-2025
1	BladeServerChassis1	IBMHS22	7870G2A	99P9952	1	AMC	04-05-2025
2	Blade Server Chassis1	IBMHS22	7870G2A	99P9472	1	AMC	04-05-2025
3	Blade Server Chassis1	IBMHS22	7870G2A	99P9458	1	AMC	04-05-2025
4	Blade Server Chassis1	IBMHS22	7870G2A	99P9928	1	AMC	04-05-2025
5	Blade Server Chassis1	IBMHS22	7870G2A	99P9937	1	AMC	04-05-2025
6	Blade Server Chassis1	IBMHS22	7870G2A	99R0255	1	AMC	04-05-2025
7	Blade Server Chassis1	IBMHS22	7870G2A	99P9943	1	AMC	04-05-2025
8	Blade Server Chassis1	IBMHS22	7870G2A	99P9845	1	AMC	04-05-2025
9	Blade Server Chassis1	IBMHS22	7870A2A	99R0238	1	AMC	04-05-2025
10	Blade Server Chassis1	IBMHS22	7870G2A	99P9389	1	AMC	04-05-2025
11	Blade Server Chassis1	IBMHS22	7870G2A	99P9478	1	AMC	04-05-2025
12	Blade Server Chassis1	IBMHS22	7870G2A	99P9926	1	AMC	04-05-2025
13	Blade Server Chassis1	IBMHS22	7870G2A	99R0262	1	AMC	04-05-2025
B	CHASSISE(2)	**IBM**	**8677-4TA**	**99AFL54**	**1**	AMC	04-05-2025
14	BladeServerChassis2	IBMHS22	7870A2A	99R0244	1	AMC	04-05-2025
15	Blade Server Chassis2	IBMHS22	7870G2A	99P9846	1	AMC	04-05-2025
16	Blade Server Chassis2	IBMHS22	7870A2A	99R0243	1	AMC	04-05-2025
17	Blade Server Chassis2	IBMHS22	7870G2A	99R0259	1	AMC	04-05-2025
18	Blade Server Chassis2	IBMHS22	7870G2A	99P9371	1	AMC	04-05-2025

19	Blade Server Chassis2	IBMHS22	7870G2A	99N6372	1	AMC	04-05-2025
20	Blade Server Chassis2	IBMHS22	7870A2A	99R0247	1	AMC	04-05-2025
21	RackBasedServers	IBMX3850 M2	72334LA	99E4310	1	AMC	04-05-2025
22	Rack Based Servers	IBMX3850 M2	72334LA	99D7158	1	AMC	04-05-2025
23	Rack Based Servers	IBMX3850 M2	72334LA	99E4314	1	AMC	04-05-2025
24	Rack Based Servers	IBMX3850 M2	72334LA	99E4321	1	AMC	04-05-2025
25	Rack Based Servers	IBMX3850 M2	72334LA	99E4322	1	AMC	04-05-2025
26	Rack Based Servers	IBMX3850 M2	72334LA	99E4318	1	AMC	04-05-2025
27	IBM Storage	IBMDS50 20	181420A	78K0Z1B	1	No	
28	IBM Tape Drive	IBM3310	3576L5B	1317777	1	No	
29	IBM Tape Drive	IBM3310	3576E9U	1376155	1	No	
30	SAN SWITCH	CISCO	MDS-9134	FOX1413G4 PW	1	No	
31	SAN SWITCH	CISCO	MDS-9134	FOX1415G1 BR	1	No	

III. HSDC Software

Sr#	OEM	License Description	Quantity	Support/ Warranty/ AMC	AMC/Support End Date
1	Symantec	Symantec End point Protection (Antivirus) 12.1PERUSER	1250	No	
2	CA	CAARCserveBackupr16.5	20	Yes	31-3-2025
3	CA Service Desk	CA Service Desk		No	
3	Red Hat	Red Hat Enterprise Linux Server, Premium(1-2sockets)	5	Yes	15-3-2028

IV. HP CHASSIS C7000 ENCLOSURES G3

Chassis 1	Make & Model	Product Number	Serial No	Warranty/ Support End Date
	HPE–Blade System c7000 Enclosure G3	681844-B21	SGH642Y4R6	30-Nov -2023
Sr. No	Blade Server SERIALNO	Make	Warranty/AMC	Warranty/Support End Date
1	SGH642Y4S3	HP	AMC	30-Nov -2023
2	SGH642Y4TJ			30-Nov -2023
3	SGH642Y4S7			30-Nov -2023
4	SGH642Y4RR			30-Nov -2023
5	SGH642Y4V5		AMC	30-Nov -2023
6	SGH642Y4TD	HP	AMC	30-Nov -2023
7	SGH642Y4SB			30-Nov -2023
8	SGH642Y4RN			30-Nov -2023
9	SGH642Y4TY			30-Nov -2023
10	SGH642Y4R7			30-Nov -2023
11	SGH642Y4RJ			30-Nov -2023
12	SGH642Y4TL			30-Nov -2023
13	SGH642Y4ST	HP	AMC	30-Nov -2023
14	SGH642Y4V7		AMC	30-Nov -2023
15	SGH414EEK3		Warranty	31-08-2023
16	SGH316SDRJ		No	31-05-2023

V. HP CHASSIS C7000 ENCLOSURESG3

Chassis 2	Make & Model	Product Number	Serial No	
	HPE–BladeSystemc7000 EnclosureG3	681844-B21	SGH642Y4R4 -30-Nov -2023	
Sr. No	Blade Server SERIALNO	Make	Warranty/AMC	Warranty/Support EndDate
17	SGH642Y4SF	HP	AMC	30-Nov -2023
18	SGH642Y4TT			30-Nov -2023
19	SGH642Y4SR			30-Nov -2023
20	SGH642Y4S5			30-Nov -2023
21	SGH642Y4T5			30-Nov -2023
22	SGH642Y4T7			30-Nov -2023
23	SGH642Y4V3			30-Nov -2023
24	SGH642Y4R9			30-Nov -2023
25	SGH746THM1			
26	SGH746THLY			
27	SGH746THM5			
28	SGH746THM3			
29	SGH642Y4T1			30-Nov -2023
30	SGH642Y4SY			30-Nov -2023
31	SGH642Y4RL			30-Nov -2023
32	SGH642Y4V1			30-Nov -2023

VI. HP CHASSIS C7000 ENCLOSURES G3

Chassis 3	Make & Model	Product Number	Serial No	Warranty/ Support End Date
	HPE–Blade Systemc7000	681844-B21	SGH642Y4R5	30-Nov -2023
Sr. No	Blade Server SERIAL NO	Make	Warranty/ AMC	Warranty/Support End Date
33	SGH642Y4RW	HP	AMC	30-Nov -2023
34	SGH642Y4SW			30-Nov -2023
35	SGH642Y4T3			30-Nov -2023
36	SGH642Y4RB			30-Nov -2023
37	SGH642Y4S9			30-Nov -2023
38	SGH642Y4RY			30-Nov -2023
39	SGH642Y4TF			30-Nov -2023
40	SGH642Y4T9			30-Nov -2023
41	SGH642Y4S1			30-Nov -2023
42	SGH642Y4V9			30-Nov -2023
43	SGH642Y4SD			30-Nov -2023
44	SGH642Y4SL			30-Nov -2023

45	SGH642Y4RF			30-Nov -2023
46	SGH642Y4VB			30-Nov -2023
47	SGH642Y4TW			30-Nov -2023
48	SGH642Y4TB			30-Nov -2023

VII. HP CHASSISC7000ENCLOSURES G3

Chassis4	Make & Model	Product Number	Serial No	Warranty/Support End Date
	HPE–BladeSystemc7000 EnclosureG3	681844-B21	SGH642Y4AV	30-Nov -2023
Sr.No	Blade Server SERIALNO	Make	Warranty/AMC	Warranty/Support End Date
49	SGH642Y4B3	HP	AMC	30-Nov -2023
50	SGH642Y4B5			30-Nov -2023
51	SGH642Y4BF			30-Nov -2023
52	SGH642Y4BB			30-Nov -2023
53	SGH642Y4AY			30-Nov -2023
54	SGH642Y4B7			30-Nov -2023
55	SGH746THM1			
56	SGH642Y4SN			30-Nov -2023
57	SGH642Y4AW			30-Nov -2023
58	SGH642Y4BD,			30-Nov -2023
59	SGH642Y4B9			30-Nov -2023
60	SGH642Y4B1			30-Nov -2023
61	SGH642Y4BL			30-Nov -2023
62	SGH642Y4BJ			30-Nov -2023
63	SGH642Y4RT			30-Nov -2023
64	SGH522VN6X			31-05-2023

VIII. SAN SWITCHES FOR NEW STORAGES

Make	Model	Serial Number	Remarks	Make	Warranty/ AMC	AMC/ SupportEnd Date
HPFlexFabric5900	5900AF	CN67FHC004		HP	AMC	30-Nov -2023
HPFlexFabric5900	5900AF	CN67FHC088				30-Nov -2023
HP-Switch-48Port	SN6000B	CZC634F307				30-Nov -2023
HP-Switch-48Port	SN6000B	CZC634F30B				30-Nov -2023
CISCOFabricSwitch -48Ports	MDS9148S	JPG2010001R	For Hitachi Storage	Cisco		
CISCOFabricSwitch -48Ports	MDS9148S	JPG2010005Q	For Hitachi Storage			
HPFlexFabric5900	5900AF	CN67FHC083		HP	AMC	30-Nov -2023
HPFlexFabric5900	5900AF	CN67FHC06G				30-Nov -2023
HP-Switch-48Port	SN3000B	USB639200G				30-Nov -2023
HP-Switch-48Port	SN3000B	USB63720D0				30-Nov -2023

IX. HP SERVERS

Model no.	Serial Number	Make	Warranty/AMC	Warranty/Support End Date
HPPROLIANTDL160	SGH628Y38H	HP	AMC	12-Aug-2023
HPPROLIANTDL160	SGH628Y38F			12-Aug-2023
HPPROLIANTDL160	SGH628Y38A			12-Aug-2023

X. STORAGES

Make	Model	Serial Number	Warranty/AMC	Warranty/ Support End Date
Hitachi	VSPG1500	57176	AMC	30-4-2024
Netapp	FAS2552	9415160000 (66)(67)	No	
Hitachi	VSP G350		No	AMC Under Process
HP EVA Storage	HSV360	SGA223007P	No	EOL
HP (Storage)3 PAR With Management HPE320G8 SGH5460LYC to 31.10.2022Server with3PAR Storage	7400c &HPE320G8	4C15478779, SGH5460LYC	AMC	31-Oct-22

XI. HP Chassis & Servers

Sr. No.	Model	Serial Number	Support/Warranty/AMC	AMC/Warranty End Date
CHASSIS	HPE BLc7000 CTO 3 IN LCD Plat Enclosure	SGH414EFPB	Warranty	31-08-2023
1	PROLIANT BL460 G8	SGH414EEK1	Warranty	31-08-2023
2	PROLIANT BL460 G8	SGH316SDRF	AMC	31-05-2023
3	PROLIANT BL460 G9	SGH540W78F	AMC	31-05-2023
4	PROLIANT BL460 G9	SGH540W78J	AMC	31-05-2023
5	PROLIANT BL460 G7	SGH2174XP2	AMC	31-05-2023
6	PROLIANT BL460 G7	SGH2174XNS	AMC	31-05-2023
7	PROLIANT BL460 G9	SGH522VN70	AMC	31-05-2023
8	PROLIANT BL460 G9	SGH522VN6V	AMC	31-05-2023
9	HPE BL460c Gen9	SGH524W8LN	AMC	31-05-2023
10	PROLIANT BL460 G9	SGH522VN6P	AMC	31-05-2023
11	PROLIANT BL460 G9	SGH524W8LV	AMC	31-05-2023
12	PROLIANT BL460 C G8	SGH414EEK9	Warranty	31-08-2023
13	PROLIANT BL460 G9	SGH522VN6S	AMC	31-05-2023
14	PROLIANT BL460 G7	SGH2174XNP	AMC	31-05-2023

Sr. Number	Model	Serial Number	Support/ Warranty/AMC	AMC/ Warranty End Date
CHASSIS	HP BLc7000 CTO 3 IN LCD ROHS Enclosure	SGH2164798	AMC	31-05-2023
	Ethernet Blade Switch MY321561VF Gigabit 20 port layer2	MY321561VF, MY321561UZ	AMC	**31-05-2023**
	SAN Switch HP Brocade"" 4GB PS20 port for 7/16Blade	CN8021B01E	AMC	**31-05-2023**
1	HP BL460c Gen8 10/20Gb FLB CTO	SGH414EEJY	Warranty	**31-08-2023**
2	HP BL460c G7 CTO	SGH2174XPO	AMC	**31-05-2023**
3	HP BL460c G7 CTO	SGH2174XP4	AMC	**31-05-2023**

4	HPE BL460c Gen9 10Gb/20Gb FLB CTO		AMC	**31-05-2023**
5	HP BL460c Gen8 10/20Gb FLB CTO	SGH414EEK5	Warranty	**31-08-2023**
6	HP BL460c G7 CTO	SGH2174XNX	AMC	**31-05-2023**
7	HP BL460c G7 CTO	SGH2174XP6	AMC	31-05-2023
8	HP BL460c G7 CTO	SGH2174XNV	AMC	31-05-2023
9	HP BL460c G8 CTO	SGH316SDRH	AMC	31-05-2023
10	HPE BL460c Gen9 10Gb/20Gb FLB CTO		AMC	31-05-2023
11	HP BL460c Gen8 10/20Gb FLB CTO	SGH414EEK7	Warranty	31-08-2023
12	HP BL460c Gen8 10/20Gb FLB CTO	SGH316SDRE	AMC	31-05-2023
13	HPE ProLiant XL190r Gen9 CTO		AMC	31-05-2023

Asset Type	**Make**	**Model**	**Warranty/AMC**	**AMC End Date**
Network Switch	Cisco	3560	No	EOL

ANNEXURE B - DETAILS OF THESE SUB-SYSTEMS UNDER BUILDING MANAGEMENT SYSTEM

Sr	Item Description in Short	As per Order		Make (Old BMS Infra)	Model No.
			Qty		
I	**Analogue Addressable Intelligent Fire Detection System**	**Current Status**			
1	Microprocessor based Analogue Addressable One loop 80 Character display Intelligent fire detection panel	Working	1	ASENWARE	AW-AFP2188
2	Intelligent Analogue Addressable Multi-criteria type Photo-thermal Detector. (Smoke Detectors)	Need check/ cleaning /service	33	ASENWARE	JTY-GD-F311
3	Intelligent Analogue Addressable fixed cum ROR Thermal Detector. (Heat Detectors)	Under replacement	3	ASENWARE	JTY-OD-F622
4	Addressable Manual Call Point with Mini Monitor Module.	Not Working	4	Siemens	
5	Electronic Sounders 85 Db	Under replacement	4	ASENWARE	
6	Fault Isolator Module	Under replacement	2	ASENWARE	
7	Response Indicators	Under replacement	**3**	Siemens	
II	**NOVEC 1320 FIRE SUPPRESSION SYSTEM (For Server Room and UPS Room)** Note: - The existing non IT infrastructure is under revamping/replacement by the CRID.				
1	120 Ltrs. Seamless cylinders (120 Ltrs is a Capacity of One Cylinder)	Working	4	Siemens	Model No: Gas - NOVEC 1230/ FM-200
2	NOVEC 1230 Gas **(85kg X 4)**	Working	340 kg	Siemens	Model No: Gas - NOVEC 1230/ FM-200
3	Master Cylinder Adapter Kit used to actuate the Slave Cylinder.	Working	1	Siemens	Model No: Gas - NOVEC 1230/ FM-200
4	**Electrical Actuator Head**	Working	1	Siemens	Model No: Gas - NOVEC 1230/ FM-200
5	**Pneumatic Actuator head**	Working	4	Siemens	Model No: Gas - NOVEC 1230/ FM-200
6	**Flexibe discharge Hoses**	Working	5	Siemens	Model No: Gas - NOVEC 1230/ FM-200
7	**Flexible Actuation Hose**	Working	4	Siemens	Model No: Gas - NOVEC 1230/ FM-200
8	M.S. Seamless pipes as per ASTM A 106 Gr. B, Schedule 40 with necessary fittings.	Working	1	Siemens	
9	NOVEC 1230 nozzles	Working	8	Siemens	
10	NOVEC 1230 system manifold sch 80 ASTM 106 gr B per cylinder	Working	1	Siemens	
11	Discharge Sign Board	Working	1	Siemens	
12	**Manifold Check Valve**	Working	4	Siemens	
13	Manual Abort cum gas release station with addressable monitor modules.	Working	2	Siemens	
14	Addressable Control / Relay Module for integration with Fire Detection Panel.	Working	2	Siemens	
III	**Access Control System**				
1	Microprocessor based 4 Readers Door Intelligent controller	Working	3	SPECTRA	ACT-1000
2	HID Prox point Proximity reader	replacement under progress	9	HID	

Sr	Item Description in Short	As per Order		Make (Old BMS Infra)	Model No.
3	Biomteric Reader with inbuilt proximity reader.	replacement under progress	3	SPECTRA	FP-1000
4	Time and Access Management Software (Licensed Version)	replacement under progress	1	SPECTRA	NETX CONTROL
5	Single Leaf Electromagnetic Lock with inbuilt sensor - 600lbs	replacement under progress	8	CAPTURE/ AEGIS	
6	Double leaf Electro magnectic Lock with in-built sensor	replacement under progress	5	CAPTURE/ AEGIS	
7	HID Proximity card with printing	replacement under progress	100	HID	
8	Panic Bar (For Emergency Door)	replacement under progress	2	Brand Not Mentioned	
9	Intelligent Addressable Control Modules (for de activation of access control doors in case of fire)	replacement under progress	3	ASENWARE	
IV	**Rodent Repellent System**				
1	12 channel Rodent Repellant Controller	Working	3	Maser	
2	Sattelites / transducers	replacement under progress	36	Maser	These are the Field equipment installed below false flooring and above false ceiling
V	**Water Leak Detection System**				
1	12 Zone Water leak detection panel.	Working	1	Sontay	WD-AMX2
2	Relay Module for each zone inbuilt in water detection panel	replacement under progress	12	Sontay	WD-AMX2 (These are the Field equipment installed above false ceiling)
VI	**CCtV Surveillance System**				
1	1/3" Color fixed dome camera	Working	40 +3(pending)	Pelco (new IP Based) camera with switches	EUROPLEX TECHNOLOGIES(Old)
2	16 Channel Windows XP embedded Digital Video Recorder	replacement under progress	1	Siemens	GCD550-PV;
3	32' LCD Monitor	replacement under progress	1	Samsung	
VII	**VESDA System**				
1	VESDA Laser Panel with Hooter	Working	1	Xtralis	VLF254
2	Aspiration Tubes for VESDA system consisting of 1" PVC Pipes	replacement under progress	1		Suction tubes (with necessary nozzels)
VIII	**PA System**				
1	Plena main BGM/Paging system controller with inbuilt 120W mixer amplifier with volume control MP3 DVD/CD player. The unit should play normal audio and video DVD/CDs as well as long-play MPEG2 ,MP3 encoded CDs with bit rates from 32kbps to 32-kbps ,	Working	1	Bosch	mono/s
2	Plena Microphone,	replacement	1	Bosch	model no.

Sr	Item Description in Short	As per Order		Make (Old BMS Infra)	Model No.
		under progress			LBB1950/00
3	6W compact ceiling speaker,	replacement under progress	25	Bosch	model no. LBD 8353/10
IX	**Building Management System**				
1	Necessary Software Packages	replacement under progress	1	SHIVAKI	
2	Microporcessor based Direct Digital Controller	replacement under progress	1	SHIVAKI	951-V & 951-S 8CH DATA LOGGER
X	**Field Equipments**				
1	Room Temperature Sensor cum Humidity Sensor	replacement under progress	3	SHIVAKI	
2	Outside Temperature and RH Sensor		1	SHIVAKI	

ANNEXURE C - APPLICATIONS HOSTED AT CURRENT SDC

Sr. No.	Domain	Sr. No.	Domain
1	advocategeneralhry.gov.in	116	minesharyana.gov.in
2	agriharyana.gov.in	117	madhuban.medleaprhry.gov.in
3	intra.agriharyana.gov.in	118	pandsharyana.gov.in
4	haims.agriharyana.gov.in	119	mmiyharyana.gov.in
5	cadaharyana.nic.in	120	pcpndtharyana.gov.in
6	cicharyana.gov.in	121	prharyana.gov.in
7	courts.medleaprhry.gov.in	122	prosecutionhry.gov.in
8	cmharyanacell.nic.in	123	secharyana.gov.in
9	dpmuhry.gov.in	124	scertharyana.gov.in
10	android.dpmuhry.gov.in	125	tcpharyana.gov.in
11	demo.dpmuhry.gov.in	126	tcpharyana.gov.in/sso
12	dstharyana.gov.in	127	eapplication.tcpharyana.gov.in
13	edisha.gov.in	128	dfs.tcpharyana.gov.in
14	citizen.edisha.gov.in	129	edraw.tcpharyana.gov.in
15	haryanareliefcamps.edisha.gov.in	130	mis.tcpharyana.gov.in
16	saral.edisha.gov.in	131	ofa.tcpharyana.gov.in
17	umang.edisha.gov.in	132	eauction.tcpharyana.gov.in
18	ws.edisha.gov.in	133	roauction.tcpharyana.gov.in
19	esachivalaya.edisha.gov.in	134	clu.ulbharyana.gov.in
20	saralharyana.nic.in	135	biswas.ulbharyana.gov.in
21	status.saralharyana.nic.in	136	online.ulbharyana.gov.in
22	aas.saralharyana.nic.in	137	saralservices.ulbharyana.gov.in
23	dashboard.saralharyana.nic.in	138	saralserstg.ulbharyana.gov.in
24	eticketing.saralharyana.nic.in	139	vmsharyana.gov.in
25	etoken.saralharyana.nic.in	140	waterstg.ulbharyana.gov.in
26	etokenhry.nic.in	141	staging.ulbharyana.gov.in
27	kms.saralharyana.nic.in	142	covidsample.haryana.gov.in
28	login.saralharyana.nic.in	143	cag.aghry.gov.in

29	ws1.edisha.gov.in	144	atmanirbhar.haryana.gov.in
30	citizenstg.edisha.gov.in	145	bankslot.haryana.gov.in
31	saralstg.edisha.gov.in	146	banking.haryana.gov.in
32	staging.edisha.gov.in	147	mistry.itiharyana.gov.in
33	umangstg.edisha.gov.in	148	hsiidcgis.org.in
34	wsstg.edisha.gov.in	149	hvpn.org.in
35	unorgworker.edisha.gov.in	150	cashless.haryana.gov.in
36	cashlessharyana.nic.in	151	esign.hartron.org.in
37	helpdesk.ifmsharyana.nic.in	152	ekharid.in
38	ifmsharyana.nic.in	153	mandippm.com
39	hrmshry.nic.in	154	kmsstg.saralharyana.nic.in
40	intrahry.gov.in	155	jansahayak.haryana.gov.in
41	bamsharyana.nic.in	156	covidcontrolroom.harayna.gov.in
42	epensionhry.nic.in	157	healthy.haryana.gov.in
43	esalaryhry.nic.in	158	rozgar.hrex.gov.in
44	otishry.nic.in	159	mis.haryanaforest.gov.in
45	eGrashry.nic.in	160	jamabandi.nic.in
46	egazetteharyana.gov.in	161	https://cag.aghry.gov.in/ords/f?p=100:1:119487931714:NEW::::
47	epossr.hry.gov.in	162	odms.aghry.gov.in/grievance
48	fdaharyana.gov.in	163	setchartron.in
49	forestharyana.gov.in	164	durgashakti.haryanapolice.gov.in
50	forestgis.forestharyana.gov.in	165	http://10.88.238.39:7001/HEX/appmanager/HexPortal/HaryanaExcise
51	harpathharyana.gov.in	166	haryanasacs.in
52	haryanapoliceonline.gov.in	167	ahdh.pashudhanharyana.gov.in
53	haryanapolice.gov.in	168	meragaonmeragaurav.gov.in
54	harsamay.gov.in	169	riprcdhry.gov.in
55	harspagy.gov.in	170	ims.haryana.gov.in
56	hartrans.gov.in	171	onetimeregn.haryana.gov.in
57	afc.hrtransport.gov.in	172	samiksha.samagra.io
58	hartronskill.org.in	173	haryanagoodgovernanceawards.haryana.gov.in
59	haryanabpas.gov.in	174	cashless.haryanahealth.gov.in
60	haryanacmoffice.gov.in	175	vc.jamabandi.nic.in
61	bk.haryanafood.gov.in	176	nhmharyana.gov.in
62	epos.haryanafood.gov.in	177	nrhmharyana.gov.in
63	lm.haryanafood.gov.in	178	midrs.nhmharyana.gov.in
64	kharif.haryanafood.gov.in	179	hr.nhmharyana.gov.in
65	haryanaismo.gov.in	180	sihfw.nhmharyana.gov.in
66	haryanapwd.gov.in	181	main.nhmharyana.gov.in
67	mail.haryanapoliceonline.gov.in	182	asha.nhmharyana.gov.in
68	haryana-rtsc.gov.in	183	ss.nhmharyana.gov.in
69	haryanatax.gov.in	184	app.nhmharyana.gov.in
70	mailgw.haryanatax.gov.in	185	pension.socialjusticehry.gov.in
71	mail1.haryanatax.gov.in	186	crdashboard.haryana.gov.in
72	mail2.haryanatax.gov.in	187	ndc.ulbharyana.gov.in

73	vanijya.haryanatax.gov.in	188	ulbshops.ulbharyana.gov.in
74	hbcc.nic.in	189	dmer.haryana.gov.in
75	https://hbcc.nic.in/cmnms	190	shopsmis.ulbharyana.gov.in
76	hbckn.org.in	191	haryanafcd.gov.in
77	hmscl.org.in	192	parivarutthan.haryana.gov.in
78	demo.hmscl.org.in	193	adv.ulbharyana.gov.in
79	hrtransport.gov.in	194	odms.aghry.gov.in
80	api.hrtransport.gov.in	195	hospitalityharyana.gov.in
81	buspass.hrtransport.gov.in	196	odms.aghry.gov.in/inspection
82	dts.hrtransport.gov.in	197	odms.aghry.gov.in/grant/
83	epay.hrtransport.gov.in	198	ithrms.haryana.gov.in
84	etickets.hrtransport.gov.in	199	happeningharyana.nic.in
85	mis.hrtransport.gov.in	200	C-form.haryanatax.gov.in
86	hryedumis.gov.in	201	award.socialjusticehry.gov.in
87	mail1.hryedumis.gov.in	202	epds.haryanafood.gov.in
88	support.hryedumis.gov.in	203	scpd.haryana.gov.in
89	training.hryedumis.gov.in	204	digisectt.haryana.gov.in
90	tremp.hryedumis.gov.in	205	hartrontraining.in
91	trreports.hryedumis.gov.in	206	farm.hvpn.org.in
92	trsch.hryedumis.gov.in	207	training.cas.hryedumis.gov.in
93	trstu.hryedumis.gov.in	208	misurvey.cadaharyana.nic.in
94	stu.hryedumis.gov.in	209	hfa.haryana.gov.in
95	sch.hryedumis.gov.in	210	ors.hartrans.gov.in
96	reports.hryedumis.gov.in	211	cis.tcpharyana.gov.in
97	mtms.hryedumis.gov.in	212	ccma.tcpharyana.gov.in
98	samiksha.schooleducationharyana.gov.in	213	highvaluetenders.dsndharyana.gov.in
99	emp.hryedumis.gov.in	214	erpcrid.edisha.gov.in
100	cas.hryedumis.gov.in	215	plasticban.ulbharyana.gov.in
101	hryrevenuecourts.gov.in	216	poorpreg.haryana.gov.in
102	hscsk.org.in	217	yogaayog.haryana.gov.in
103	hsfdc.org.in	218	ebooking.hrtransport.gov.in
104	hshrc.gov.in	219	Fams.hvpn.org.in
105	hsiidc.org.in	220	rps.hpsc.gov.in
106	hssc.gov.in	221	subdivision.ulbharyana.gov.in
107	lawandlegislativehry.gov.in	222	rp.hpsc.gov.in
108	localaudithry.gov.in	223	schemes.haryanascbc.gov.in
109	fsl.medleaprhry.gov.in	224	Jamabandi.nic.in
110	medleaprhry.gov.in	225	wgrs.ulbharyana.gov.in
111	android.medleaprhry.gov.in	226	hshrc.in
112	covid19.medleaprhry.gov.in	227	gis.ulbharyana.gov.in
113	demo.medleaprhry.gov.in	228	rohsamb.tcpharyana.gov.in
114	demo1.medleaprhry.gov.in	229	rohsiidc.tcpharyana.gov.in
115	demo2.medleaprhry.gov.in	230	rohsvp.tcpharyana.gov.in
		231	rotcp.tcpharyana.gov.in

ANNEXURE E - DG SET INFRASTRUCTURE

Cummins Generators details are mentioned below,

- Make- CUMMINS make 3 numbers.
- Model - NTA-855-G2-I
- Rating - 320 * 3 KVA
- Sr. No- 25358372, 25358373 ,25358369
- Commissioning date- 18- March - 2011
- Current status- Running and Under AMC of authorized Dealer of CUMMINS

SECTION 5

MINIMUM TECHNICAL SPECIFICATIONS

5.1 MINIMUM TECHNICAL SPECIFICATIONS OF THE PRODUCTS:

Please note that the specifications given below are the minimum suggested technical specifications. Bidders are free to offer any specification over and above the minimum indicated. The bidders are further required to submit the technical brochures along with the technical bid besides filling the technical Performa at annexure-4. The offered product should be available on public domain.

COMMON SPECIFICATIONS FOR ALL OEMS:

CSP.REQ.001	**Warranty & Post warranty Support**	5 years On-site comprehensive warranty support after Go Live acceptance from day 1. 2 years post warranty support as per Haryana States' CAMC/AMC policy must be offered to CRID after completion of warranty period. The rates to be offered for every BOQ (solution including both software & hardware and individual as applicable) as per format 2 point 5 which is to be uploaded in the Financial Bid document. The discovery of these shall not be considered for financial evaluation i.e. declaring L1. However, the Purchaser reserves the right to compare the rates offered with other bidders for the same Make/Model/Solution and can negotiate based on the same. All required licenses should be PERPETUAL in nature and should have NO dependency on underlying hardware with 5 years On-site comprehensive Annual Technical Support from respective OEM. In case, any item doesn't come with PERPETUAL licenses, the MSI shall provision subscription licenses for scope of work as per this RFP. Note:- The said clause may be applicable to every related clause mentioned in this RFP corrigendum.
CSP.REQ.002	**Training**	The respective OEM must provide comprehensive training to SDC Officials on the Solution for an appropriate period or 15 days at Chandigarh split in following sessions. Sessions can be as Under; 1. Session 1: At the time of installation and commissioning for implementing best practices with the experience of OEM keeping in view over all architecture of project. CRID shall be part of this process. 2. Session 2: Administration, Management and Performance Tuning. The session must be instructor lead and may be conducted physical or online as on need basis. This may be repeated in first year after Go-Live as per the requirement of CRID.
CSP.REQ.003	**Documentation**	Standard Operating Procedures and User Guide should be developed for ensuring the proper operations and controls
CSP.REQ.004	**IPv6 readiness**	should support IPv6 and solution should be IPv6 compliant to ensure all features of IPv6

5.2 SERVER

S. No.	Parameter	Minimum Specifications
SER.REQ.001	Motherboard	Minimum number of sockets available & minimum sockets populated from Day 1: 2
SER.REQ.002	Form Factor	2 U RACK mounted
SER.REQ.003	Total Core per server	Latest Generation Processors of OEMs (AMD/Intel) 128Cores (min. 2 proc with 64core per processor)
SER.REQ.004	Configured CPU	Processor Base Frequency (GHz) 2.0 GHz Or higher and should support memory speed@ 4800 MT/s or higher
SER.REQ.005	Memory slots	24 or higher DIMM slots
SER.REQ.006	Memory configured	Type DDR 5 SDRAM with ECC 4400 Mhz or higher supported PCIe Gen 5 RAM Size 1 TB or Higher
SER.REQ.007	Capacity Drive	1. 2x 800 NVMe or higher (in RAID 1)
SER.REQ.008	RAID/HBA Controller	RAID controllers with minimum 12Gbps or higher speed with 4 GB or higher Cache Supporting RAID 0 & 1
SER.REQ.009	I/O slots Bus Slot	At least 3 PCIe Gen5 Slots upgradeable to 4
SER.REQ.0010	FC HBA	Dual Port HBA supporting 32Gbps and should also support 16Gbps backward compatibility
SER.REQ.0011	Ethernet ports	2 number 10/25G or Higher with 25 G QSFP28 from day 1
SER.REQ.0012	Certification and Compliance & Industry standard compliance	1. OS: Microsoft Windows Server, Hyper-V, VMWare, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES) /Cent OS 2. RoHS compliant 3. Appropriate KVM solution to be bundled in the solution for supporting the total servers supplied under this RFP with provision of adding 25% extra quantity of servers. The solution to include peripherals like KBD, Mouse VDU and necessary numbers of cables/connectors etc. required for functionality
SER.REQ.0013	Power & temperature	Platinum rated redundant Hot plug Power Supplies Should support hot plug redundant power supplies with minimum 91% efficiency

SER.REQ.0014	Configuration & Management	**1. Management Features-1**
		• Remoter power on/ Shutdown of server
		• Remote Management of Server over LAN & WAN with SSL encryption through gigabit management port
		• Should have virtual Media support with all required licenses.
		  ○ Remote KVM
		  ○ Encrypted virtual media
		  ○ Server Health Logging
		  ○ Out of Band Management

S. No.	Parameter	Minimum Specifications
		• Detection of the Service Pack /firmware for Server and notifications for any hotfixes that may be available for the particular Configuration. OEM's customer advisories based on their relevance to server configuration. **Mgmt. feature 2:** • Management of multiple Servers from single console with single source of truth for multiple sites. • Automated infrastructure management for patch upgrades version upgrades etc. • Simplified management with analytics driven actionable intelligence. • admin flexibility to provide metadata tags to the resources varing between server and accounts based on user requirement or each System to enable users to filter and sort systems based on user-assigned attributes • Hardware Profile based deployment to multiple Servers simultaneously • Policy template for deployment of single policy to multiple Servers simultaneously • Platform inventory and health status • Server utilization statistics collection (including firmware updates and diagnostic tools) • Should provide an alert in case the system is not part of OEM hardware compatibility test • Should have customizable dashboard to show overall faults/health/inventory for all managed infrastructure the solution should provide option to create unique dashboards for individual users. The user should be flexibility to select name for dashboards and widgets (viz. health utilization etc) • Self-service portal deployment for automated provisioning • Real-time out-of-band hardware performance monitoring & alerting 3. Server should have dedicated 1Gbps remote management port. Server should support agentless management using the out-of-band remote management port
SER.REQ.0015	Server Node Security / System security	**1. Security feature 1:** • Secure Boot (Firmware and Bios Level Security) Immutable Hardware root of trust or Dual Root of Trust • Server should provide policy-based security • Server should provide server intrusion detection • OEM to offer Server firmware free from any malicious code Advanced Encryption Standard (AES) or and Triple Data Encryption Standard (3DES) **2. Security feature 2** • Provision for Cryptographic firmware updates • Capability to stop execution of Application/Hypervisor/ Operating System on predefined security breach • Secure /Automatic BIOS recovery • Network Card secure firmware boot System should provide automatic firmware upgrade and feature of rollback

S. No.	Parameter	Minimum Specifications
		3. Security feature-3 Should have dashboard for firmware baselines while performing minimum required firmware checks and highlighting out-of-compliance devices for updates with the selected firmware baseline
SER.REQ.0016	IPv4/6 Ready	The Hardware should be IPv4 & IPv6 compliant & ready from day one
SER.REQ.0017	Warranty & Post warranty Support	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support
SER.REQ.0018	Fans	Redundant hot-plug system fans
SER.REQ.0019	Operating Systems and Virtualization Software Support	1. Virtualization: VM ware, HyperV, OpenStack, Kubernetes 2. OS: Microsoft Windows Server, Hyper-V, VMWare, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES)/ Cent OS
SER.REQ.0020	SPEC int_rate_base 2017 for the product (must be available on SPEC dot ORG before evaluation)	1000 Or higher
SER.REQ.0021	SPEC fp_rate_2017 for the product (must be available on SPEC dot ORG before evaluation)	1000 Or higher

5.3 SAN STORAGE

S.No.	Parameter	Minimum Specifications
SAN.REQ.001	Storage	• Storage should be True Enterprise Class Storage and should have the capability to scale up and scale out. Storage system must guarantee 99.9999% data availability architecture and All flash NVMe array only
SAN.REQ.002	Storage Size/Scalability	• a. True Enterprise Storage should be supplied with 2 PB of usable space in RAID 6 (hot spare and scalable upto usable minimum 4 PB having same size and category of NVME disk as supplied with accordance of clause SAN.REQ.004 (excluding all overhead configuration like RAID configuration formatting and hot spare disk, de-dup). • b. True Enterprise Storage should be configured with at least 2TB of DRAM Cache expandable up to 6 TB of Cache, which should be available across all controller , should be dynamically used for Read and Write operations to meet the over all performance • c. The usable storage capacity as above must be available after enabling all features as defined under minimum technical specifications."
SAN.REQ.003	Cache Protection	• The storage should have protection of cache data during a power down either scheduled or unexpected power outage by battery backup for at least 24 hours OR by de staging the data in cache to non-volatile disk.
SAN.REQ.004	Flash Drive/ speed	• The storage array must be supplied with dual ported NVMe SSD MLC/TLC drives with PCI Gen3 NVMe or higher from day one. Supplied each drive capacity should have capacity/size such that disk rebuild time in RAID 6 must not more than 15 hours..
SAN.REQ.005	Controllers	• Offered Storage shall be supplied with at-least 4 active-active storage controllers and scalable up to 8 controllers with true active-active multi-controller/node scale-up and scale-out architecture. However, in case of failure of any controller(s), the remaining working controller(s) should be able to cater to entire load of the solution and should not lead to decrease in Read and write performance with no adverse effect on the overall performance of the storage.
SAN.REQ.006	Ports (per controller/per controller pair)	• Front end port - FC port - 8 x 32 Gbps speed expandable 16 x 16/32. All FC port should be populated from day one.
SAN.REQ.007	CPU	• Offered storage shall have minimum dual CPUs per controllers
SAN.REQ.008	Operating System and Virtualization Support	• The storage solution should support all latest operating system and cluster environments. The storage solution should support virtual infrastructure (like VMware / Hyper-V/ KVM etc). Should have capabilities for booting VMs from the SAN. Should be supplied with virtualization aware APIs for provisioning and managing the storage array from the virtual infrastructure.
SAN.REQ.009	Protocol Support	• Storage should support protocol – FC,NVMEoF,. All license must be supplied for the maximum capacity offered by the storage system.

S.No.	Parameter	Minimum Specifications
SAN.REQ.0010	RAID support	• Should support various hardware industry standard RAID levels 6
SAN.REQ.0011	Online RAID Group expansion	• Must support online expansion of RAID Group. Must be able to add additional disks on the fly to expand the RAID group capacity.
SAN.REQ.0012	Multi-pathing and SAN Security	• The multi-pathing software should provide multi-pathing from all leading OEM's. The Storage should provide provision LUN Masking and SAN Security
SAN.REQ.0013	No Single Point of Failure	• The proposed solution should be with No Single Point of Failure (NSPOF). All the components should be redundant and hot swappable including power supply, fans, disk drive, controllers etc.
SAN.REQ.0014	Performance	• Minimum Aggregate front-end IOPS of proposed array (8K I/O Block size) should be 20,00,000 using 70:30 Read/write ratio and 8K block size and with deduplication and compression enabled from day 1 and storage solution should support sub latency up to 200µs.
SAN.REQ.0015	Management software	• All the necessary software to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots etc. Single Command and GUI or Integrated Web Console for entire storage system for configuration, managing and administration of storage and associated functionalities including deployment, automation, provisioning, and protection and monitoring management . • Should provide the functionality of proactive monitoring of Disk drive and Storage system for all possible disk failures and SSD wear out details • Should be able to create instantaneous or Point in Time Snapshot copies of volumes which can be either a full clone or incremental snapshot of the volumes. • Should provide monitoring of IOPs, read/write, cache, throughput etc. in real time or better OEM monitoring functions.
SAN.REQ.0016	Remote Replication	• The storage array should support hardware-based data replication at the array controller level across all models • The storage should support both synchronous and asynchronous data replication to remote site across minimum 2 storage arrays without using third party software with zero data loss. • The storage should support incremental replication after resumption from Link Failure situation or during failback operations. • Any additional Software/hardware required to achieve above mentioned replication features must be supplied along with the storage • Minimum 2 dedicated Replication IP Ports required per controller.
SAN.REQ.0017	RANSOMEWARE Protection	Offered Storage must be supplied with safe & secure storage with Ransomware protection or any one of the following data protection mechanism: • Inbuilt or through third party solution or immutable protection or application consistent snapshot or active vault & physical air gap tool or data isolation & air gaps or

S.No.	Parameter	Minimum Specifications
		through WORM/versioning snapshots to protect data from any kind of attack and provide support (update and upgrades) from day 1, till the scope of the project + 2 years. The usable storage as indicated in SAN.REQ.002 must not be utilized for enabling these features.
SAN.REQ.0018	Supported Software and licences	• Thin Provisioning, Inline-Compression, Inline deduplication, Snapshot, restore snapshot, Cloning and application & VM aware backup. Asynchronous and synchronous remote replication/mirroring for Disaster Recovery, encryption, Quality of Service Software for optimizing IOPS and /or bandwidth
SAN.REQ.0019	Warranty &Post warranty Support	• 5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.4 SAN SWITCH

S.No.	Parameter	Minimum Specifications
SANS.REQ.001	Architecture	1. The SAN switch shall support non- blocking architecture with minimum 48 active ports full duplex in single domain with no oversubscription and in a single physical Switch. 2. Auto-sensing 8, 16, and 32 Gbit/sec capabilities. 3. All 48 autosensing Fibre Channel ports should be capable of speeds of 8,16 and 32 Gbps, with 32 Gbps of dedicated bandwidth for each port. 4. The switch should protect SAN and End devices from corrupted frames (inbuilt CRC and Slow Drain detection and Mitigation)
SANS.REQ.002	Rack Mount	The switch shall be rack mountable and be supplied with proper rack mount kit to mount.
SANS.REQ.003	High Availability	SAN Switch shall be deployed in high availability (1+1) configuration
SANS.REQ.004	Management	Support for web-based management and shall also support CLI.
SANS.REQ.005	ISL Trunking	The switch shall be able to support frame based ISL trunking with consecutive ports (using 16/32 Gbit/sec SFPs). Switch should support ISL Trunking license from day one.
SANS.REQ.006	Performance	The SAN Switch must provide aggregate bandwidth of 1.5 Tbps half duplex and 3 Tbps full duplex.
SANS.REQ.007	Fabric Services	1. Monitoring and Alerting Policy 2. Adaptive Networking (Ingress Rate Limiting, Traffic Isolation, QoS) 3. Fabric Performance Monitoring 4. Dynamic Path Selection (DPS) 5. BB Credit Recovery 6. FDMI 7. Frame Redirection 8. NPIV 9. Registered State Change Notification (RSCN); Reliable Commit Service (RCS)

S.No.	Parameter	Minimum Specifications
SANS.REQ.008	SFP	The switch shall be provided with SFPs for all active ports.
SANS.REQ.009	Zoning & Security feature	1. Support for hardware and software zoning and ACL 2. Policy based security and centralized fabric management. 3. Support for secure access. 4. Support for FC based authentication. 5. Support for RADIUS/TACACS, SSH, SNMP 6. Support for port binding. 7. Trunking capability with required software licenses
SANS.REQ.0010	Power Supply	Switch should have dual power supply, Switch should have no single point of failure and all components should be hot swappable.
SANS.REQ.0011	Warranty & Post warranty Support	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.5 OBJECT STORAGE

S.No.	Parameter	Minimum Specifications
OBJS.REQ.001	Capacity	Storage should be supplied with usable 250TB from day 1 using erasure coding with at least 3 disk protection in each disk group or 1 complete node failure(excluding all overhead configuration like configuration formatting and hot spare disk, de-dup) or equivalent in RAID6. Each disk size should not be more than 18TB.The usable storage capacity as above must be available after enabling all features as defined under minimum technical specifications.
OBJS.REQ.002	Nodes and architecture	Storage should be in symmetric / asymmetric and distributed clustered architecture. Must be configured with at least 4 nodes upgradeable to 6 nodes. Each storage node should be supplied with 4 no's of 10 Gbps/ 25 Gbps or higher SFP+ ports with transceivers.
OBJS.REQ.003	Cache	Each storage node should be configured with 64 GB or more DRAM based cache for read and write operations. In addition, storage should have SSD based cache, If SSD cache not available then storage should supplied with equivalent DRAM based cache.
OBJS.REQ.004	Expandability	The object storage cluster shall be scalable to minimum 2 PB in a single cluster by adding drives and nodes. Proposed Object storage must provide automatic balancing of the stored capacity across all nodes in a cluster, ensuring data gets evenly distributed across all nodes. When new nodes are added or removed from the cluster, existing data should be redistributed among all nodes without compromising the performance of the storage box.
OBJS.REQ.005	No single point of failure	Storage system must be offered with no single point of failure. The Scale-Out Storage should have capability 1 node failure in the storage system without data unavailability or data loss. Data should be striped across all storage nodes in the proposed storage system, so that performance of all nodes can be utilized for all read and write operations.
OBJS.REQ.006	Protocols and OS support	1. HTTP, S3. All protocols must be supported from Day1 with the storage. 2. Storage solution must support multiple protocols at the same time on the same piece of hardware including but not limited to HTTP, S3 . **3.** Must provide access for a variety of operating systems UNIX, Linux, and Windows latest versions
OBJS.REQ.007	Compression and de-duplication	Storage should be offered with the capability of inline/post process data reduction via compression . Licenses should be provided from day one for entire capacity.
OBJS.REQ.008	Management	Support the management, administration and configuration of the whole storage platform through a single management interface along with CLI. 1. Full View showing details like Cluster status with Zone, Server & Node details etc. 2. SNMP MiB Browsing, Traps and Graphical Usage Monitoring 3. Auditing capabilities. 4. REST APIs for monitoring & management 5. Offered storage shall support role Based Access

S.No.	Parameter	Minimum Specifications
		Control (RBAC) 6. Proposed storage should have monitoring and alert mechanism to report capacity, CPU and bandwidth utilization. 7. Proposed storage should maintain transactional logs and should support functionality to audit these logs.
OBJS.REQ.009	Security	The system must support encrypting data at rest. The system must be able to support Write Once Read Many (WORM) or equivalent compliant The system must support Role Base Access Control with Integration with Active Directory and LDAP. The system must be able to support System Auditing for system as well as supported protocols. The system should have automated file system integrity and data integrity checks built in to prevent data loss data integrity issues due to data inconsistencies or file system corruption
OBJS.REQ.0010	RANSOMEWARE Protection	Offered Storage must be supplied with safe & secure storage with Ransomware protection or any one of the following data protection mechanism: Inbuilt or through third party solution or immutable protection or application consistent snapshot or active vault & physical air gap tool or data isolation & air gaps or through WORM/versioning snapshots to protect data from any kind of attack and provide support (update and upgrades) from day 1, till the scope of the project + 2 years. The usable storage capacity as indicated in OBJ.REQ.001 must not be utilized for enabling these features."
OBJS.REQ.0011	IPv6 Support	All devices should be IPv6 ready from day 1.
OBJS.REQ.0012	Warranty & Post warranty Support	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.6 NETWORK ATTACHED STORAGE (NAS)

S.No.	Parameter	Minimum Specifications
NAS.REQ.001	Controllers and Architecture	1. Storage should be Fully Symmetric OR Asymmetric Clustered/Active-Active Load balanced Architecture for Scale-Out NAS/Scale-Up NAS. The Scale-out- NAS system must be Appliance and File System, where end to end HW, SW and OS has single lifecycle and from single OEM. 2. Storage must have purpose-built Operating System File System or Software defined storage Operating System and File System proprietary to OEM. 3. Architecture should have no single point of failure and must support non-disruptive firmware upgrade for end-to-end storage cluster. 4. At least Dual Storage controllers must be in active - active for performance and capacity.
NAS.REQ.002	Onboard Memory	Offered Storage solution should be configured with minimum 500GB or more DRAM based cache memory across controllers. Storage memory should be protected from power failure battery backed cache to protect cache for 24 hours. The usable storage capacity as above must be available after enabling all features as defined under minimum technical specifications.
NAS.REQ.003	NAS OS	Storage should be an appliance or Software defined storage Operating System and File System and all hardware, software and firmware support including upgrades, patches etc. must be provided by NAS OEM.
NAS.REQ.004	Network Ports (Per Controller)	Each storage controller must be offered with minimum 2 x 10G/25G optical ports populated with minimum 2x25G(SFP28) module from day1
NAS.REQ.005	Disk Type	Storage must support different kinds of disks types likes NVMe/SSD/SAS.
NAS.REQ.006	Total Storage Capacity and performance	Storage should be supplied with 500TB of usable space with 1. 20% of total capacity as NVME (TLC/MLC) SSD/ SSD as tier1 and 2. 80% of total capacity as 10K RPM SAS disks/ 7200 RPM NL - SAS or better from day1) as a solution (with single box or dual box)Solution to have erasure coding/ RAID6 with at least 2 disk protection (excluding all overhead configuration like configuration formatting and hot spare disk, de-dup). Overall performance of NAS solution must be minimum 3GBps for 32K block size. Overall performance of NAS solution must be minimum 3GBps for 32K block size.
NAS.REQ.007	Snapshots	Offered Storage must be supplied with safe & secure storage with Ransomware protection or any one of the following data protection mechanism: inbuilt or through third party solution or immutable protection or application consistent snapshot or active vault & physical air gap tool or data isolation & air gaps or through WORM/versioning snapshots to protect data from any kind of attack and provide support (update and upgrades) from day 1, till the scope of the project + 2 years. The usable storage as indicated in NAS.REQ.002 must not be utilized for enabling

S.No.	Parameter	Minimum Specifications
		these features.
NAS.REQ.008	Protocol Support	Storage must support latest version of protocols like NFS, SMB, CIFS etc. without additional licenses. Storage must support integration with directory services.
NAS.REQ.009	File Sharing	Storage should allow access to the same file via different protocol for data sharing.
NAS.REQ.0010	Management	Storage management, administration and configuration of the whole storage platform through a single management interface along with CLI and GUI
NAS.REQ.0011	Security	1. The system must have native support for Write Once Read Many (WORM) or equivalent, compliant to SEC17a-4. 2. Storage must offer Role Base Access Control (RBAC) with Integration with Active Directory and LDAP **3.** The system must offer System Auditing for system as well as supported protocols
NAS.REQ.0012	Scalability	The NAS should be scalable up to 2 PB. and additional controllers or cache as required must be offered to meet the same or better performance as provisioned from day 1.
NAS.REQ.0013	Warranty &Post warranty Support	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.7 SERVER RACKS

S.No.	Minimum Specifications
SR.REQ.001	Pre-configured IT rack consisting of welded symmetrical frame of rolled 16-fold profile all frame sections with integral system punching on a 25 mm DIN pitch pattern, Enclosures should be able on all sides: on the left, right, front and rear, at the top or round corners with four-point locking rod, comfort handle for semi-cylinder (30/10) mm, with security lock 3524. door hinge may be swapped to opposite side without dismantling locking rods. U labelling of both mounting levels can be read from the front for easy one-man assembly. Rear mounting angles prepared for both-sided accommodation of a Power Distribution Unit (PDU) space-saving side mounting between mounting level and side panel in the Zero-U space.
SR.REQ.002	42 U Network and server rack with static total load capacity of both mounting levels should be 15,000 N. enclosure must suit row-based climate control with sheet steel vented surface area with min 70% perforated front door and divided vented sheet steel door at the rear with 60% area, with roof plate and bottom cover, without side panels. With two 482.6 mm (19") mounting levels, front and rear, on depth stays and complete earthing kit side panels at the end of each row, one-piece screw fastened
SR.REQ.003	Material: Sheet steel,
SR.REQ.004	Surface finish: Nano Ceramic Coated, electro-dip coat primed to 20 microns and powder coated RAL 7035 to 80 to 120 microns
SR.REQ.005	Approvals: ISO 9001, 14001 and 45001 with UL60950-1, and UL2416,
SR.REQ.006	**IPPDU: -**2 No of IPPDU per rack High-end power distribution with 24xC13, 6xC19 Sockets in a compact design,
SR.REQ.007	**Technical specifications** i Feature- 3 Phase, 32 Amps PDUs, with per phase energy measurement. ii Input Voltage- 440V AC, 50-60Hz iii Input Current-32 Amps iv Slots EN 60 320/ C13- 24 Nos, Slots EN 60 320/ C19- 6 Nos v PDU Input Connector: EN 60 309/CEE vi Compliance RoHS Compliant vii Cable Length Min 03 mtrs viii LCD Display ix Ports RJ-45 – Ethernet, USB – For firmware update x Supported Protocols: HTTP Telnet, TCP/IP v4, DHCP, SNMPV1, FTP(SMTP) xi Support for Sensor types- Temperature, Temperature / humidity xii No. of Sensors per PDU: Min 02, xiii Environment Temperature: 0°C to 45°C xiv Humidity: 10 – 95 % relative humidity (Noncondensing) xv Parameters Measured Parameter Accuracy Voltage (V) Up to 2% Current (A) Up to 2% Frequency (Hz) Up to 2% Active Power (kW) Up to 2% Active Energy (kWh) Up to 2% Apparent Power (KVA) Up to 1% Power Factor monitoring Load Imbalance detection on dashboard MCB Monitoring

5.9 NETWORKING

5.10 TOR(L3) SWITCH

S.No.	Parameter	Minimum Specifications
TOR.REQ.001	**Solution Requirement**	The Switch should support non-blocking Layer 2 switching and Layer 3 routing
TOR.REQ.002		Power supplies and Fan should have 1:1/N+1 level of redundancy
TOR.REQ.003		Switch should support IEEE Link Aggregation/ Ethernet Bonding functionality to group multiple ports for redundancy
TOR.REQ.004		Switch should support VLAN tagging (IEEE 802.1q)
TOR.REQ.005		Switch should support Configuration roll-back and check point
TOR.REQ.006		Switch should support minimum 128 VRF instances
TOR.REQ.007		Switch should support minimum 3.6 Tbps or more of switching capacity & should be non-blocking capacity including the IP routing & forwarding, PBR, QOS, ACL and IPv6 host & IPv6 Routing services
TOR.REQ.008		The switch should support hardware-based sharing at wire speed using LACP and multi chassis Ethernet channel/LAG
TOR.REQ.009		The switch/ switch series and Switch OS should be EAL3/NDPP/NDcPP certified under Common Criteria.
TOR.REQ.0010		Switch should support the complete STACK of IPv4 and IPv6 services
TOR.REQ.0011	**H/w & Interfaces**	Proposed switch must have minimum 48x10G/25G Interfaces populated with minimum 44x25G(SFP28) module & 4x10G(SFP+) for Server connectivity And minimum 6x40/100G interfaces with 5x100G (QSFP28) & 1x40G (QSFP+)from day one for uplink connectivity
TOR.REQ.0012		should have console port and Management interface for out of Band management
TOR.REQ.0013		Switch should be rack mountable (1U) and support side rails if required
TOR.REQ.0014		Switch should have hardware health monitoring capabilities and should provide different parameters through SNMP
TOR.REQ.0015		Switch should support for different logical interface types like loopback, VLAN, SVI/RVI, Port Channel, multi chassis port channel/LAG etc.
TOR.REQ.0016	**Features**	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN /NVGRE
TOR.REQ.0017		Switch should support VXLAN and EVPN or equivalent for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data centre
TOR.REQ.0018		Switches supplied/offered must be SDN ready from day 1 & compatible with SDN solution offered under this RFP
TOR.REQ.0019	**L2 support**	Spanning Tree Protocol (IEEE 801.D, 802.1W, 802.1S)
TOR.REQ.0020		Switch should support VLAN Trunking (802.1q) and should support minimum 4000 VLAN
TOR.REQ.0021		Switch should support basic Multicast IGMP v1, v2, v3

S.No.	Parameter	Minimum Specifications
TOR.REQ.0022		Switch should support minimum 90K or more no. of MAC addresses
TOR.REQ.0023		Switch should support 8 Nos. of link or more per Port channel (using LACP) and support 48 port channels or more per switch
TOR.REQ.0024		Switch should support Industry Standard Port/Link Aggregation for All Ports across any module or any port.
TOR.REQ.0025		Switch should support multi chassis Link Aggregation for All Ports across any module or any port of the switch and Link aggregation should support 802.3ad LACP protocol for communication with downlink/uplink any third-party switch or server
TOR.REQ.0026		Solution must support TACACS+, RADIUS, LDAP or Local Authentication. It must also provide an integration with the syslog servers
TOR.REQ.0027		Switch should support Jumbo Frames up to 9K Bytes on all available Ports
TOR.REQ.0028		Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities
TOR.REQ.0029		Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures
TOR.REQ.0030	**L3 Support**	Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface
TOR.REQ.0031		Switch should support basic routing feature i.e. IP Classless, default routing and Inter VLAN routing
TOR.REQ.0032		Switch should support static and dynamic routing protocol IS-IS/OSPF, BGP, MSDP and Multicast PIM-SM & PIM-SSM., RIP
TOR.REQ.0033		Switch should provide multicast traffic reachable using PIM-SM, PIM-SSM/Bi-Dir-PIM, IGMP v1 v2 &v3
TOR.REQ.0034		Switch should support minimum 64 k IPv4, min 64K IPv6 and 6k Multicast
TOR.REQ.0035	**Additional features**	Switch should provide gateway level of redundancy in IPv4 and IPv6 using HSRP/VRRP
TOR.REQ.0036		Telemetry & Visibility using Netflow/jflow/sflow, SPAN, RSPAN /Remote Port Mirroring
TOR.REQ.0037		Switch should support for BFD for Fast Failure Detection as per RFC 5880
TOR.REQ.0038	**QOS**	Switch system should support 802.1P classification and marking of packet using CoS, DSCP, Source physical interfaces, Source/destination IP subnet, Source/destination TCP/UDP ports and Protocol types (IP/TCP/UDP)
TOR.REQ.0039		Switch should support methods for identifying different types of traffic for better management and resilience using QOS

S.No.	Parameter	Minimum Specifications
TOR.REQ.0040		Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy
TOR.REQ.0041		The Switch should support DC Bridging i.e. IEEE 802.1Qbb Priority Flow Control (PFC), Data Centre Bridging Exchange (DCBX), IEEE 802.1Qaz Enhanced Transmission Selection (ETS), Explicit Congestion Notification (ECN).
TOR.REQ.0042	**Security**	Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail
TOR.REQ.0043		Switch should support for stringent security policies based on time of day of Layer-2 to Layer-4
TOR.REQ.0044		Switch should support for external database for AAA using TACACS+ & RADIUS
TOR.REQ.0045		The switch should support DHCP Server providing DHCP services (for IPv4 and IPv6) with DHCP snooping
TOR.REQ.0046		Switch should support Spanning tree BPDU protection Proprietary
TOR.REQ.0047		Switch should support Dynamic ARP Inspection or equivalent to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol
TOR.REQ.0048	**MGMT**	Switch should support for embedded RMON/RMON-II/SNMP(v2/v3 or both) for central NMS management and monitoring.
TOR.REQ.0049		Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail
TOR.REQ.0050		Switch should provide remote login for administration using Telnet & SSHv2
TOR.REQ.0051		Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures
TOR.REQ.0052		Switch should support for management and monitoring status using different type of Industry standard NMS using SNMP v1 v2 & v3, Filtration of SNMP using access list, SNMP MIB support for QoS
TOR.REQ.0053		Switch should support central time server synchronization using Network Time Protocol NTP v4
TOR.REQ.0054		Switch should provide different privilege for login in to the system for monitoring and management
TOR.REQ.0055		All Functionalities of Switch shall be IPv6 compliant, and it should work on IPv6 Platform without any additional hardware/ software.
TOR.REQ.0056		Switch and optics should be from the same OEM
TOR.REQ.0057		The switch should support netflow/sFlow or equivalent for traffic analysis
TOR.REQ.0058		All required Cables, Accessories and Licences should be provided from Day-1
TOR.REQ.0059	**Warranty & Post warranty Support**	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.11 SPINE CORE

S.No.	Parameter	Minimum Specification
SC.REQ.001	**General Requirement**	The Switch should support non-blocking Layer 2 switching and Layer 3 routing
SC.REQ.002		Switch should support the complete STACK of IP V4 and IPV6 services. (Static routing, BGP,PBR, Multicast Routing, Vx- lan with BGP,MPLS/GRE
SC.REQ.003		All the features mentioned in the specifications shall be enabled/activated. Any licenses required shall be included from Day 1
SC.REQ.004	**Hardware and Interface Requirement**	The switch should have minimum 32 ports of 40G/100GbE POPULATED WITH 24 QSFP28(100Gbps) and minimum 8 ports of 40G/100GbE POPULATED WITH 8 QSFP+(40Gbps) Tansceivers from day 1
SC.REQ.005		Switch should have console port for local management & management interface for Out of band management
SC.REQ.006		The switch should have dual, redundant, field-replaceable, hot-swappable power supplies and field-replaceable, hot-swappable fans with front-to-back airflow
SC.REQ.007	**Performance Requirement**	The switch should support 100,000 IPv4 unicast routes and 100,000 IPv6 unicast routes entries.
SC.REQ.008		Switch should support minimum 128 VRF instances with route leaking functionality
SC.REQ.009		The switch proposed should have minimum 32 MB Packet Buffer
SC.REQ.0010		The switch should support minimum 6k multicast routes
SC.REQ.0011		Switch should support a minimum of 6.4.Tbps BW
SC.REQ.0012		The proposed switch should have minimum 16GB DRAM, 8GB Flash Memory.
SC.REQ.0013	**Layer2** Features	Switch should support Network Virtualisation using Virtual Over Lay Network using VXLAN (RFC 7348)
SC.REQ.0014		Switch should support VXLAN & EVPN for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data centre
SC.REQ.0015		IEEE 802.1D Spanning Tree Protocol, IEEE 802.1w Rapid Spanning Tree Protocol and IEEE 802.1s Multiple Spanning Tree Protocol
SC.REQ.0016		Switch should support VLAN Trunking (802.1q)
SC.REQ.0017		Switch should support minimum 90K no. of MAC addresses
SC.REQ.0018		Switch should support VLAN tagging (IEEE 802.1q)
SC.REQ.0019		The switch should support hardware based load sharing at wire speed using LACP and multi chassis ether channel/LAG, should support 8 Nos. of link or more per Port channel (using LACP).
SC.REQ.0020		Switch should support layer 2 extension over VXLAN (RFC7348) across all DataCenter to enable VM mobility & availability
SC.REQ.0021		Switch should provide gateway level of redundancy in IPv4 and IPv6 using HSRP/ VRRP
SC.REQ.0022	**Layer3 Features**	Switch should support static and dynamic routing
SC.REQ.0023		Switch should provide multicast traffic reachable using: (PIM-SM (RFC 4601), PIM-SSM (RFC 3569),
SC.REQ.0024		The switch should support Internet Group Management

S.No.	Parameter	Minimum Specification
		Protocol (IGMPv1, v2, and v3) and Multicast Listener Discovery (MLDv1 and v2)
SC.REQ.0025		The Device should support 802.1p CoS and DSCP classification, ACL based classification, VLAN based classification.
SC.REQ.0026	**Quality of Service**	The switch should support Strict priority (SP) queuing, Explicit Congestion Notification (ECN) or equivalent for congestion avoidance and Access control lists (ACLs) for both IPv4 and IPv6 traffic
SC.REQ.0027		Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x
SC.REQ.0028		Switch should support for external database for AAA using TACACS+ / Radius
SC.REQ.0029		Switch should support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding
SC.REQ.0030		Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined
SC.REQ.0031		Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail e.g. Sflow
SC.REQ.0032		Switch should provide remote login for administration using: (telnet, SSHv2)
SC.REQ.0033		Device should support local and encapsulated remote port mirroring with support for ACL filtering for targeted capture analysis/reporting and simplified troubleshooting.
SC.REQ.0034		Switch should support for management and monitoring status using different type of Industry standard NMS using: (SNMP v3 with Encryption)
SC.REQ.0035		The switch should have Command Line Interface (CLI) with a hierarchical structure and SSH, Secure FTP/TFTP support
SC.REQ.0036		The switch should support Precision Time Protocol (PTP)/NTP
SC.REQ.0037	**Certifications and Industry Recognition**	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support
SC.REQ.0038		The switch should be Common Criteria Certified (EAL or NDPP or NDcPP)
SC.REQ.0039		The switch should have RoHS compliance
SC.REQ.0040		Switches supplied/offered must be SDN ready from day 1 & compatible with SDN solution offered under this RFP

5.12 L3 SWITCH (FIBRE)

S.No.	Minimum Specifications
Form Factor	
L3S.REQ.001	19" Rack Mountable 1U Height with Redundant Power Supply (RPS) from day 1
Architecture	
L3S.REQ.002	Switch Should support memory of minimum 8 GB DRAM and 8 GB Flash memory or more to support multiple software images for backup purposes, log report and future scalability
L3S.REQ.003	The switch throughput of minimum 3 Tbps or more without compromising on Switching & routing performance from day 1
L3S.REQ.004	Traffics handling capacity should be minimum 500 Mpps from Day 1
L3S.REQ.005	Should support jumbo frames
L3S.REQ.006	The switch should have Redundant, Hot Swappable Power supply from day one
L3S.REQ.007	Should have at least 100k IPv4, 50k IPv6 routes and 6k Multicast Routes
L3S.REQ.008	Switch should support Clustering/stacking of at least 2 switches through stacking / MC-LAG or equivalent technology
L3S.REQ.009	All modules/ SFP, fan trays & Power supplies should be hot swappable
Interfaces	
L3S.REQ.0010	Minimum 48x10/25 Gbps ports populated with minimum 12x25G SFP28 & 36x10G SFP+ and minimum 6x40/100G ports populated with 6xQSFP+ (40Gbps) trans receiver for From day 1
Protocols	
L3S.REQ.0011	Should have static routing, RIP, OSPF, OSPFv3, uRPF, VRRP, PBR, IP SLA/RPM or equivalent PIM, PIM SSM, BGP
L3S.REQ.0012	IEEE Standards IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 1588v2/NTP
L3S.REQ.0013	Should Support Segmentation Protocol Network segmentation protocols VXLAN and VRF/virtual router, EVPN.
L3S.REQ.0014	At least 64K MAC Addresses and at least 4000 active VLAN.
L3S.REQ.0015	Should Support management protocols SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS and TACACS+.
L3S.REQ.0016	IPV6 Ready from day 1
Security	
L3S.REQ.0017	802.1x authentication and accounting, IPv4 and IPv6 ACLs, Dynamic VLAN assignment and should support SSH, TLS based /GUI based interface access to the switch for out of band Management
L3S.REQ.0018	Should provide IPv6 Security mechanism viz. IPv6 RA Guard or equivalant, IPv6 DHCP Guard/DHCP snooping, IPv6 Neighbour Discovery, Source Guard etc.
L3S.REQ.0019	Telemetry & Visibility using Netflow/jflow/sflow, SPAN, RSPAN /Remote Port Mirroring
L3S.REQ.0020	Should support QOS 802.1p class of service, marking, classification, policing and shaping and at least eight egress queues.
L3S.REQ.0021	The switch/ switch series and Switch OS should be EAL3/NDPP/NDcPP certified under Common Criteria.

S.No.	Minimum Specifications
L3S.REQ.0022	All required Cables, Accessories and Licences should be provided from Day-1
Warranty & Post warranty Support	
L3S.REQ.0023	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support
L3S.REQ.0024	Switches supplied/offered must be SDN ready from day 1 & compatible with SDN solution offered under this RFP

5.13 L3 COPPER

S.No.	Minimum Specifications
Form Factor	
L3C.REQ.001	19" Rack Mountable 1U Height with Redundant Power Supply (RPS) from day 1
Architecture	
L3C.REQ.002	Switch Should support memory of minimum 8 GB DRAM and 8 GB Flash memory or more to support multiple software images for backup purposes, log report and future scalability
L3C.REQ.003	The switch throughput of minimum 1.32 Tbps or more without compromising on Switching & routing performance from day 1
L3C.REQ.004	Traffics handling capacity should be minimum 500 Mpps from Day 1
L3C.REQ.005	Should support jumbo frames
L3C.REQ.006	The switch should have Redundant, Hot Swappable Power supply from day one
L3C.REQ.007	Should have at least 100k IPv4, 50k IPv6 routes and atleast 6k Multicast Routes
L3C.REQ.008	Switch should support Clustering/stacking of at least 2 switches through stacking / MC-LAG or equivalent technology
L3C.REQ.009	All modules/ SFP, fan trays & Power supplies should be hot swappable
Interfaces	
L3C.REQ.0010	Should be supplied with 48 x 1/10G ethernet ports(RJ45) and with minumum 2x40/100Gbps ports populated with minimum 2xQSFP+ (40Gbps) transreceiver for Uplink From day 1
Protocols	
L3C.REQ.0011	Should have static routing, RIP, OSPF, OSPFv3, uRPF, VRRP, PBR, IP SLA/RPM or equivalent PIM, PIM SSM, BGP
L3C.REQ.0012	IEEE Standards IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 1588v2/NTP
L3C.REQ.0013	Should Support Segmentation Protocol Network segmentation protocols VXLAN and VRF/virtual router, EVPN.
L3C.REQ.0014	At least 64K MAC Addresses and at least 4000 active VLAN.
L3C.REQ.0015	Should Support management protocols SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS and TACACS+.
L3C.REQ.0016	IPV6 Ready from day 1
Security	
L3C.REQ.0017	802.1x authentication and accounting, IPv4 and IPv6 ACLs, Dynamic VLAN assignment and should support SSH, TLS based/GUI Based interface access to the switch for out of band Management
L3C.REQ.0018	Should provide IPv6 Security mechanism viz. IPv6 RA Guard or equivalant, IPv6 DHCP Guard/DHCP snooping, IPv6 Neighbour Discovery, IPv6 Source Guard etc.
L3C.REQ.0019	Telemetry & Visibility using Netflow/jflow/sflow, SPAN, RSPAN /Remote Port Mirroring
L3C.REQ.0020	
L3C.REQ.0021	Should support QOS 802.1p class of service, marking, classification, policing and shaping and at least eight egress queues.
L3C.REQ.0022	The switch/ switch series and Switch OS should be EAL3/NDPP/NDcPP certified under Common Criteria.
L3C.REQ.0023	All required Cables, Accessories and Licences should be provided from Day-1
Warranty & Post warranty Support	
L3C.REQ.0024	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support
L3C.REQ.0025	Switches supplied/offered must be SDN ready from day 1 & compatible with

S.No.	Minimum Specifications
	SDN solution offered under this RFP

5.14 CORE ROUTER- DC

S.No.	Minimum Specifications
CRDC.REQ.001	Proposed Router should be modular based and shall have Redundant control Plane.
CRDC.REQ.002	Should have N+1 power supply redundancy. There should not be any impact on The Router performance in case one of the power supplies fails
CRDC.REQ.003	All power supplies should be hot swappable for high availability
CRDC.REQ.004	IPv4 Routing, IPv6 Routing Border Gateway Protocol, Intermediate System-to-Intermediate System [IS-IS], Open Shortest Path First [OSPF]), IGMP, PIM SSM, OSPFv3 for IPv6,
CRDC.REQ.005	MPLS TE (Fast re-route), DiffServ-Aware TE, Inter-AS VPN, Resource Reservation Protocol (RSVP), VPLS, BGP-LU, LDP, EVPN, L2VPN, L3VPN
CRDC.REQ.006	Proposed router should be supplied with minimum 16x1/10G Interfaces populated with 16xSR SFP+(10G) modules & minimum 2x100G Interface POPULATED WITH 02 QSFP28(100Gbps)Transceivers from day one. Proposed Router should support upscaling of ports by upgrading OS/License/Line cards in Future with minimum one vacant expansing slots.
CRDC.REQ.007	The Router Hardware should support at least 1 Tbps (Full Duplex) throughput rate.
CRDC.REQ.008	The router should support the following functionality from the day one:-
CRDC.REQ.009	a) Minimum 3 M IPv4 FIB
CRDC.REQ.0010	b) Minimum 1M IPv6 RIB/FIB
CRDC.REQ.0011	c) Minimum 10K MPLS Labels
CRDC.REQ.0012	d) router should be able to route Label Stack.
CRDC.REQ.0013	The operating system shall be modular and run all critical functions (E.g.; Routing protocols, Forwarding plane, management tasks) in separate memory protected modules.
CRDC.REQ.0014	Router shall have option of checking configuration before committing and option of rolling back.
CRDC.REQ.0015	Digital Optical Monitoring (DOM) should be supported, optics information retrievable including RX/TX-power, threshold- monitoring/alarming, inventory.
CRDC.REQ.0016	It shall support role based privileges for the system access and RADIUS/TACAS authentication for the System admin.
CRDC.REQ.0017	The router should have a Console or Out-of-band Management.
CRDC.REQ.0018	All interfaces shall support services like L2VPN, L3VPN and multicast VPN for both IPv4 and IPv6
	Security:
CRDC.REQ.0019	a) The router should have mechanism to protect itself from DDoS attack.
CRDC.REQ.0020	The router should support filtering based on different parameters like: src ip, dst ip, src port, dst port, protocol etc
CRDC.REQ.0021	The router should support IPFIX, Netflow/ Jflow or equivalent.
CRDC.REQ.0022	The router should support IP SLA or RPM (or equivalent) for performance measurements, it should also support monitoring of IP SLA/RPM (or equivalent) probes using SNMP polling or through syslog
CRDC.REQ.0023	Shall support Strict Priority Queuing or Low Latency Queuing to support real time application like Voice and Video with minimum delay and jitter
CRDC.REQ.0024	Should support following class of service features as : Classification, policing, marking, shaping, filtering
CRDC.REQ.0025	b) Manage congestion using a weighted random early detection (WRED) algorithm
CRDC.REQ.0026	c) RFC 2474, Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers

S.No.	Minimum Specifications
CRDC.REQ.0027	d) Single Rate Three Color Policer RFC 2697
CRDC.REQ.0028	e) RFC 2698, A Two Rate Three Color Policer
CRDC.REQ.0029	f) Round Robin, WFQ, CBWFQ scheduling algorithms or equivalent
CRDC.REQ.0030	g) Router should be able to classify based on 802.1 ad, 802.1 p, EXP and DSCP bits
CRDC.REQ.0031	The router shall support traffic interface mirroring in both directions for both IPv4 & IPv6.
CRDC.REQ.0032	The router shall support provision for event based scripts that shall be capable of performing actions based on certain triggers
CRDC.REQ.0033	The router shall support aggregated Ethernet and it shall be possible to bundle minimum 4 links.
CRDC.REQ.0034	IGMP v1 v2 and v3 as described in RFC 2236 and RFC 3376 with IGMP Routing Policies to filter IGMP requests.
CRDC.REQ.0035	Router shall support SNMP v2/v3 and NTP
CRDC.REQ.0036	Shall support BFD: single hop, multi-hop and micro BFD
CRDC.REQ.0037	Router to support GRE tunnels (RFC 2784)
CRDC.REQ.0038	The device should comply to the following safety standards
CRDC.REQ.0039	a) EN 55022 Class A Emissions (Europe) or higher
CRDC.REQ.0040	b) FCC Class A (USA) Radiated Emissions
CRDC.REQ.0041	c) UL 60950-1 Information Technology Equipment - Safety
CRDC.REQ.0042	d) EN 60825-1 /EN60950-1 Safety of Laser Products or higher
CRDC.REQ.0043	Router Should Support Dual Image/Partition with USB flash drive booting option for OS recovery
CRDC.REQ.0044	Router should support jumbo frame.
CRDC.REQ.0045	Router should comply to following Temperature performance parameters:
CRDC.REQ.0046	i. Operating Temperature: 0 to 40 degree C or better
CRDC.REQ.0047	ii. Storage Temperature: -10 to 60 degree C or better
CRDC.REQ.0048	The operating system of the Routers category/series/family should be MEF-9/14 or CE (Carrier Ethernet) or latest Certified/compliant if not then roadmap for the same shall be submitted at the time of bidding.
CRDC.REQ.0049	The Router shall be designed for continuous operations with dual fan system.
CRDC.REQ.0050	Routers should be rack mountable to fit into a standard 19-inch rack
CRDC.REQ.0051	The OEM shall ensure that supplied optics shall be from same OEM
	Segment Routing
CRDC.REQ.0052	a) The router should support SR-MPLS data plane and protocols , OSPF/IS- IS (or both) and BGP Segment routing extensions
CRDC.REQ.0053	b) Traffic Steering of SR policies with Autoroute Include and Segment Routing TI-LFA SRLG Protection
CRDC.REQ.0054	C) Mandatory: LSP ping, trace-route & Desireable: Pseudo wire Ping over Segment Routing, trace route for binding-SID
CRDC.REQ.0055	d) MPLS-LDP interworking with SR-ISIS/SR-OSPF
CRDC.REQ.0056	f) Shall support SR and MPLS (LDP) Interworking Mapping Server
CRDC.REQ.0057	g) Label distribution protocol and segment routing should coexist and there should support option to prefer LDP over segment routing.
CRDC.REQ.0058	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.15 ROUTER NL-DR

S.No.	Minimum Specifications
RNLDR.REQ.001	Proposed Router should be modular based and shall have Redundant control Plane.
RNLDR.REQ.002	Should have N+1 power supply redundancy. There should not be any impact on The Router performance in case one of the power supplies fails
RNLDR.REQ.003	All power supplies should be hot swappable for high availability
RNLDR.REQ.004	IPv4 Routing, IPv6 Routing Border Gateway Protocol, Intermediate System-to-Intermediate System [IS-IS], Open Shortest Path First [OSPF]), IGMP, PIM SSM, OSPFv3 for IPv6,
RNLDR.REQ.005	MPLS TE (Fast re-route), DiffServ-Aware TE, Inter-AS VPN, Resource Reservation Protocol (RSVP), VPLS, BGP-LU, LDP, EVPN, L2VPN, L3VPN
RNLDR.REQ.006	Proposed router should be supplied with minimum 06x1/10G Interfaces populated with 06xSR SFP+(10G) modules & minimum 2x100G Interface POPULATED WITH 02 QSFP28(100Gbps) Transceivers from day one. Proposed Router should support upscaling of ports by upgrading OS/License/Line cards in Future with minimum one vacant expansion slot.
RNLDR.REQ.007	The Router Hardware should support at least 0.5 Tbps (Full Duplex) throughput rate.
RNLDR.REQ.008	The router should support the following functionality from the day one: -
RNLDR.REQ.009	a) Minimum 3 M IPv4 FIB
RNLDR.REQ.0010	b) Minimum 1M IPv6 RIB/FIB
RNLDR.REQ.0011	c) 10K MPLS Labels
RNLDR.REQ.0012	d) router should be able to route Label Stack.
RNLDR.REQ.0013	The operating system shall be modular and run all critical functions (E.g.; Routing protocols, Forwarding plane, management tasks) in separate memory protected modules.
RNLDR.REQ.0014	Router shall have option of checking configuration before committing and option of rolling back.
RNLDR.REQ.0015	Digital Optical Monitoring (DOM) should be supported, optics information retrievable including RX/TX-power, threshold- monitoring/alarming, inventory.
RNLDR.REQ.0016	It shall support role based privileges for the system access and RADIUS/TACAS authentication for the System admin.
RNLDR.REQ.0017	The router should have a Console or Out-of-band Management.
RNLDR.REQ.0018	All interfaces shall support services like L2VPN, L3VPN and multicast VPN for both IPv4 and IPv6
	Security:
RNLDR.REQ.0019	a) The router should have mechanism to protect itself from DDoS attack.
RNLDR.REQ.0020	The router should support filtering based on different parameters like: src ip, dst ip, src port, dst port, protocol etc
RNLDR.REQ.0021	The router should support IPFIX, Netflow/ Jflow or equivalent.
RNLDR.REQ.0022	The router should support IP SLA or RPM (or equivalent) for performance measurements, it should also support monitoring of IP SLA/RPM (or equivalent) probes using SNMP polling or through syslog
RNLDR.REQ.0023	Shall support Strict Priority Queuing or Low Latency Queuing to support real time application like Voice and Video with minimum delay and jitter
RNLDR.REQ.0024	Should support following class of service features as : Classification, policing, marking, shaping, filtering

S.No.	Minimum Specifications
RNLDR.REQ.0025	b) Manage congestion using a weighted random early detection (WRED) algorithm
RNLDR.REQ.0026	c) RFC 2474, Definition of the Differentiated Services Field in the IPv4 and IPv6 Headers
RNLDR.REQ.0027	d) Single Rate Three Color Policer RFC 2697
RNLDR.REQ.0028	e) RFC 2698, A Two Rate Three Color Policer
RNLDR.REQ.0029	f) Round Robin, WFQ, CBWFQ scheduling algorithms or equivalent
RNLDR.REQ.0030	g) Router should be able to classify based on 802.1 ad, 802.1 p, EXP and DSCP bits
RNLDR.REQ.0031	The router shall support traffic interface mirroring in both directions for both IPv4 & IPv6.
RNLDR.REQ.0032	The router shall support provision for event based scripts that shall be capable of performing actions based on certain triggers
RNLDR.REQ.0033	The router shall support aggregated Ethernet and it shall be possible to bundle minimum 4 links.
RNLDR.REQ.0034	IGMP v1 v2 and v3 as described in RFC 2236 and RFC 3376 with IGMP Routing Policies to filter IGMP requests.
RNLDR.REQ.0035	Router shall support SNMP v2/v3 and NTP
RNLDR.REQ.0036	Shall support BFD: single hop, multi-hop and micro BFD
RNLDR.REQ.0037	Router to support GRE tunnels (RFC 2784)
RNLDR.REQ.0038	The device should comply to the following safety standards
RNLDR.REQ.0039	a) E N 55022 Class A Emissions (Europe) or Higher
RNLDR.REQ.0040	b) FCC Class A (USA) Radiated Emissions
RNLDR.REQ.0041	c) UL 60950-1 Information Technology Equipment - Safety
RNLDR.REQ.0042	d) EN 60825-1 /EN60950-1 Safety of Laser Products or higher
RNLDR.REQ.0043	Router Should Support Dual Image/Partition with USB flash drive booting option for OS recovery
RNLDR.REQ.0044	Router should support jumbo frame.
RNLDR.REQ.0045	Router should comply to following Temperature performance parameters:
RNLDR.REQ.0046	i. Operating Temperature: 0 to 40 degree C or better
RNLDR.REQ.0047	ii. Storage Temperature: -10 to 60 degree C or better
RNLDR.REQ.0048	The operating system of the Routers category/series/family should be MEF-9/14 or CE(Carrier Ethernet) or latest Certified/compliant if not then roadmap for the same shall be submitted at the time of bidding.
RNLDR.REQ.0049	The Router shall be designed for continuous operations with dual fan system.
RNLDR.REQ.0050	Routers should be rack mountable to fit into a standard 19-inch rack
RNLDR.REQ.0051	The OEM shall ensure that supplied optics shall be from same OEM
RNLDR.REQ.0052	Segment Routing
RNLDR.REQ.0053	a) The router should support SR-MPLS data plane and protocols , OSPF/IS- IS (or both) and BGP Segment routing extensions
RNLDR.REQ.0054	b) Traffic Steering of SR policies with Autoroute Include and Segment Routing TI-LFA SRLG Protection
RNLDR.REQ.0055	c) Mandatory: LSP ping, trace-route Desirable: Pseudo wire Ping over Segment Routing, trace route for binding-SID
RNLDR.REQ.0056	d) M PLS-LDP interworking with SR-ISIS / SR-OSPF
RNLDR.REQ.0057	f) Shall support SR and MPLS (LDP) Interworking Mapping Server

S.No.	Minimum Specifications
RNLDR.REQ.0058	g) Label distribution protocol and segment routing should coexist and there should support option to prefer LDP over segment routing.
RNLDR.REQ.0059	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.16 FABRIC MANAGER SDN

S. No.	Minimum Specifications
SDN.REQ.001	The overall System network design & operations must be based on Open Standards' implementation for Networking, with the minimum of eBGP/OSPF underlay, eBGP/MP-BGP/EVPN overlay and VXLAN H/W VTEP where required.
SDN.REQ.002	The overall System must provide the capability to build both simple and complex analytics, against the context of the reference design and network topology.
SDN.REQ.003	Interaction between the Central Server and the switching fabric must be held on the management plane only and Fabric must have fully distributed architecture
SDN.REQ.004	The system must provide open APIs to enable an automated system wide build of the DC
SDN.REQ.005	The deployed network must be able to operate and run without interruption, in case the Central Server is not present for any reason. There must not be any relationship between the Central Server and the operational running of the Fabric.
SDN.REQ.006	The System must enable integration between physical and virtualised infrastructures under the scope of this RFP.
SDN.REQ.007	The System must provide Spine & Leaf Fabric design capability.
SDN.REQ.008	The System must provide a web-based UI to design, build, deploy & Monitor Spine & Leaf Fabric.
SDN.REQ.009	The System must provide hardware and software abstraction layer or orchestration layer for underlay network proposed in this RFP so that underlay and overlay designs can be created.
SDN.REQ.0010	.The System must provide/show the number of ports between the leaf (Top of Rack) and spine switches.
SDN.REQ.0011	.The System must provide an easily exportable/ viewable Cabling Map/topology for the completed Fabric.
SDN.REQ.0012	The System must provide an open API that enables the networking Fabric to be built to the very same level as the UI.
SDN.REQ.0013	The System must provide the capability to design (stage) the networking Fabric as one, i.e. not switch-by-switch, through a single interface.
SDN.REQ.0014	The System must not be constructed of separate sub-systems stitched together by one overarching UI, which independently serve design, build, deploy and operations' capabilities. Network Devices should be auto discovered with quick deployment options for network wide configuration deployment.
SDN.REQ.0015	The System must provide the capability to build and extend the Fabric design quickly and easily, by utilising addressing pools i.e. ASNs, IPv4, IPv6 VNIs.
SDN.REQ.0016	The System must provide the capability to build a complete network representation in which logical layers can be applied, with a minimum of all addressing information (IP / ASNs / VNIs), VRFs and the overlay.
SDN.REQ.0017	The System must provide continuous, closed-loop validation or configuration comparisons of the desired Fabric state (as declared in design, build or deploy phase) /configuration against the actual operational state/configuration of the physical network.
SDN.REQ.0018	The System must provide the capability to dynamically extend, or modify, the Fabric representation, and push & rollback such changes to the running Fabric through a single interface.
SDN.REQ.0019	The solution should provide realtime monitoring of various parameter of the network using realtime state streaming telemetry or better technology.
SDN.REQ.0020	The fabric should have centralised dashboard to upgrade the entire fabric with ease without incurring traffic downtime in fabric core.

S. No.	Minimum Specifications
	The System must integrate with 3rd-party systems through open APIs for additional reporting, with the minimum of time series databases and graphing applications.
SDN.REQ.0021	All the hardware, software and licenses must be included as part of the solution as per the required specification from Day 1
SDN.REQ.0022	Technical support for solution must be directly from single OEM. OEM should have 24x7 available over email and Phone.
SDN.REQ.0023	1. Solution offered for fabric-manager/SDN must be compatible with all network devices offered under this RFP & All licences should be provided with the devices for the mentioned features. The licences should be perpetual/Subscription based in nature and must be supplied from day -1. 2. Solution must also integrate seamlessly/independently with virtualization solution offered through this RFP and should provide/support micro-segmentation from day 1 3. Any/all Licences if Subscription must be supplied for duration of scope of the project in this RFP + 2 years
SDN.REQ.0024	Anything extra (e.g. transceiver, fiber cables, etc) required to setup the fabric as per requirement has to be provided by the bidder without any extra cost from day 1.
SDN.REQ.0025	Fabric manager/controller should not be part of the data plane and a network device must continue to forward packet in case it looses connectivity to the manager.
SDN.REQ.0026	Fabric should be capable to show in real time congestion hotspots in the network with Link Level utilization/ buffer level utilization info from the network devices.
SDN.REQ.0027	The solution is expected to provide realtime monitoring of various parameters like CPU, Memory, interface stats (traffic counter, error, discard), MAC table, ARP table, IPv6 ND table, RIB, BGP, capacity parameters file system storage parameters, VXLAN, running config, traffic flow (sflow/IPFIX/Netflow), POE utilization stats, LLDP, MLAG /ESILAG Stats, Switch environment stats (FAN, Temperature, Power Supply), etc with streaming telemetry.
SDN.REQ.0028	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.17 GLOBAL SERVER LOAD BALANCER (GSLB)

S.No.	Parameter	**Minimum Specification**
GSLB.REQ.001	Traffic Ports support	The appliance must have minimum 4 x 10G SFP+ port populated from day1 . The appliance should have dedicated Out-of-band Management Port and Console Port.
GSLB.REQ.002	Device L4 Throughput	Device L4 Throughput: Minimum 20 Gbps with capacity to scale upto minimum 40 Gbps (to support 40Gbps ISP link)
GSLB.REQ.003	Device L7 Throughput	Should be minimum 60-80% of the L4 throughput
GSLB.REQ.004	Layer 4 Concurrent Connection	Concurrent Connections: 40 Million
GSLB.REQ.005	Layer 4 connections per second	At least 750K connections per sec
GSLB.REQ.006	Layer 7 requests per second	At least 1250K connections per sec
GSLB.REQ.007	RAM & Harddisk	Device must be supplied with sufficient RAM to meet and sustain above performance parameters along with minimum 400 GB Hard disk capacity with enough storage to store log up to minimum 2 months from day1.
GSLB.REQ.008	Virtualization	The proposed device should have Hypervisor Based Virtualization feature(that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. Should be capable of virtualization and support minimum 2 and scalable up to 4 virtual instances each virtual instance having dedicated resources including hard disk, CPU, RAM, Operating system and SSL resources from day1
GSLB.REQ.009	Topology	Following Topologies or Equivalent should be supported: • Client Network Address Translation (Proxy IP)-InLine • Mapping Ports --- Aggregation • Direct Server Return----Asymmetric Topology • One Arm Topology Application ---Out of Path Mode • Direct Access Mode -Client and Server ITP preserve • Assigning Multiple IP Addresses---VLAN
GSLB.REQ.0010	Network	Should support for IPv4 and IPv6 traffic along with DNS functionality from day-1. The solution should provide compressive support for IPv6 functions to help with ipv4-to-ipv6 transition without business disruption and must provide support for dual stack, NAT 64, DNS 64, NAT 46, IPv6 NAT, etc
GSLB.REQ.0011		It should support advance functions Authoritative name sever, DNS proxy /DNS NAT, full DNS server with DNSEC, application load balancing from day one. It should be capable of handling complete Full DNS bind records including A,MX, AAAA, CNAME, NAPTR, NS,PTR, SOA, SRV, TXT etc. independently
GSLB.REQ.0012		The proposed device should support standard VRRP for High Availability purpose or equivalent

S.No.	Parameter	**Minimum Specification**
GSLB.REQ.0013		The Load Balancer Shall have full traffic control and be able to route requests to servers based on region, device, browser, or a number of other factors. This enables organization to deliver customized application responses to users. Device must have Dynamic routing protocols like OSPF, RIP1, RIP2, BGP or equivalent from Day 1
GSLB.REQ.0014		The Proposed Solution must have performed load balancing for Layers 4 through 7 of the Open Systems Interface (OSI) reference model with support to the IP, TCP and UDP protocols
GSLB.REQ.0015		The Proposed Solution must have the ability to configure TCP and UDP health check for real web servers
GSLB.REQ.0016		Appliance should support Local Application Switching, Server load Balancing, HTTP, TCP Multiplexing, Compression, Caching, TCP Optimization, Filter-based Load Balancing, Content-based Load Balancing, Persistency, HTTP Content Modifications
GSLB.REQ.0017		The Proposed Solution must have TCP Multiplexing
GSLB.REQ.0018	Matrices	The proposed appliance should support the below metrics or similar metrices: — Hash, — Weighted Hash, — Least Connections, — Least Connections Per Service, — Round-Robin, — Response Time, — Bandwidth, etc
GSLB.REQ.0019	Application/ Others	The Proposed Solution must have diagnostics which are readily available and easy to send to support (capture core dumps, configurations, logs, and so on)
GSLB.REQ.0020		Solution must have Centralized Management & Reporting Solution from Day 1 or The appliance should be manageable via HTTPS
GSLB.REQ.0021		It should have the capability of Rate shaping & QoS Support to optimize and handle heavy Layer 4 through 7 traffic loads while delivering Latency Sensitive Applications
GSLB.REQ.0022		Device should be accessed through the below or similar methods: • Using the CLI • Using SNMP • REST API • Using the Web Based Management
GSLB.REQ.0023	Warranty& Post warranty Support	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.18 SERVER LOAD BALANCER (SLB)

S.No.	Parameter	Minimum Specification
SLB.REQ.001	Traffic Ports support	8 x 25G SFP28 port and 2X40G QSFP+ ports . The appliance should have dedicated Out-of-band Management Port and Console Port
SLB.REQ.002	Device L4 Throughput	Device L7 Throughput: Minimum 40 Gbps and scalable up to 80 Gbps
SLB.REQ.003	Layer 4 Concurrent Connection	Concurrent Connections: 40 Million
SLB.REQ.004	Layer 4 connections per second	Appropriate Layer 4 connections per second in accordance to Layer 7 connection defined in this RFP to meet the desired performance parameter.
SLB.REQ.005	Layer 7 requests per second	At least 3 Million connections per sec
SLB.REQ.006	RAM & Harddisk	Device must be supplied with sufficient RAM to meet and sustain above performance parameters along with minimum 500 GB Hard disk capacity to store log up to minimum 2 months
SLB.REQ.007	SSL Throughput	The server load balancer should support minimum 40 Gbps of SSL throughput
SLB.REQ.008		Appliance must provide minimum SSL TPS of 50K with RSA 2K keys and 30K TPS with ECC ECDSA P-256. The proposed solution must have the capability to provide SSL offloading using both RSA and ECC based Keys
SLB.REQ.009	SSL offload capabilities	The Load Balancer shall support offloading of SSL connections
SLB.REQ.0010	Virtualization	The proposed device should have Hypervisor Based Virtualization feature(that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. Should be capable of virtualization and support minimum 4 and scalable up to 6 virtual instances each virtual instance having dedicated resources including hard disk, CPU, RAM, Operating system and SSL resources from day1
SLB.REQ.0011	Topology	Following Topologies or Equivalent should be supported: • Client Network Address Translation (Proxy IP)-InLine • Mapping Ports --- Aggregation • Direct Server Return----Asymmetric Topology • One Arm Topology Application ---Out of Path Mode • Direct Access Mode -Client and Server ITP preserve • Assigning Multiple IP Addresses---VLAN
SLB.REQ.0012	Network	Should support for IPv4 and IPv6 traffic along with full DNS functionality from day-1 and capable of record resolution for A and AAAA record.
SLB.REQ.0013		The solution should support link aggregation for bonding links to prevent network interfaces from becoming a single point of failure
SLB.REQ.0014		The proposed device should support standard VRRP for High Availability purpose or equivalent

S.No.	Parameter	Minimum Specification
SLB.REQ.0015		The Load Balancer Shall have full traffic control and be able to route requests to servers based on region, device, browser, etc. This enables organization to deliver customized application responses to users. Device must have Dynamic routing protocols like OSPF, RIP1, RIP2, BGP or equivalent from Day 1
SLB.REQ.0016	Matrices	The proposed appliance should support the below metrics or similar metrices: — Hash, — Weighted Hash, — Least Connections, — Least Connections Per Service, — Round-Robin, — Response Time, — Bandwidth, etc
SLB.REQ.0017	Application/ Others	The Proposed solution should have application delivery features such as Layer-7 load balancing, Layer-7 content switching, caching & compression, hardware based SSL offload and server side compression.
SLB.REQ.0018		It should have the capability of Rate shaping & QoS Support to optimize and handle heavy Layer 4 through 7 traffic loads while delivering Latency Sensitive Applications
SLB.REQ.0019		Device should be accessed through the below or similar methods: • Using the CLI • Using SNMP • REST API • Using the Web Based Management
SLB.REQ.0020	Warranty & Post warranty Support	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.19 BACKUP

5.20 PURPOSE BUILT BACKUP APPLIANCE (PBBA)

S. No.	Requirement	Minimum Specification
PBBA.REQ.001	General Features	Proposed PBBA VTL Appliances should be configured with minimum usable 1 PB front-end for overall capacity of appliance without de duplication & compression from Day 1. It should not restrict the number of servers, VMs, applications ,structured & unstructured data, database that can be backed up.
PBBA.REQ.002		Keeping in view required front end capacity and the backup policy explained in this RFP the vendor shall provide sufficient amount of usable capacity from Raw disk capacity for 5 years in the backup appliances from day one.
PBBA.REQ.003	Feature	PBBA VTL Appliance should be configured with RAID 6 or DDP or equivalent along with hot spare disks.
PBBA.REQ.004	Feature	As PBBA VTL Appliance soluiton should be expandable up to minimum usable 2 PB Front-end capacity from Day 1. The soluiton can be offered in a single box or 2 boxes max with single management console.
PBBA.REQ.005	Feature	Proposed PBBA VTL appliance shall come with all appropriate licenses of SW and HW for the proposed capacity. The proposed appliance should be offered with all required SW & HW to function as per requirement.
PBBA.REQ.006	Feature	Software Licensing:
PBBA.REQ.007	Feature	LAN/SAN Connection: Minimum 4 x 10/25 Gig SFP+ (fully populated) along with 4x16/32Gbps FC/FCOE ports with all required accessories.
PBBA.REQ.008	Feature	PBBA VTL appliance should have support for Encryption, Deduplication and Replication (Replication from appliances to appliances over TCP/IP network) from Day1.
PBBA.REQ.009	Feature	PBBA should have manual/Automated Data Integrity check for backup data on device
PBBA.REQ.0010	Feature	The proposed appliance should be able to deliver a throughput of up to 60 TB/hr (at target side) Or more, considering without deduplication and compression ratio. Deduplication and compression must be ensured at target/backup appliance end.
PBBA.REQ.0011	Feature	Scheduling:
PBBA.REQ.0012		b. Backup software used in PBBA should be able to retrieve data from tape to client server directly.
PBBA.REQ.0013		c. logs & reports e.g. de-duplication report, Data growth analysis report, Compute utilization report during backup etc.
PBBA.REQ.0014	Feature	PBBA based backup solution should support following replication capabilities:

S. No.	Requirement	Minimum Specification
PBBA.REQ.0015		a. Subsequent Replication should transfer only difference data from previous successful replication.
PBBA.REQ.0016		b. Replication should provide the flexibility to transfer only dedup data.
PBBA.REQ.0017		c. should provide compression of data while replication.
PBBA.REQ.0018		d. Proposed appliance should support bi-directional, many-to-one, one-to-many, and one-to-one replication.
PBBA.REQ.0019	Feature	PBBA VTL appliance should be provided with all features/capabilities available within it. Even If any new updates/version upgrade are released in PBBA after purchase during scope of the project, those should be provided without any additional cost.
PBBA.REQ.0020	Feature	Proposed disk appliance should be offered with battery backed up RAM / NVRAM for protection against data loss in power failure scenario and continuous automated file system check to ensure data integrity
PBBA.REQ.0021	Protection & retention	Proposed appliance should support retention lock/retention/ Immutability feature or any other to ensure that no data is deleted/overwritten accidently and support for point-intime copies of a LUN or volumes with minimal performance impact.
PBBA.REQ.0022	Updates and patch support	Software updates and patches: For the period of minimum 5 years.
PBBA.REQ.0023	Warranty& Post warranty Support	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.21 BACKUP SOFTWARE

S.No.	Minimum Specifications
BKPS.REQ.001	Backup software shall support GUI with centralized management / Single interface for management of all backup activities. The offered software shall support following application and database backup for PostgreSQL, 64-bit Active Directory, LDAP, Maria DB, MS SQL, Oracle, MySQL, nosql database like mongodb, casendra etc and nosql analytics database like drude and others. Version is a subjective thing and backup software should cover all latest versions & previous 3 versions along with all future version till the scope of work + 2 years
BKPS.REQ.002	The offered software shall support Advanced sharing of different media across the environment (disk, tape library and optical). The backup software should leverage the capabilities of PBBA (as specified in PBBA Specifications)
BKPS.REQ.003	The offered software shall support multiple level of backups including full, incremental, differential and synthetic full. (Synthetic full backup is a type of subsequent full backup that makes a comparison to the previously backed up data on the storage and uploads only the current changes from the backup source.) The proposed Backup Software should have in-built frequency (daily/weekly/monthly/etc.) and calendar-based scheduling system.
BKPS.REQ.004	The offered software shall support Disk-to-disk-to-tape (D2D2T) & Disk-to-tape (D2T) mechanism. It shall provide deduplication and compression technologies for backup efficiency.
BKPS.REQ.005	Proposed Front-end capacity based license shall include unlimited database license including PostgreSQL, 64-bit Active Directory, LDAP, Maria DB, MS SQL, Oracle, MySQL, nosql database like mongodb, casendra etc and nosql analytics database like drude and others 200 Host based licenses required having all databases including PostgreSQL, 64-bit Active Directory, LDAP, Maria DB, MS SQL, Oracle, MySQL, nosql database like mongodb, casendra etc and nosql analytics database like drude and others for which backup is required. Total capacity-based licenses (backup approx. 300 TB Front End Capacity). Backup Software should have the capability to provide back up to DR and NLDR as well and all the licenses to be in use and effective from day one Bidder shall include license as per capacity OR agent based on proposed software
BKPS.REQ.006	The proposed software shall have block level technology to store single copy collected from multiple repository. The proposed backup software should support the capability to write up to multiple data streams to single tape device or multiple tape devices in parallel from multiple clients to leverage the throughput of the drives using multiplexing technology

<table>
<tr><th>S.No.</th><th>Minimum Specifications</th></tr>
<tr><td>BKPS.REQ.007</td><td>The software shall be able to Compress and Encrypt data at the Client-side and this feature shall be available even during de-duplication.</td></tr>
<tr><td>BKPS.REQ.008</td><td>The offered software shall support AES256 Encryption algorithms from Day 1</td></tr>
<tr><td>BKPS.REQ.009</td><td>Backup software shall support multi tenancy feature for creation of distinct data zones.</td></tr>
<tr><td>BKPS.REQ.0010</td><td>The offered software shall be able to auto discover guest VMs, VMs with database instances and dynamically protect them with application consistent granular recovery for PostgreSQL, 64-bit Active Directory, LDAP, Maria DB, MS SQL, Oracle, MySQL, nosql database like mongodb, casendra etc and nosql analytics database like drude and others on windows & Linux, Unix. Also need table level recovery for above said databases.</td></tr>
<tr><td>BKPS.REQ.0011</td><td>The software should include or exclude specific files and directories from backup jobs.</td></tr>
<tr><td>BKPS.REQ.0012</td><td>The offered software shall support IPV4 and IPV6 addressing system.</td></tr>
<tr><td>BKPS.REQ.0013</td><td>The offered software shall have inbuilt capability to do trend analysis for capacity planning of backup environment.

Backup software should provide inbuilt dashboard for reporting such as data deduplication report, CPU utilization report, Job Report, Session Detail Report, Application Trending and Media Assure Report and other capabilities for capacity planning of backup environment.</td></tr>
<tr><td>BKPS.REQ.0014</td><td>The offered software shall support heterogeneous media server agent failover.</td></tr>
<tr><td>BKPS.REQ.0015</td><td>The proposed software shall support file archival for based on age or quota with seamless access on multiplatform (Windows, Linux and Unix).</td></tr>
<tr><td>BKPS.REQ.0016</td><td>The proposed software shall have inbuilt capability to protect the backed up disk volume from malware.</td></tr>
<tr><td>BKPS.REQ.0017</td><td>Proposed backup software shall have inbuilt capability to protect the backed up volume from Ransom ware.</td></tr>
<tr><td>BKPS.REQ.0018</td><td>The proposed backup software should support both backups using snapshot/hardware based and software based as well as backup to tapes for long term and offline data retention.</td></tr>
<tr><td>BKPS.REQ.0019</td><td>Proposed backup software should be capable to take backups directly on Tapes without any disk staging. The proposed backup solution should allow creating tape clone facility</td></tr>
<tr><td>BKPS.REQ.0020</td><td>The Proposed solution should be support to Identification, Classification and Protection of Structured Data allowing the appropriate level of privacy controls using data masking and supports Format Preserving Encryption (FE)/ Standard AES 256 bit encryption at the application/DB level which should be applied in place or archive according to its sensitivity and usage needs.</td></tr>
<tr><td>BKPS.REQ.0021</td><td>5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support</td></tr>
<tr><td>BKPS.REQ.0022</td><td>Proposed backup and retention policy:
<table>
<tr><th>Backup Type</th><th>Frequency</th><th>Retention</th></tr>
<tr><td>Full Backup</td><td>Day 0</td><td>1 year</td></tr>
<tr><td>Differential/Incremental</td><td>Daily End of Day</td><td>1 Months</td></tr>
<tr><td>Weekly Full</td><td>At the end of 1 week</td><td>1 Months</td></tr>
<tr><td>Monthly Full</td><td>At the end of 1 Month</td><td>1 Years</td></tr>
<tr><td>Yearly Full</td><td>At the end of 1 Year</td><td>3 Years</td></tr>
</table></td></tr>
</table>

S.No.	Minimum Specifications
BKPS.REQ.0023	This capacity based license shall be based on one time full actual backup size i.e. front end data backup capacity.
BKPS.REQ.0024	Capacity based license shall include all features of backup software such as agent based backup (DB and file system), image backup, NDMP backup etc.
BKPS.REQ.0025	Capacity based license shall include feature for secondary backup location also for Tape out, object storage and replication.
BKPS.REQ.0026	GUI: The Software should have web based Graphical User Interface (GUI) so that all backup can be managed centrally, regardless of location. GUI should be same across heterogeneous platform to ensure easy administration.
BKPS.REQ.0027	Recovery: Software must maintain a database for all backup jobs, policy jobs meta-data etc., and should have the capability of re-creating master system in case of disaster using this database.
BKPS.REQ.0028	The proposed backup solution should be able to perform cross platform instant virtual machine Recovery and File System recovery.
BKPS.REQ.0029	DB Backup: Should provide online backup for PostgreSQL, 64-bit Active Directory, LDAP, Maria DB, MS SQL, Oracle, MySQL, nosql database like mongodb, casendra etc and nosql analytics database like drude and others on windows & Linux, Unix.
BKPS.REQ.0030	De-duplication: The PBBA should support target based de-duplication along with source base de-duplication for improved backup window and lesser footprint.
BKPS.REQ.0031	Ability to configure automated backups for specific days and weeks within a month, while maintaining a simplified methodology for complex date scenarios.
BKPS.REQ.0032	PBBA based backup solution should provide policy based system for backup scheduling i.e. clients with same data to be backed up may be added or removed from policy when required.
BKPS.REQ.0033	PBBA based backup solution should provide sets creation for backup selection, schedule, target backup device such that when this set is modified its impact should be visible to all jobs/policies using that particular set.
BKPS.REQ.0034	PBBA based backup solution should provide flexibility to backup data in multiple streams for lesser backup window.
BKPS.REQ.0035	PBBA based backup solution Should have following TAPEOUT capabilities: Should have capability to transfer all data that is backed up on disk to tape without client server intervention.
BKPS.REQ.0036	Backup software used in PBBA should be able to retrieve data from tape to client server directly.
BKPS.REQ.0037	The proposed backup software should have provision of replication/recovery of Backup server in case of any failure/disaster without affecting any related service.
BKPS.REQ.0038	The PBBA based backup solution should have following reporting capabilities: a. Full job completion report. Overview of the full backup jobs that were successful, partially successful and failed for each day.
BKPS.REQ.0039	b. Full backup data volume report. Overview of the total data volumes that were backed up for each day.
BKPS.REQ.0040	c. logs & reports e.g. de-duplication report, Data growth analysis report, Compute utilization report during backup etc.
BKPS.REQ.0041	PBBA based backup solution should have following capabilities for image level backup:a. Should support image level backup on host/hypervisor level for multiple vendors like Hyper-V, Vmware etc.
BKPS.REQ.0042	b. Should support source based deduplication while image level backup.
BKPS.REQ.0043	c. Should support granular recovery from image level backup.

S.No.	Minimum Specifications
BKPS.REQ.0044	d. Software should provide instant recovery of image level backup.
BKPS.REQ.0045	Backup software should support always incremental policy for all kinds of backup (agent based file system and DB backup, image based backup).
BKPS.REQ.0046	Proposed backup software should support direct access of VM files/images of different virtualization vendors from backup storage.
BKPS.REQ.0047	The backup software should be able to encrypt the backed up data using 256-bit AES encryption on the backup client and should not demand for additional license, any such license if needed should be quoted for the total number of backup clients asked for.
BKPS.REQ.0048	The backup solution should also support online LAN Free SAN based backups of databases through appropriate agents; Important Applications being PostgreSQL, 64-bit Active Directory, LDAP, Maria DB, MS SQL, Oracle, MySQL, nosql database like mongodb, casendra etc and nosql analytics database like drude and others
BKPS.REQ.0049	Should able to dynamically break up large save sets into smaller save sets to be backed up in parallel to allow backups to complete faster for Windows, Unix and Linux clients.
BKPS.REQ.0050	Should have in-built calendar based scheduling system and also support check-point restart able backups for file systems. It should support various level of backups including full, incremental, differential backups
BKPS.REQ.0051	The proposed backup software should have the capability to enable overwrite protection on the backup sets from the backup software console on proposed disk backup appliance to protect accidental overwriting of earlier backups.
BKPS.REQ.0052	The solution must support client-direct backup feature for file system, applications and databases to reduce extra hop for backup data at backup/media server to cater stringent backup window.
BKPS.REQ.0053	Backup software must support Robotic/automated Tape library, the licensing of such library should be on the unlimited number of slots and not on the drive counts as additional drives are added to improve performance. Must support OST, VTL, NFS. CIFS for proposed backup disk appliance
BKPS.REQ.0054	Must support source capacity based licensing and host based licensing as well.
BKPS.REQ.0055	Backup Solution must support multi tenancy feature for creation of distinct data zones where the end users have access without being able to view data, backups, recoveries, or modify in other data zones.
BKPS.REQ.0056	Backup Solution should also have configurable ReST API/API support for management, administration and reporting on backup infrastructure.
BKPS.REQ.0057	The proposed solution should have inbuilt feature for extensive alerting and reporting with pre-configured and customizable formats. The proposed solution must have capability to do trend analysis for capacity planning of backup environment not limiting to Backup Application/Clients, Virtual Environment, Replication etc.
BKPS.REQ.0058	The proposed backup software should be able to recreate backed up data from existing volumes from metadata backups. The solution should offer recovery of specific volumes for recovery from metadata in case of a disaster recovery.
BKPS.REQ.0059	The proposed backup solution should provide capability for a single file restore from complete backup store
BKPS.REQ.0060	The solution should be capable of integration with active directory/ldap infrastructure for ease of user rights management along with role based access control to regulate the level of management
BKPS.REQ.0061	The solution should have the capability to manage and monitor backups at remote

S.No.	Minimum Specifications
	locations from a single backup server, where clients can backup data to a local disk backup device without the need of local media server or sending primary backup copy over the WAN
BKPS.REQ.0062	The solution should have the capabilities to backup as well as archive data to cloud with other cloud service providers.
BKPS.REQ.0063	Backup software should have capability to sync the backups from one PBBA to other PBBA at a remote location over any TCP/IP network.
BKPS.REQ.0064	Software updates and patches: For the period of minimum 5 + 2 years.
BKPS.REQ.0065	Requisite Hardware and software to install and commission backup software in HA and Failover mode must be supplied from day 1. All required software licenses should be PERPETUAL in nature and should have NO dependency on underlying hardware with 5 years On-site comprehensive Annual Technical Support from respective OEM

5.22 TAPE LIBRARY

S.No.		Minimum Specifications
TL.REQ.001	Technical	The Tape Library unit shall be configured with 6 x LTO Gen-9 FC Tape Drives and minimum of 60 Cartridge slots or more
TL.REQ.002	Scalability	Offered tape library shall be scalable to 12 x LTO9 FC Tape drive. Drive scalability to be met by only adding Tape drive and expansion units and shall be scalable up to 280 data cartridges slots or more (Further to be scaled on demand)
TL.REQ.003	Technical	Tape Library should support six backup jobs simultaneously in day one
TL.REQ.004	Media	100 x LTO-9 Media cartridge with bar code with labels, 6 x cleaning cartridge.
TL.REQ.005		Offered Tape drive should be proposed with FC interface.
TL.REQ.006	Technical	Offered LTO-9 drive in the library shall conform to the Data rate matching technique for higher reliability.
TL.REQ.007	Security	Offered LTO-9 drive in the library shall offer WORM support and embedded AES 256 bit encryption.
TL.REQ.008	Security	Offered Library shall be provided with a hardware device /appliance, etc. to keep all the encrypted keys in Physical/ Virtual appliance in redundant fashion to Manage & keep Encryption keys
TL.REQ.009	Performance	Offered each LTO-9 drive shall have native speed of 400 MB per Sec or more
TL.REQ.0010	Technical	Offered tape Library shall have partitioning support and shall have flexibility to have separate partition for each offered drive. Vendor shall offer the required license for partition.
TL.REQ.0011	Technical	Tape Library shall provide native Fiber connectivity to SAN Environment.
TL.REQ.0012	Functional	For optimal Performance. Tape Library shall provide native 8/16/32 Gbps FC interface connectivity to SAN switches.
TL.REQ.0013	Technical	Tape library shall support removable magazine and mail slot.
TL.REQ.0014	Technical	Tape Library shall be offered with at-least 5 mail slots and shall be scalable to at-least 30 mail slots.
TL.REQ.0015	Technical	Tape Library shall have GUI Front panel.
TL.REQ.0016	Functional	Tape Library shall have option for redundant power supply.
TL.REQ.0017	Functional	Offered tape Library must support both data and control path failover for the offered drives.
TL.REQ.0018	Technical	Tape Library shall be supplied with software which can predict and prevent failures through early warning and shall also suggest the required service action.
TL.REQ.0019	Functional	Offered Software shall also have the capability to determine when to retire the tape cartridges and what compression ratio is being achieved.
TL.REQ.0020	Functional	Tape Library shall provide web based remote monitoring capability
TL.REQ.0021	Warranty	5 Years i.e. 24x7x365 days including holidays
TL.REQ.0022	Technical	Should be offered with Control Path and Data Path Failover
TL.REQ.0023	Management & Monitoring	Tape library management software should support advanced reporting and management features
TL.REQ.0024	Cables for connectivity	Required cables and installation should be provided as per the proposed solution
TL.REQ.0025	Warranty & Post warranty	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

S.No.		Minimum Specifications
	Support	

5.23 CYBER SECURITY

5.24 WEB APPLICATION FIREWALL (WAF)

S.No.	Parameter	Minimum Specifications
WAF.REQ.001	Traffic Ports	The Appliance should have minimum dedicated 8 x 10G SFP+ ports and 2X40G QSFP+ all pre-populated from day 1 and out of band management port with Dual Hot Swappable power supply from day one
WAF.REQ.002	Appliance based	The appliance should be dedicated appliance and from different vendor than firewall and NGFW
WAF.REQ.003	Certification	The proposed WAF should be ICSA/ EAL/ NDPP/NSS Lab certified
WAF.REQ.004	OWASP Top 10 attacks Protection	WAF should protect against OWASP top 10 vulnerabilities.
WAF.REQ.005	SQL Injection Protection	SQL Injection should be protected by WAF
WAF.REQ.006	Cross-Site Scripting (XSS) protection	The WAF should prevent XSS cross-site attacks
WAF.REQ.007	Throughput	WAF should provide at least 8 Gbps of WAF throughput /45 Gbps of SSL throughput from day 1 and it should not degrade after enabling Access logs, Web firewall logs and enabling security policies. WAF latency should be less than 30 milliseconds.
WAF.REQ.008	Support of JSON	XML/ JSON support
WAF.REQ.009	Request per sec	WAF should support at-least 3 Million L7 request Per Second
WAF.REQ.0010	Signature Updates	Should support automatic signature updates to protect against known and potential application security threats.
WAF.REQ.0011	Logging & Reporting	i)Ability to identify and notify system faults and loss of performance II) Should support Log Aggregation lll)Should support multiple log formats such as CSV, Syslog, TXT, etc. IV) Should support inbuilt Reporting and sending the report via E-Mail V) Should support report formats in PDF, HTML, WORD, RTF, etc.. VI) Reports should be customizable. VII) Report Distribution Automatically via email VIII) Web application firewall should support centralized management and reporting for multiple appliances IX) ALL Logs must have compliance to separate Log Server/SIEM solutions as per standard norms and this appliance must be capable to retain/store 2 months log. X) It shall support to generate reports like pie-chart, bar-chart based on user defined security compliance baseline- XI) should support authentication, authorization and accounting (AAA) integration with external authentication support providers such as Active Directory, RADIUS/TACACS+

S.No.	Parameter	Minimum Specifications
WAF.REQ.0012	HA Deployment	The WAF should support HA deployment (Active/Active or Active/Passive)
WAF.REQ.0013	Modes	The appliance should be able to perform in multiple modes such as Active mode, passive mode, Transparent mode, proxy mode,
WAF.REQ.0014	HTTP Version	Must support multiple HTTP versions such as HTTP/1.0, HTTP1.1 & HTTP 2.0.
WAF.REQ.0015	IPV4/IPV6	WAF should respectively support working modes based on IPv4 and IPv6 environments, and be able to support IPv4 and IPv6 dual-stack
WAF.REQ.0016	BOT attack	should provide protection against BOT attack from day1.
WAF.REQ.0017	Policy	The WAF solution must support Security Policy to be applied per application, rather than one single policy for an entire system.
WAF.REQ.0018	Brute Force protection	Should have controls against Brute force attacks
WAF.REQ.0019	Buffer over flow attack protection	System must support protection from buffer overflow
WAF.REQ.0020	Auto-Learn	Should have the capability to Auto-Learn Security Profiles required to protect the infrastructure.
WAF.REQ.0021	Virtualization	WAF should have Virtualization feature that virtualizes the device resources – including CPU, memory, network, operating system and acceleration resources and should support minimum 4 virtual instances from day 1.
WAF.REQ.0022	Hiding Sensitive Content Parameters:	It should be able to Mask values of sensitive parameters (for example, passwords, credit card and social security details, Aadhaar no.)
WAF.REQ.0023	RSA KEY	Appliance must provide minimum SSL TPS of 50K with RSA 2K keys and 30K TPS with ECC ECDSA P-256 The proposed solution must have the capability to provide SSL offloading using both RSA and ECC based keys
WAF.REQ.0024	Web Anti-Defacement (WAD) function	The WAF should support Web Anti-Defacement (WAD) function to detect and prevent the defaced web pages from being returned to the client.
WAF.REQ.0025	Management	Should provide GUI Management User Interface
WAF.REQ.0026		The solution must provide Role-Based Access Control or multiple user roles that facilitate separation of duties.
WAF.REQ.0027		The solution must allow the user to use a standard browser to access the management UI.
WAF.REQ.0028	Warranty & Post warranty Support	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support
WAF.REQ.0029		POC

5.25 ADVANCED PERSISTENCE THREAT - ANTI APT

S.No.	Parameter	Minimum Specifications
APT.REQ.001	Security Features	The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance.
APT.REQ.002		The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections, VBS, WMI and Malware families etc. through a dashboard
APT.REQ.003		The proposed solution must be able to provide intelligence feed for malware information, threat profile and containment remediation recommendations wherever applicable.
APT.REQ.004		Should have Advanced Threat Scan Engine to detect zero-day threats, embedded exploit code, rules for known vulnerabilities and enhanced parsers/ other utility handling file deformities/ sanity
APT.REQ.005		The proposed solution should have a built-in/ external document vulnerabilities detection capabilities and also support external vulnerability detection to assure analysis precision and analysis efficiency
APT.REQ.006		The proposed solution should be able to store packet captures (PCAP) of all malicious communications detected by sandbox.
APT.REQ.007		Solution should be deployed on premise along with on premise sandboxing capability and no data should be allowed to go on public cloud.
APT.REQ.008		Solution must be on premise dedicated Anti APT solution and should avoid single point of failure adhering NCIIPC, Cert-In, NIST and DSCI guidelines. The APT solution should be able to integrate with the Proposed NGFW for automatic blocking / threat update..
APT.REQ.009		Should performs static and dynamic analysis to identify an object's notable characteristics: AutoStart or other system configuration, Anti-security and self-preservation,, File drop, download, , or replication, redirection, or data theft, Malformed, or with known malware traits, Process, service, or memory object change and Rootkit, Suspicious network or messaging activity
APT.REQ.0010		Should have extensive detection techniques utilize file, web, IP, mobile application reputation/ data coming from mobile apps of the hosted applications in Data Center, heuristic analysis, advanced threat scanning, pre-defined/custom sandbox analysis, and correlated threat intelligence to detect ransomware, zero-day exploits, advanced malware, and attacker behaviour.
APT.REQ.0011		Should detect from Targeted attacks and advanced threats, Targeted and known ransomware attacks, Zero-day malware and document exploits, Attacker behaviour and network activity, Web threats, including exploits and drive-by downloads, Phishing, spear phishing, and other email threats, Data exfiltration, Bots, Trojans, worms, key loggers and Disruptive applications

S.No.	Parameter	Minimum Specifications
APT.REQ.0012		The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behaviour, Lateral Moment, Asset and data discovery and data Exfiltration.
APT.REQ.0013		Proposed solution should be able to provide customizable/Pre-defined sandbox and network based threat detection solution to match customer's endpoint environments. Access different information about Affected Hosts on the following views: Displays a summary of affected hosts by attack phase, provides access to Host Details views and Displays host event details in chronological order
APT.REQ.0014	**Deployment Mode**	The Proposed solution should support In- line deploymentmode supporting SSL/TLS decryption along with monitorInter-VLAN traffic on a Port Mirror Session/TAP mode. Should also support with tight integration with SSL Offloader/Internal Firewall.
APT.REQ.0015		Integration with major 3rd party security OEMs.
APT.REQ.0016	**Extensive File support**	Should support common file formats including but not limited to executables, JAVA, PDF, MS Office documents/ open source office documents, common multimedia contents such as JPEG/GIF/BMP/WMF and ZIP/RAR/7ZIP/TNEF archives Should support extensive File Types i.e. Compressed Files (7z, rar, zip, cab, jar, gz, tar, bz2), Script Based (bat, ps1, vbs, js), Executables (exe, dll, scr) and Office Documents / PDF (doc / docx, ppt / pptx, xls / xlsx, pdf, mdb), .bat, .cmd, .cell, .chm, .csv, .class, .cla, .dll, .ocx, .drv, .doc, .dot, .docx, .dotx, .docm, .dotm, .cpl, .exe, .sys, .crt, .scr, .gul, .hta, .htm, .html, .hwp, .hwpx, .iqy, .jar, .js, .jse, .jtd, .lnk, .mov, .pdf, .ppt, .pps, .pptx, .ppsx, .psl, .pub, .rtf, .slk, .svg, .swf, .vbe, .vbs, .wsf, .xls, .xla, .xlt, .xlm, .xlsx, .xlsb, .xltx, .xlsm, .xlam, .xltm, .xml, .xht, .xhtml, .url and other major file formats/ extensions
APT.REQ.0017	**Traffic Inspection**	Should monitors all inbound and outbound network traffic and should allow administrator to categorize files as safe based on Hash values (MD5, SHA 256, SHA 512 etc.) also should scan files and URL web reputation.
APT.REQ.0018	**Performance**	Proposed solution should support minimum 28000 samples/day processing capacity also should able to run at least 20 parallel sandboxes images scalable up to 50 for analysis of payload
APT.REQ.0019		Proposed solution should support at-least 4 Gbps of aggregated inspection throughput using single appliances by intercepting traffic of different segments
APT.REQ.0020		Proposed solution should have sufficient storage in RAID 1 from day one in order to meet the desired scope and increase the required storage during O&M phase if needed without any additional cost
APT.REQ.0021	**Sandbox**	Pre-defined/Custom Sandbox: Domain Check, Software Check, User Settings check, Requisite file check Office version check, Windows License check Browser Check (Sandbox pre-defined/ Customized with OS and Applications in the Environment)
APT.REQ.0022		Should support pre-defined/ customized sandbox solution handling files from Windows servers (Win 10, Win 11,

S.No.	Parameter	Minimum Specifications
		Windows Server 2012, 2016, 2019, 2022 or higher) and Linux servers
APT.REQ.0023		The proposed solution should provide visibility into scan histories of each file scanned that are aborted, completed, or in progress.
APT.REQ.0024		The solution should provide reports in (but not limited to) PDF/CSV formats.
APT.REQ.0025	**Warranty & Post warranty Support**	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.26 NETWORK INTRUSION PREVENTION SYSTEM (NIPS)

S.No.		Minimum Specifications
NIPS.REQ.001	**System Performance**	Solution should have 20 Gbps of real-world throughput with scalability up to 40 Gbps on same appliance (i.e Appliance may be either single appliance or stacking multiple appliance supporting upto 40 Gbps throughput) from day1 supporting scalable architecture
NIPS.REQ.002		Should have 8 million legitimate concurrent Sessions/Concurrent connections scalable up to 15 million and 300,000 new Connections per second from day one which should scalable up to 650000 new Connections per second.
NIPS.REQ.003		Should introduce minimum latency <40 microseconds or as required to maintain the throughput and features defined in the specifications. Also should have inbuilt SSL decryption capability.
NIPS.REQ.004		Should be a standalone dedicated NIPS appliance and should not be from NGFW, Routing, switching based vendor to avoid single point of failure adhering NCIIPC, Cert-In, NIST and DSCI guidelines.
NIPS.REQ.005	**Security Feature**	Should support industry leading VA scanners integration to fine tune the IPS policy to shield vulnerabilities automatically by leveraging virtual patching functionality or equivalent.
NIPS.REQ.006		Should supports inspection of Asymmetric traffic consisting jumbo frames, DGA defence filters, Machine learning, Virtual patching capability or equivalent capability.
NIPS.REQ.007		Should support Layer 2/ Layer 1 Fallback option to bypass traffic even with the power on, in event of un-recoverable internal software error such as firmware corruption and memory errors etc.
NIPS.REQ.008		Should support 'VLAN Translation' feature which allows IPS to be deployed on a stick (out of line) but still protect all Inter-VLAN traffic in the same way as in-line deployment
NIPS.REQ.009		Should protect all Inter-VLAN traffic in the same way as in-line deployment.
NIPS.REQ.0010		Should be based on purpose-built platform that has On-board L2 Switch and dual plane architecture for Data and control plane and NIPS should be independent standalone solution
NIPS.REQ.0011	**Threat Intelligence**	Should have Vulnerability based filters/ rules/ signatures covering entire Vulnerability footprint, which understands various exploit patterns.
NIPS.REQ.0012		Support firmware, signature upgrade/Reboot without require downtime
NIPS.REQ.0013		Should have the capability to manage and convert other vendor's signature(such as snort)
NIPS.REQ.0014		Should have machine learning to detect exploit kit landing page.
NIPS.REQ.0015		Should bypass traffic for IPS internal issues i.e. memory hang, firmware crash etc.
NIPS.REQ.0016		Should provide bandwidth rate limit to control the unwanted traffic such as P2P, Online Game, etc.

S.No.		Minimum Specifications
NIPS.REQ.0017		Should have at least inbuilt 14000 + signatures/Filters pertaining to security and applications apart from user define signatures/filters
NIPS.REQ.0018		Should have a power failure bypass modular that can support hot swappable function which allows traffic to bypass even after a modular get unplugged out of IPS Box during the RMA procedure
NIPS.REQ.0019		Solution must alert effective and ineffective filter in case of noisy filters
NIPS.REQ.0020		The proposed management system shall support 'threat insights' dashboard that show correlated data such as how many breached host, how many IOC data, 3rd party VA scan integration data and how many pre-disclosed vulnerability discovered
NIPS.REQ.0021		Should support SPAN/TAP and Inline and passive mode deployment
NIPS.REQ.0022		Should be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploit type and the reputation score
NIPS.REQ.0023		Should have inbuilt fail-open and fail-close capability for all ports
NIPS.REQ.0024		Should support out-of-the-box configuration that will protect the network straight from the initial deployment
NIPS.REQ.0025		Performance/throughput should not be altered/degraded by enabling all the features/licenses
NIPS.REQ.0026		Should have dual plane architecture for Data and Control plane having its local /centralized management to configure policies and reporting
NIPS.REQ.0027		Should support zero power interface cards to allow traffic flow without inspection in case of appliance power failure
NIPS.REQ.0028		The proposed management system shall also be able to provide a customized 'At-a-glance-Dashboard' to provide overall status of the network traffic and attack going through
NIPS.REQ.0029		Should support SNMP and a private MIB that can be utilized from an Enterprise Management Application
NIPS.REQ.0030		The central management server should serve as a central point for security policies management including versioning, rollback, import and export (backup) tasks
NIPS.REQ.0031		The management server must provide rich reporting capabilities include customizable report for All attacks, Specific & Top N attack, Source, Destination, Misuse and Abuse report, Rate limiting report, Traffic Threshold report, Device Traffic Statistics and Advance DDoS report
NIPS.REQ.0032		Solution should provide feedback based on existing vulnerabilities, exploits and suspicious network traffic and tuning IPS sensor (E.g. Selecting rules, configuring policies, updating policies, etc...)
NIPS.REQ.0033		Solution should provide support in removing assigned rules if a vulnerability or software no longer exists
NIPS.REQ.0034		The management server must support the archiving and backup of events and exports through various protocols and storage devices. Solution must allow the report to be exported into other format such as PDF, HTML, CSV, XML

S.No.		Minimum Specifications
		etc.
NIPS.REQ.0035		Should be able to manage locally independently
NIPS.REQ.0036	**Global Certification**	The OEM must have been evaluated and recommended by latest/ last available report of NSS labs/ Common Criteria/ICSA/EAL4/NDPP for the proposed solution
NIPS.REQ.0037	**Health Check**	The NGIPS shall achieve the following industry recognized security certification standards: 1. FIPS 140-2 or equivalent 2. IPv6
NIPS.REQ.0038		Solution should protect against advance malwares and should offer URL filtering/Web Reputation intelligence or equivalent capability from day 1.
NIPS.REQ.0039	**Warranty & Post warranty Support**	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.27 HOST INTRUSION PREVENTION SYSTEM (HIPS)

S.No.	Parameter	Minimum Specifications
HIPS.REQ.001	**Security Modules**	Proposed solution should support modules including Antimalware, HIPS, Firewall, Application control, File Integrity Monitoring, Log correlation, C&C/ C2 prevention must be available in single agent
HIPS.REQ.002	**Supported OS Platforms**	The proposed server security solution must support multiple platforms of server operating systems i.e. Windows, Linux RedHat, CentOS, Oracle, Debian, SUSE,Ubuntu, AIX, Amazon Linux etc.
HIPS.REQ.003		The Proposed solution must support Anti-malware, HIPS, Integrity Monitoring, Host Firewall for the below mentioned server operating system:
HIPS.REQ.004		Microsoft Windows Server (2008 &2008 R2, 2012 & 2012 R2, 2016,2019), Red Hat Enterprise Linux (6,7,8), Solaris (10.0,11.0,11.1,11.2,11.3,11.4), Oracle Linux (6,7,8), AIX (6.1,7.1,7.2), CentOS (6,7,8) and Suse Linux (11,12,15)
HIPS.REQ.005	**Firewall Security Feature**	The firewall shall be bidirectional for controlling both inbound and outbound traffic and should have the capability to define different rules to different network interfaces
HIPS.REQ.006		Firewall rules should filter traffic based on source and destination IP address, port, MAC address, direction etc. and should detect reconnaissance activities such as port scans and should support state full inspection functionality
HIPS.REQ.007		Solution should provide policy inheritance exception capabilities and ability to lock computer (prevent all communication) except with management server.
HIPS.REQ.008		Solution should have ability to run internal port scan on individual servers to know the open ports and will help administrator create rules.
HIPS.REQ.009		The firewall should be able to detect protocol violations of standard protocols and provision inclusion of packet data on event trigger for forensic purposes.
HIPS.REQ.0010		Solution should have security profiles that allows firewall rules to be configured for groups of systems, or individual systems.
HIPS.REQ.0011	**HIPS Security Features**	The proposed solution should support Deep Packet Inspection (HIPS/IDS) and should support creation of customized DPI rules if required.
HIPS.REQ.0012		Deep Packet Inspection should have feature of zero day protection for both known and unknown vulnerabilities until the next scheduled maintenance window.
HIPS.REQ.0013		The solution should be a high- performance HIPS engine to intelligently examine the content of network traffic entering and leaving hosts.
HIPS.REQ.0014		Deep packet Inspection should protect operating systems, commercial off-the-shelf applications, and custom web applications against attacks such as SQL injections and cross-site scripting.
HIPS.REQ.0015		Solution should facilitate and provide ability for recommendations against existing vulnerabilities, exploits, suspicious network traffic and dynamically tuning IDS/IPS sensor (E.g. Selecting rules, configuring policies, updating

S.No.	Parameter	Minimum Specifications
		policies, etc.)
HIPS.REQ.0016		Solution should facilitate/ provide recommendation for removing of assigned rules if a vulnerability or software no longer exists - E.g. If a patch is deployed or software is uninstalled corresponding signatures are no longer required
HIPS.REQ.0017		The solution should allow imposing HTTP Header length restrictions and have the capability to inspect and block attacks that happen over SSL.
HIPS.REQ.0018		The solution should allow or block resources that are allowed to be transmitted over http or https connections and capable of blocking and detecting of IPv6 attacks.
HIPS.REQ.0019		Detailed events data to provide valuable information, including the source of the attack, the time and what the potential intruder was attempting to exploit, shall be logged.
HIPS.REQ.0020		Solution should offer protection for virtual, physical, cloud and docker container environments.
HIPS.REQ.0021		Deep Packet Inspection should have Exploit rules which are used to protect against specific attack variants providing customers with the benefit of not only blocking the attack but letting security personnel know exactly which variant the attacker used (useful for measuring time to exploit of new vulnerabilities).
HIPS.REQ.0022		Deep Packet Inspection should have pre-built rules to provide broad protection and low-level insight, for servers. For operating systems and applications, the rules limit variations of traffic, limiting the ability of attackers to exploit possible attack vectors. Generic rules are also used to protect web applications (commercial and custom) from attack by shielding web application vulnerabilities such as SQL Injection and Cross-Site Scripting.
HIPS.REQ.0023		Solution should work in Tap/detect only mode and prevent mode and support automatic and manual tagging of events also have CVE cross referencing when applicable for vulnerabilities.
HIPS.REQ.0024		Solution should provision inclusion of packet data on event trigger for forensic purposes and shall protect against fragmented attacks also should allow to block based on thresholds
HIPS.REQ.0025		Deep packet inspection should have signatures to control based on application traffic. These rules provide increased visibility into & control over the applications that are accessing the network. These rules will be used to identify malicious software accessing the network.
HIPS.REQ.0026		Solution should have Security Profiles which allows DPI rules to be configured for groups of systems, or individual systems. For example, all Linux/Windows servers use the same base security profile allowing further fine tuning if required. Solution to have capability to suggest rules (user defined or automatic) based on Server Posture and alerts for de-provisioning of rules, if the vulnerability no longer exists.
HIPS.REQ.0027	**Integrity Monitoring Security**	Integrity Monitoring module should be capable of monitoring critical operating system and application elements files, directories, registry keys to detect suspicious

S.No.	Parameter	Minimum Specifications
	Features	behaviour, such as modifications, or changes in ownership or permissions.
HIPS.REQ.0028		The solution should be able to monitor System Services, Installed Programs and Running Processes for any changes also extensive file property checking whereby files and directories are monitored for changes to contents or attributes (ownership, permissions, size, etc.).
HIPS.REQ.0029		Solution should be able to track addition, modification, or deletion of Windows registry keys and values, access control lists, or web site files are further examples of what can be monitored.
HIPS.REQ.0030		Solution should support any pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, etc.) and support custom rules as well.
HIPS.REQ.0031		Solution should have automated recommendation of integrity rules to be applied as per Server OS and can be scheduled for assignment/assignment when not required.
HIPS.REQ.0032		Solution should have by default rules acting at Indicators of Attacks detecting suspicious/malicious activities.
HIPS.REQ.0033		In the Event of unauthorized file change, the proposed solution shall report reason, who made the change, how they made it and precisely when they did so.
HIPS.REQ.0034		Solution should have Security Profiles which allows Integrity Monitoring rules to be configured for groups of systems, or individual systems. For example, all Linux/Windows servers use the same base security profile allowing further fine tuning if required.
HIPS.REQ.0035		Solution should have an intuitive rule creation and modification interface includes the ability to include or exclude files using wildcards filenames, control over inspection of sub-directories, and other features.
HIPS.REQ.0036		Solution should support the following: Multiple groups of hosts with identical parameters, Regex or similar rules to define what to monitor, Ability to apply a host template based on a regex of the hostname, Ability to exclude some monitoring parameters if they are not required, Ability to generate E Mail and SNMP alerts in case of any changes, Solution should support creation of custom Integrity monitoring rule and Solution should provide an option for real time or scheduled Integrity monitoring based on operating system.
HIPS.REQ.0037	**Anti-Malware Security Features**	Anti-malware should support Real Time, Manual and Schedule scan and should have flexibility to configure different real time and schedule scan times for different servers and should have feature to try & backup ransomware encrypted files and restoring the same as well.
HIPS.REQ.0038		Solution should support excluding certain file, directories, file extensions from scanning (real time/schedule) and use a combination of cloud-based threat intelligence combined with traditional endpoint security technologies.
HIPS.REQ.0039		Solution should support True File Type Detection, File extension checking and have heuristic technology blocking files containing real-time compressed executable code.

S.No.	Parameter	Minimum Specifications
HIPS.REQ.0040		The proposed solution should be able to detect and prevent the advanced threats which come through executable files, PDF files, Flash files, RTF files and and/or other objects using Machine learning
HIPS.REQ.0041		The proposed solution should be able to perform behaviour analysis for advanced threat prevention and have its own threat intelligence portal for further investigation, understanding and remediation an attack.
HIPS.REQ.0042		Solution deployment should cause limited interruption to the current network environment also should have Ransomware Protection in Behaviour Monitoring.
HIPS.REQ.0043		Solution should have Highly Accurate machine learning - Pre-execution and Run time analysis, document exploit prevention to address known/Unknown threats.
HIPS.REQ.0044	**Log Analysis functional Features**	Solution should have a Log Inspection module/ equivalent log inspection features which provides the ability to collect and analyse operating system, databases and applications logs for security events.
HIPS.REQ.0045		Solution must recommend rules for threat log analysis as per the Server OS and support assignment/unassigment of rules where ever required.
HIPS.REQ.0046		Solution should have Security Profiles/Policies allowing Log Inspection rules to be configured for groups of systems, or individual systems. E.g. all Linux/Windows servers use the same base security profile allowing further fine tuning if required.
HIPS.REQ.0047		Solution should have ability to forward events to an SIEM system or centralized logging server for eventual correlation, reporting and archiving also should allow setting of severity levels to reduce unwanted event triggering.
HIPS.REQ.0048		Customized rule creation should support pattern matching like Regular Expressions or simpler String Patterns. The rule will be triggered on a match also ability to set dependency on another rule will cause the first rule to only log an event if the dependent rule specified also triggers.
HIPS.REQ.0049	**Application Control Functional Features**	Solution should allow administrators to control what has changed on the server compared to initial state and should prevent unknown and uncategorized applications from running on critical servers also must support Global Blocking on the basis of Hashes and create blacklist for the environment.
HIPS.REQ.0050		Solution should have option to allow to install new software or update by setting up maintenance mode and should have ability to scan for an inventory of installed software & create an initial local ruleset.
HIPS.REQ.0051		Change or new software should be identified based on File name, path, time stamp, permission, file contents etc. and must have ability to enable maintenance mode during updates or upgrades for predefined time period.
HIPS.REQ.0052		Logging of all software changes except when the module is in maintenance mode and Should support Windows & Linux operating systems.
HIPS.REQ.0053		Should have the ability to enforce either Block or Allow unrecognized software and must support Lock Down mode:

S.No.	Parameter	Minimum Specifications
		No Software is allowed to be installed except what is detected during agent installation.
HIPS.REQ.0054	**Command & Control Functional Features**	solution must be able to block all communication to Command & control center and must be able to identify communication over HTTP/HTTPS protocols and commonly used Http ports.
HIPS.REQ.0055		Solution must provide by default security levels i.e. High, Medium & low so that it eases the operational effort and Solution must have an option of assessment mode only so that URLs are not blocked but logged.
HIPS.REQ.0056		solution must be able to detect/prevention communications to Global C&C's and Allow administrators to create user defined list of allowed/blocked URL's.
HIPS.REQ.0057	**Management Features**	Management of proposed solution should be GUI based on either windows and/ or linux platform in high availability configuration for DC/DR setup to manage both windows and linux environment.
HIPS.REQ.0058		Agent installation methods should support manual local installation, packaging with third party software distribution systems and distribution through LDAP/ Active Directory.
HIPS.REQ.0059		The solution should give the flexibility of deploying features either as agent based or agentless for different modules depending on organization's data center environment.
HIPS.REQ.0060		The solution should have comprehensive Role Based Access Control features including controlling who has access to what areas of the solution and who can do what within the application.
HIPS.REQ.0061		The solution shall allow grouping security configurations together in a policy and also allow to apply these configurations to other similar systems.
HIPS.REQ.0062		The solution should support Web Services if it is required to export data out to other custom reporting solutions and shall allow creation of custom lists, such as IP Lists, MAC lists etc. that can be used in the policies that are created.
HIPS.REQ.0063		Administrators should be able to selectively rollback rules applied to agents and should maintain full audit trail of administrator's activity.
HIPS.REQ.0064		Solution should have an override feature which would remove all the applied policies and bring the client back to default policies.
HIPS.REQ.0065		The solution shall allow updates to happen over internet or shall allow updates to be manually imported in the central management system and then distributed to the managed agents. Additionally, solution must also have an option of defining machine to be updater relay only.
HIPS.REQ.0066	**Integration**	Should have capabaility to share suspicious files to Firewall/ Anti-APT solution as per RFP specifications to detect and mitigate zero-day threats having common threat sharing platform for holistic visibility and control
HIPS.REQ.0067	**Global Certification**	OEM must have coverage at least 30 zeroday/undisclosed vulnerabilities of Microsoft continuously from past 5 years and data should be publically available.
HIPS.REQ.0068		The proposed solution should be EAL 2 + certified
HIPS.REQ.0069	**Warranty &**	5 years On-site comprehensive warranty with 24x7x365

S.No.	Parameter	Minimum Specifications
	Post warranty Support	solution (Hardware & associated software) support

5.28 INTERNAL FIREWALL

S.No.	Minimum Specifications
INTFW.REQ.001	The proposed Enterprise/core & Perimeter NGFW shall be from a different OEM. The appliance-based security platform should be capable of providing firewall, application visibility, IPS functionality and antivirus in a single appliance.
INTFW.REQ.002	The OEM shall provide 365x7x24 days technical support. The OEM shall provide the login credentials with highest level of permissions to raise the technical issues in the name ofDITECH/CRID Haryana, search knowledgebase, download the patches and upgrades, documents and manage the device on OEM sites. The successful Bidder must provide the login credentials.
INTFW.REQ.003	The solution provided should not be end of support before 5 years from Date of sign off of project. It should continue to provide the following for next five years: a) Upgrades and latest OS version in market b) Updates c) Patches and Fixes
INTFW.REQ.004	During the support period as mentioned in point above, the proposed solution shall receive the following a) Firmware and latest OS Upgrades for the quoted model b) Updates/Signatures c) Patches and Fixes
INTFW.REQ.005	The proposed solution should have seamless integration with APT for detecting and mitigating zero-day threats leveraging sandbox analysis asked in the tender. Firewall should be able to integrate with other OEM APT
INTFW.REQ.006	The proposed solution shall not be End-of-support by the OEM for 5 years from the date of bid submission
INTFW.REQ.007	The appliance should not have any active internal or external Wi-Fi, Bluetooth, NFC components.
	Specification
INTFW.REQ.008	The proposed firewall solution/platform shall run on a hardened OS and delivered on purposeful built hardware and security appliance.
INTFW.REQ.009	Solution/platform shall provide features and licenses for a period of 5 years for Firewall, IPS, Site to Site VPN, Granular Application control, Anti-Malware, IPS, DNS Security, Identity Awareness and Anti-Bot on same platform/appliance managed through a centralized management console.
INTFW.REQ.0010	Solution/platform shall support Application level and "Stateful" policy inspection technology to prevent traffic leakage. It shall also have application intelligence for commonly used TCP/IP protocols like telnet, ftp, http, web 2.0 application etc.
INTFW.REQ.0011	The proposed security platform shall be supplied, installed and configured in N+1 redundancy. **High-Availability Features** Firewall should support -Active/Standby and Active/Active failover, -ether channel or equivalent functionality for the failover control and providing additional level of redundancy - redundant interfaces to provide interface level redundancy before device failover, -802.3ad Ether channel or equivalent functionality to increase the bandwidth for a segment. Firewall should have integrated redundant power supply

S.No.	Minimum Specifications
	Solution shall support configuration of dual stack gateway on a bond interface or on a sub-interface of a bond interface.
INTFW.REQ.0012	Firewall OS, CVE (Common Vulnerabilities and Exposures) must be available/disclosed on public web sites
INTFW.REQ.0013	It shall be possible to centrally manage Firewall and all the associated modules/ functionalities/ services over secure channel.
INTFW.REQ.0014	solution/platform shall be supplied with the support for all standard static and dynamic routing protocols.
INTFW.REQ.0015	The solution/platform shall support VLAN tagging (IEEE 802.1q).
INTFW.REQ.0016	Solution/platform shall have integration with Identity Awareness Capabilities on the security appliance via Active Directory or RADIUS.
INTFW.REQ.0017	Solution/platform shall support Application awareness and granular control functionalities for all the commonly available Web 2.0 applications and tools.
INTFW.REQ.0018	shall provide IPv4 and IPv6 support and must have IPv6 ready/USGv6R1 Standard International /National Certification or STQC certification for trusted supply chain compliance
INTFW.REQ.0019	Solution/platform shall support Link aggregation functionality (LACP/PAGP) to group multiple ports as single Channel.
INTFW.REQ.0020	Solution/platform shall not have any licensing restriction on number of users and shall be supplied for unlimited users unless specified otherwise.
INTFW.REQ.0021	Solution/platform shall support site-to-site, Remote Access IPsec VPN & SSL VPN functionality Should be supplied with 10,000 SSL VPN users license from dayone
INTFW.REQ.0022	The firewall appliance/platform shall provide minimum 5 numbers of virtual systems/domains from Day 1. The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode.
Performance Requirements	
INTFW.REQ.0023	The proposed internal firewall with features as mentioned (Firewall, IPS, VPN, Application visibility control, Mobile Access, Anti-virus, Anti-Malware, Anti-Spyware, URL Filtering, Antibot, Advance Networking & clustering, Identity Awareness) must provide threat prevention throughput of at least 20 Gbps considering in real world/production environment/Application Mix with all features/licenses enabled on day 1 and scalable up to 40 Gbps future upgrade without replacing or augmenting the hardware/solution supplied. The bidder shall submit the performance test report reference from public documents or from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by person with PoA.
INTFW.REQ.0024	Proposed appliance/platform shall support at least 20 million concurrent session expandable up to 40 million sessions on L4 or 3.2 million concurrent sessions expandable upto 6.4 million concurrent session on L7 and minimum 800,000 new connection per second on L4 from day 1 or or 150,000 new connection per second on L7 and scalable to handle additional requirements(i.e minimum1,600,000 new connection per second on L4 or 300,000 new connection per second on L7) without replacing the existing hardware.
INTFW.REQ.0025	Solution/platform shall have minimum following ports: - 8 usable 1 Gig interfaces SFP/Copper -4 usable 10 Gig SFP+ Interfaces - 4 usable 25/10 Gig SFP28 Interfaces

S.No.	Minimum Specifications
	- Separate & Dedicated 1 x 1G port for out of band management - port for HA connectivity - 4 x 40 Gig QSFP+ Ports with SR transceivers From day 1
INTFW.REQ.0026	Proposed appliance/platform must have integrated redundant hot-swappable power supplies
INTFW.REQ.0027	The proposed firewall/solution architecture should have control/management Plane separated from the Data Plane whereby Control/Management Plane should handle Management functions like configuration, reporting & Data Plane should handle Signature matching, Security processing & Network Processing.
INTFW.REQ.0028	The proposed solution/platform hardware should be a multicore CPU architecture with a hardened 64-bit operating system to support higher memory and should support minimum of 96 GB of RAM or higher from day 1 and scalable to support 128GB RAM without changing the existing hardware.
INTFW.REQ.0029	The firewall/solution must have at least usable 480GB (SSD) storage from day 1.
	Network Protocols/Standards Support Requirements
INTFW.REQ.0030	The proposed firewall shall support Dual Stack IPv4 / IPv6 application control and threat inspection support in: - Tap Mode - Transparent mode (IPS Mode) - Layer 2 - Layer 3 - Should be able operate mix of multiple modes
INTFW.REQ.0031	The proposed firewall must support at-least the following routing protocols: - Static - RIP v2 - OSPFv2/v3 with graceful restart - BGP v4 with graceful restart
INTFW.REQ.0032	The proposed firewall/platform shall be able to handle unknown /unidentified applications with actions like allow, block or alert.
INTFW.REQ.0033	The proposed firewall/platform shall have granular application identification technology based upon deep packet inspection.
INTFW.REQ.0034	The proposed firewall/platform shall warn the end user with a customizable page when the application is blocked.
INTFW.REQ.0035	The proposed firewall/platform shall delineate specific instances of instant messaging/Social Network Applications (Facebook Chat, WhatsApp, Telegram, WeChat etc.).
INTFW.REQ.0036	The proposed firewall/platform shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability. The proposed firewall shall be able to protect the user from the malicious content upload or download by any application. Example Blocking a malicious file download via a chat or file sharing application.
INTFW.REQ.0037	The Firewall/platform shall provide stateful engine support for all common protocols of the TCP/IP stack.
INTFW.REQ.0038	The Firewall/platform shall provide NAT functionality, including dynamic and static NAT translations.
INTFW.REQ.0039	Firewall/platform should have creating access-rules with IPv4 & IPv6 objects wise, user/groups wise, application wise, application wise geolocation control, url wise, zone wise, vlan wise, etc.
INTFW.REQ.0040	Should have more than pre-defined 3000 distinct application signature (excluding custom application signatures) as application detection mechanism to optimize security effectiveness and should be able to create new application

S.No.	Minimum Specifications
	categories for operational efficiency
INTFW.REQ.0041	Solution should support the following authentication protocols: - LDAP - Radius (vendor specific attributes) - Token-based solutions (i.e. Secure-ID) - Kerberos The proposed firewall's SSL VPN shall support the following authentication protocols - LDAP - Radius - Token-based solutions (i.e. Secure-ID) - Kerberos - SAML - Any combination of the above
INTFW.REQ.0042	a) Network address translation (NAT) shall be supported so that the private IP addresses of hosts and the structure of an internal network can be concealed by the firewall.
INTFW.REQ.0043	b) Network Address Translation (NAT) shall be configurable as 1:1, 1: many, many: 1, many: many.
INTFW.REQ.0044	c) Reverse NAT shall be supported.
INTFW.REQ.0045	d) Port address translation /Masquerading shall be supported.
INTFW.REQ.0046	Dynamic Host Configuration Protocol (DHCP)& Virtual Private Network (VPN) shall be supported
INTFW.REQ.0047	The firewall/platform shall support Internet Protocol Security (IPsec).
INTFW.REQ.0048	Key exchange with latest Internet Key Exchange (IKE), Public Key Infrastructure PKI (X.509) shall be catered to.
INTFW.REQ.0049	Support Latest Encryption algorithms including AES 128/192/256(Advanced Encryption Standards), 3DES etc.
INTFW.REQ.0050	Support Latest Authentication algorithms including SHA-1(Secure Hash Algorithm-1), SHA-2(Secure Hash Algorithm-2) etc.
INTFW.REQ.0051	IPsec NAT traversal shall be supported.
	Firewall Policy Requirements
INTFW.REQ.0052	Firewall//platform shall be able to configure rules based on the following parameter -- a) Source/Destination IP/Port/Geo locations b) Time and date access c) User/group role (After Integration with AD) d) Customizable services e) Combination of one or multiple of above mentioned parameters
INTFW.REQ.0053	The Firewall/platform shall be able to filter traffic even if the packets are fragmented.
INTFW.REQ.0054	It shall support the VOIP Applications Security by supporting to filter SIP, H.323, MGCP etc.
INTFW.REQ.0055	Firewall/platform shall support Access for Granular user, group &machine based visibility and policy enforcement. It shall have following features:
	a) The firewall/platform shall mask/NAT the internal network from the external world. The proposed firewall must be able to operate in routing/NAT mode
	b) Multi-layer, stateful, application -inspection-based filtering shall be supported.
	c) It shall provide network segmentation features with capabilities that facilitate deploying security for various internal, external and DMZ

S.No.	Minimum Specifications
	(Demilitarized Zone) sub-groups on the network, to prevent unauthorized access.
	d) Ingress/egress filtering capability shall be provided.
	e) There shall be support for detection of reconnaissance attempts such as IP address sweep, port scanning etc.
	f) Basic attack protection features listed below but not limited to : • Maximum no of protections against attacks that exploit weaknesses in the TCP/IP protocol suite. • It shall enable rapid detection of network attacks • TCP reassembly for fragmented packet protection • SYN cookie protection , SYN Flood, Half Open Connections • DoS/DDoS Protection • Protection against IP spoofing • Malformed packet protection
	Application Control Feature Set
INTFW.REQ.0056	a. Should be capable of dynamically IPS policies/Profiles (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention. b. Solution detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques.
INTFW.REQ.0057	Should have more than 11,000 (excluding custom signatures) IPS signatures or more.
INTFW.REQ.0058	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to security events.
INTFW.REQ.0059	Solution must have IOC management / IP reputation intelligence feeds from native/third party and custom lists of IP addresses including a global blacklist. Should support DNS threat intelligence feeds to protect against threats. The proposed NGFW must be able to ingest threat intelligence / help create a security intelligence/ threat intelligence.
INTFW.REQ.0060	The Appliance OEM must have its own threat intelligence analysis centre and should use the global footprint of security deployments for more comprehensive network protection without any integration with 3rd party. The detection engine should support the capability of detecting variants of known threats, as well as new threats
INTFW.REQ.0061	Enforce policy on individual users and user groups: Policy to allow or deny certain types of traffic must be enforceable on individual users or user groups.
INTFW.REQ.0062	User-developed application & IPS signatures: The application control & IPS function shall allow to create new application & IPS signatures.
	Anti-APT (Zero Day Protection)
INTFW.REQ.0063	The Proposed NGFW must support the integration with On-Prem (No cloud based) Anti-APT devices. Security grid must have automation capability to create key stitches using integrations out of the box for firewalls/ integration through APIs, Sandbox solution
INTFW.REQ.0064	Internal firewall must have centralized console for analysis for organization wide security view and centralized logging must be shared with proposed SIEM solution.
	Administration, Management, Logging & Reporting
INTFW.REQ.0065	Solution must have tracking mechanism for the changes done on policy management dashboard and maintain audit trails.
INTFW.REQ.0066	The Firewall Management Solution, log server and reporting server can be

S.No.	Minimum Specifications
	either hardware appliance or VM based solution.
INTFW.REQ.0067	In case of VM based management solution, VM infrastructure will be provided by customer. will provide VM based infrastructure for hosting the management solution including storage &compute. All other third party licenses including OS, software components, databases etc. for running the solution has to be provided by the bidder for the entire duration of the project. All licenses shall be Enterprise class. The bidder has to provide required licenses in case of any upgrade/change of any component of the whole solution during entire period of the project. Solution has to be configured by the bidder to cater to smooth operation of the whole solution. Solution should be scalable to use more storage and compute if required.
INTFW.REQ.0068	The Solution shall receive logs for the overall proposed solution in a single virtual system, and shall not be separate for each module of proposed firewalls. All the logs shall be stored for 180 days or as per the standard set by the government with all features and policies enabled. The sizing of the disk space has to be done accordingly.
INTFW.REQ.0069	PIM-SM, PIM-SSM, IGMP v1, v2, and v3
INTFW.REQ.0070	The offered firewall solution must be a appliance and should be provided with redundant Fans and power supplies
INTFW.REQ.0071	Solution should be able to detect & prevent the Bot communication with ICC. DNS Security should support predictive analytics to disrupt attacks that use DNS for Data theft and Command and Control
INTFW.REQ.0072	Solution should have n Multi-tier engine to detect & prevent Command and Control IP/URL and DNS.
INTFW.REQ.0073	Firewall Policies : 45,000 or more
	Management & Logging/Reporting
INTFW.REQ.0074	The management must be accessible via a web-based interface and ideally with no need for additional client software
INTFW.REQ.0075	The management solution must be capable of role-based administration
INTFW.REQ.0076	The solution must provide multiple report output types or formats, such as PDF, HTML, and CSV.
INTFW.REQ.0077	The solution must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.
	Architecture
INTFW.REQ.0078	The administrator must be able to view report on the CPU usage for management activities and CPU usage for other activities.
	Next Generation Firewall Features
INTFW.REQ.0079	Should support Two Factor Authentication for Browser-Based Authentication (support for RADIUS challenge/response in Captive Portal and RSA SecurID next Token/Next PIN mode)
	Threat Protection
INTFW.REQ.0080	The proposed firewall shall have on box Anti-Virus/Malware, Anti Spyware signatures and should have minimum signatures update window of every two hours
INTFW.REQ.0081	NGFW should have a vast categorization database where websites are classified based on site content, features, and safety in more than 68 benign and malicious content categories
INTFW.REQ.0082	The proposed firewall should have SSL decryption and shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy)
INTFW.REQ.0083	The firewall should support TLSv1.2 and TLSv1.3 decryption and also supports

S.No.	Minimum Specifications
	Outbound and Inbound inspection.
INTFW.REQ.0084	Should support SLAAC Stateless Address Auto configuration
INTFW.REQ.0085	The proposed firewall must have support for mobile protocols like GTP, SCTP.
INTFW.REQ.0086	The proposed solution should support the ability to create QoS policy on a per rule basis: -by source address -by destination address -by application (such as Skype, Bittorrent, YouTube, azureus) -by port and services
INTFW.REQ.0087	Bidirectional Forwarding Detection (BFD)
INTFW.REQ.0088	The Solution should support DNS security
INTFW.REQ.0089	**Monitoring, Management and Reporting**
INTFW.REQ.0090	Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis
INTFW.REQ.0091	Should have built in report templates base on Applications, Users, Threats, Traffic and URLs
INTFW.REQ.0092	Should be able to create report base on SaaS application usage
INTFW.REQ.0093	Should be able to create reports base user activity
INTFW.REQ.0094	Should be able to create custom report base on custom query base any logging attributes
	Authorization
INTFW.REQ.0095	Original Manufacturer Authorization Certificate to be submitted along with the bid. We reserve the right to reject in case deviation on the basis of technical compliance as submitted in the tender document.
INTFW.REQ.0096	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.29 EXTERNAL FIREWALL

S.No.	Minimum Specifications
EXTFW.REQ.001	The proposed Enterprise/core & Perimeter NGFW shall be from a different OEM.
EXTFW.REQ.002	The OEM shall provide 365x7x24 days technical support. The OEM shall provide the login credentials with highest level of permissions to raise the technical issues, search knowledgebase, download the patches and upgrades, documents and manage the device on OEM sites. The successful Bidder must provide the login credentials.
EXTFW.REQ.003	The solution provided should not be end of support before 5 years from Date of sign off of project. It should continue to provide the following for next five years: a) Upgrades and latest OS version in market b) Updates c) Patches and Fixes
EXTFW.REQ.004	During the support period as mentioned in point above, the proposed solution shall receive the following a) Firmware and latest OS Upgrades for the quoted model b) Updates/Signatures c) Patches and Fixes
EXTFW.REQ.005	The proposed solution shall not be End-of-support by the OEM for 5 years from the date of bid submission
EXTFW.REQ.006	The appliance should not have any active internal or external Wi-Fi component.
	Specification
EXTFW.REQ.007	The proposed firewall solution/platform shall run on a hardened OS and delivered on purposeful built hardware and security appliance.
EXTFW.REQ.008	Solution/platform shall provide features for Firewall, IPS, Application control, Anti-Malware and Anti-Bot on same platform/appliance managed through a centralized management console.
EXTFW.REQ.009	Solution/platform shall support Application level and "Stateful" policy inspection technology to prevent traffic leakage. It shall also have application intelligence for commonly used TCP/IP protocols like telnet, ftp, http, web 2.0 application etc.
EXTFW.REQ.0010	The proposed firewall solution (platform/appliance(s)) shall be supplied, installed and configured in N+1 redundancy. High-Availability Features Firewall should support -Active/Standby and Active/Active failover, -ether channel or equivalent functionality for the failover control and providing additional level of redundancy - redundant interfaces to provide interface level redundancy before device failover, -802.3ad Ether channel or equivalent functionality to increase the bandwidth for a segment. Firewall should have integrated redundant power supply Solution shall support configuration of dual stack gateway on a bond interface or on a sub-interface of a bond interface. Solution should Support NAT64, NAT46,NAT66/NPTv6.
EXTFW.REQ.0011	Appliance/platform shall not require any downtime/ reboot for failover & backup purpose.
EXTFW.REQ.0012	Firewall OS, CVE (Common Vulnerabilities and Exposures) must be available/disclosed on public web sites
EXTFW.REQ.0013	It shall be possible to centrally manage Firewall and all the associated modules/ functionalities/ services over secure channel.
EXTFW.REQ.0014	solution/platform shall be supplied with the support for static and dynamic routing protocols.

S.No.	Minimum Specifications
EXTFW.REQ.0015	The solution/platform shall support VLAN tagging (IEEE 802.1q).
EXTFW.REQ.0016	Solution/platform shall have integration with Identity Awareness Capabilities on the security appliance via Active Directory or RADIUS.
EXTFW.REQ.0017	Solution/platform shall support Application awareness and granular control functionalities for all the commonly available Web 2.0 applications and tools.
EXTFW.REQ.0018	shall provide IPv4 and IPv6 support and must have IPv6 ready/USGv6R1 standard certification.
EXTFW.REQ.0019	The proposed firewall solution (platform/appliance(s)) shall support Link aggregation functionality (LACP/PAGP) to group multiple ports as single Channel.
EXTFW.REQ.0020	Solution/platform shall not have any licensing restriction on number of users and shall be supplied for unlimited users unless specified otherwise.
EXTFW.REQ.0021	Solution/platform shall support site-to-site, Remote Access IPsec VPN & SSL VPN functionality
EXTFW.REQ.0022	The proposed firewall solution (platform/appliance(s)) shall provide minimum 10 numbers of virtual systems/domains from Day 1. Should be scalable up to 30 virtual systems/ domains
	Performance Requirements
EXTFW.REQ.0023	Threat Prevention throughput of at least 10 Gbps with real world/production environment/Application Mix with all features/licenses enabled scalable up to 20 Gbps from day 1. The solution should have provision of additional 10G license for future upgrade without replacing or augmenting the hardware supplied. The bidder shall submit the performance test report reference from public documents or from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by person with PoA. The appliance should support x Forward feature
EXTFW.REQ.0024	The proposed firewall solution (platform/appliance(s)) shall support at least 8 million concurrent sessions on L4 or at least 1.5 million concurrent session on L7 and minimum 400,000 new connections per second on L4 from day 1 or minimum 120,000 new connections per second on L7 from day 1 and scalable to at least 16 million concurrent sessions on L4 or at least 3 million concurrent sessions on L7 and minimum 800,000 new connection per second on L4 or minimum 240,000 new connection per second on L7 without replacing the existing hardware
EXTFW.REQ.0025	The proposed firewall solution (platform/appliance(s)) shall have minimum following ports: - 8 usable 1 Gig interfaces SFP/Copper - 8 usable 25/10 Gb populated with SFP28 Interfaces with SR transceivers - 2 usable 40 Gig QSFP+ Interfaces with SR transceivers - Separate & Dedicated 1 x 1G port for out of band management - Separate & dedicated port for HA connectivity
EXTFW.REQ.0026	Proposed appliance/platform must have integrated redundant hot-swappable power supplies and redundant fan
EXTFW.REQ.0027	The proposed firewall solution (platform/appliance(s)) architecture should have Control/ Management Plane separated from the Data Plane in the Device architecture itself, whereby Control/ Management Plane should handle Management functions like configuration, reporting and logging, and Data Plane should handle Signature matching (like exploits, virus, spyware, CC#),

S.No.	Minimum Specifications
	Security processing (like apps, users, content/URL, policy match, SSL decryption, application identification etc) & Network Processing (like flow control, route lookup, QoS, NAT etc).
EXTFW.REQ.0028	The proposed solution/platform hardware should be a multicore CPU architecture with a hardened 64-bit operating system to support higher memory and should support minimum of 96 GB of RAM or higher from day 1 and scalable to support 128 GB RAM without changing the existing hardware.
	Network Protocols/Standards Support Requirements
EXTFW.REQ.0029	The proposed firewall shall support Dual Stack IPv4 / IPv6 application control and threat inspection support in: - Tap Mode - Transparent mode (IPS Mode) - Layer 2 - Layer 3 - Should be able operate mix of multiple modes
EXTFW.REQ.0030	The proposed firewall must support the following routing protocols: - Static - RIP v2 - OSPFv2/v3 with graceful restart - BGP v4 with graceful restart
EXTFW.REQ.0031	The proposed firewall/platform shall be able to handle unknown /unidentified applications with actions like allow, block or alert.
EXTFW.REQ.0032	The proposed firewall/platform shall have granular application identification technology based upon deep packet inspection.
EXTFW.REQ.0033	The proposed firewall/platform shall warn the end user with a customizable page when the application is blocked.
EXTFW.REQ.0034	The proposed firewall/platform shall delineate specific instances of instant messaging/Social Network Applications (Facebook Chat, WhatsApp, Telegram, WeChat etc.).
EXTFW.REQ.0035	The proposed firewall/platform shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability. The proposed firewall shall be able to protect the user from the malicious content upload or download by any application. Example Blocking a malicious file download via a chat or file sharing application.
EXTFW.REQ.0036	The Firewall/platform shall provide stateful engine support for all common protocols of the TCP/IP stack.
EXTFW.REQ.0037	The Firewall/platform shall provide NAT functionality, including dynamic and static NAT translations.
EXTFW.REQ.0038	Firewall/platform should have creating access-rules with IPv4 & IPv6 objects wise, user/groups wise, application wise, geolocation control, url wise, zone wise, vlan wise, etc.
EXTFW.REQ.0039	Should have more than pre-defined 4000 distinct application signature (excluding custom application signatures) as application detection mechanism to optimize security effectiveness and should be able to create new application minimum 24 or more categories for operational efficiency
EXTFW.REQ.0040	Solution should support the following authentication protocols: - LDAP - Radius - Token-based solutions (i.e. Secure-ID) - Kerberos The proposed firewall's SSL VPN shall support the following authentication

S.No.	Minimum Specifications
	protocols - LDAP - Radius - Token-based solutions (i.e. Secure-ID) - Kerberos - SAML - Any combination of the above
EXTFW.REQ.0041	a) Network address translation (NAT) shall be supported so that the private IP addresses of hosts and the structure of an internal network can be concealed by the firewall.
EXTFW.REQ.0042	b) Network Address Translation (NAT) shall be configurable as 1:1, 1: many, many: 1, many: many.
EXTFW.REQ.0043	c) Reverse NAT shall be supported.
EXTFW.REQ.0044	d) Port address translation /Masquerading shall be supported.
EXTFW.REQ.0045	Dynamic Host Configuration Protocol (DHCP)& Virtual Private Network (VPN) shall be supported
EXTFW.REQ.0046	The firewall/platform shall support Internet Protocol Security (IPsec).
EXTFW.REQ.0047	Key exchange with latest Internet Key Exchange (IKE), Public Key Infrastructure PKI (X.509) shall be catered to.
EXTFW.REQ.0048	Support Latest Encryption algorithms including AES 128/192/256(Advanced Encryption Standards), 3DES etc.
EXTFW.REQ.0049	Support Latest Authentication algorithms including SHA-1(Secure Hash Algorithm-1), SHA-256(Secure Hash Algorithm-2) etc.
EXTFW.REQ.0050	IPsec NAT traversal shall be supported.
	Firewall Policy Requirements
EXTFW.REQ.0051	Firewall//platform shall be able to configure rules based on the following parameter -- a) Source/Destination IP/Port/Geo locations b) Time and date access c) User/group role d) Application and services e) Combination of one or multiple of above-mentioned parameters Firewall for stateful blocking, Anti-Spoofing, IP Reputation, Geo-Protection, Dropping Invalid Connections
EXTFW.REQ.0052	The Firewall/platform shall be able to filter traffic even if the packets are fragmented.
EXTFW.REQ.0053	It shall support the VOIP Applications Security by supporting to filter SIP, H.323, MGCP etc.
EXTFW.REQ.0054	Firewall/platform shall support Access for Granular user, group &machine-based visibility and policy enforcement. It shall have following features:
EXTFW.REQ.0055	a) The firewall/platform shall mask/NAT the internal network from the external world.
EXTFW.REQ.0056	b) Multi-layer, stateful, application -inspection-based filtering shall be supported.
EXTFW.REQ.0057	c) It shall provide network segmentation features with capabilities that facilitate deploying security for various internal, external and DMZ (Demilitarized Zone) sub-groups on the network, to prevent unauthorized access.
EXTFW.REQ.0058	d) Ingress/egress filtering capability shall be provided.
EXTFW.REQ.0059	e) There shall be support for detection of reconnaissance attempts such as IP address sweep, port scanning etc.

S.No.	Minimum Specifications
EXTFW.REQ.0060	f) Basic attack protection features listed below but not limited to : • Maximum no of protections against attacks that exploit weaknesses in the TCP/IP protocol suite. • It shall enable rapid detection of network attacks • TCP reassembly for fragmented packet protection • SYN cookie protection , SYN Flood, Half Open Connections • DoS/DDoS Protection • Protection against IP spoofing • Malformed packet protection
	Application Control Feature Set
EXTFW.REQ.0061	a. Should be capable of dynamically IPS policies/Profiles (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention. Should have pre-defined threat prevention policies to configure from day1 with minimal human intervention b. Solution detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques.
EXTFW.REQ.0062	Should have more than 11,000 (excluding custom signatures) IPS signatures or more.
EXTFW.REQ.0063	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.
EXTFW.REQ.0064	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to security events.
EXTFW.REQ.0065	Solution must have IOC management / IP reputation intelligence feeds from native/third party and custom lists of IP addresses including a global blacklist. Should support DNS threat intelligence feeds to protect against threats
EXTFW.REQ.0066	The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection without any integration with 3rd party. The detection engine should support the capability of detecting variants of known threats, as well as new threats
EXTFW.REQ.0067	Enforce policy on individual users and user groups: Policy to allow or deny certain types of traffic must be enforceable on individual users or user groups.
EXTFW.REQ.0068	User-developed application & IPS signatures: The application control & IPS function shall allow to create new application & IPS signatures. IPS must have a mechanism to convert SNORT signatures and upload in the IPS signatures database.
EXTFW.REQ.0069	The Proposed NGFW must support the integration with On-Prem (No cloud based) Anti-APT devices.
	Administration, Management, Logging & Reporting
EXTFW.REQ.0070	Solution must have mechanism to track and report the changes done on policy management and maintain audit trails.
EXTFW.REQ.0071	The Firewall Management Solution, log server and reporting server can be either hardware appliance or VM based solution.

S.No.	Minimum Specifications
EXTFW.REQ.0072	In case of VM based management solution, VM infrastructure will be provided for hosting the management solution including storage &compute. All other third-party licenses including OS, software components, databases etc. for running the solution will be provided for the entire duration of the project. All licenses will be Enterprise class. The required licenses will be provided in case of any upgrade/change of any component of the whole solution during entire period of the project. Solution has to be configured by the bidder to cater to smooth operation of the whole solution. Solution should be scalable to use more storage and compute if required.
EXTFW.REQ.0073	The Solution shall receive logs for the overall proposed solution in a single virtual system, and shall not be separate for each module of proposed firewalls. All the logs shall be stored for 180 days as per the government standards with all features and policies enabled. The sizing of the disk space has to be done accordingly.
EXTFW.REQ.0074	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.
EXTFW.REQ.0075	d. Should support Multicast protocols like IGMP, PIM, etc
EXTFW.REQ.0076	The solution must have data loss prevention by defining the categories of sensitive information that is required to filter.
	Management & Logging/Reporting
EXTFW.REQ.0077	The solution should come with a web based administration interface or GUI console.
EXTFW.REQ.0078	Solution must be able to define the Custom roles in addition to predefined roles (e.g., Owner, Viewer, Operator,Editor, Super User) to control permissions flexibly and accurately
EXTFW.REQ.0079	The Solution must be able to generate report in PDF/HTML Formats for all the Security Functionalities including IPS, AV,ABOT,Evasions and Applications, And should be able to export logs in csv format.
	Architecture
EXTFW.REQ.0080	The administrator must be able to view status on the CPU usage of management and firewall. The solution should provide Performance of Network devices like CPU, memory & buffers etc., LAN and WAN interfaces, Network segments and VLANs.
EXTFW.REQ.0081	The device or any of its family should not have any feature of wireless within its hardware or software.
EXTFW.REQ.0082	Should support Two Factor Authentication for browser based authentication (for RADIUS challenge/response in Captive Portal and RSA SecurID next Token/Next PIN mode)
EXTFW.REQ.0083	The proposed firewall shall have on box IPS, Anti-Virus/Malware, Anti Bot/ Spyware signatures and should have minimum signatures update window of every two hour
EXTFW.REQ.0084	The proposed firewall should have a vast categorisation database where websites are classified based on site content, features, and safety in more than 68 benign and malicious content categories
EXTFW.REQ.0085	The proposed firewall should have SSL decryption and shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy)
EXTFW.REQ.0086	The firewall supports TLSv1.2 and TLSv1.3 decryption
EXTFW.REQ.0087	Should support SLAAC Stateless Address Auto configuration

S.No.	Minimum Specifications
EXTFW.REQ.0088	The proposed solution should support the ability to create QoS policy on a per rule basis: -by source address -by destination address -by application -by port and services
EXTFW.REQ.0089	Bidirectional Forwarding Detection (BFD)
EXTFW.REQ.0090	The Solution should support DNS security
	Monitoring, Management and Reporting
EXTFW.REQ.0091	Should have separate real time logging base on all Traffic, Threats, User IDs, URL filtering, Data filtering, Content filtering, unknown malware analysis, Authentication, Tunnelled Traffic and correlated log view base on other logging activities
EXTFW.REQ.0092	Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis
EXTFW.REQ.0093	Should have built in report templates base on Applications, Users, Threats, Traffic and URLs
EXTFW.REQ.0094	Should be able to create reports base user activity
EXTFW.REQ.0095	Should be able to create custom report base on custom query base any logging attributes
EXTFW.REQ.0096	**Authorization**
EXTFW.REQ.0097	Original Manufacturer Authorization Certificate to be submitted along with the bid. We reserve the right to reject in case deviation on the basis of technical compliance as submitted in the tender document.
	Support & Warranty
EXTFW.REQ.0098	There should be at least RMA dept and one TAC/Technical support centre(RTS) for support in India). The proposed firewall solution (platform/appliance(s)) should be proposed with perpetual/ subscription licenses for all feature enabled from day1 during scope of work of this RFP i.e. 5 years from go live + 2 years for software updates upgrade including OEM support for said activities. Following Feature must be available in the proposed firewall solution (platform/appliance(s)) : (Firewall,IPS,IPSec VPN,Application visibility control,Mobile Access,Anti-virus,Anti-Malware,Anti-Spyware, URL Filtering,Antibot,Advance Networking & clustering,Identity Awareness,DNS Security)
EXTFW.REQ.0099	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.30 SIEM UEBA

S. No.	Minimum Specifications
SIEM.REQ.001	The offered solution should have following functional components: a. Management & Reporting b. Normalization and Indexing c. Correlation Engine d. Data Management e. UEBA or equivalent
SIEM.REQ.002	UEBA can be either a purpose build appliance / Software base / VM based. In any case, the OEM to provide all the required licenses, storage, infrastructure and all features without degrading the performance.
SIEM.REQ.003	The SIEM solution with hardened OS/OS hardening should be sized for 25,000 sustained EPS at all levels and 50,000 peak/burst EPS real world traffic. SIEM solution should be licensed based on standard licensing parameter (i.e. sustained events per second) and should be perpetual. OR SIEM solution must support minimum 5000 devices with appropriate licenses. SIEM must have device/ EPS licensing.
SIEM.REQ.004	The SIEM must be able to collect log/event data from various sources such as servers, network and cyber security devices, and applications. It should support various log/event formats and protocols such as syslog, SNMP, WMI etc. generated in heterogenous DC environment. The system should support collecting events/logs in real-time and/or batch mode. The solution should have single integrated facility for log investigation, incident management etc. with a search facility to search the collected raw log data for specific events or data.
SIEM.REQ.005	The system should be able to aggregate log/event data from multiple sources and create a single view of security events. The aggregation should be done in real-time to provide a complete and accurate view of security events. The system should support real-time and batch processing of data to ensure that security events are detected and analyzed in a timely manner.
SIEM.REQ.006	The solution should be storing both raw logs as well as normalized logs. The same should be made available for analysis and reporting. Solution should be sized to provide online storage for 6 months and archival data for 2 years at central site.
SIEM.REQ.007	Intelligent next generation SOC must be able to detect any anomalies, report in real time and can take action as programmed. It should have core SIEM and UEBA capabilities to provide unified SOC monitoring through layered security defence platform to SecOps team.
SIEM.REQ.008	The Solution should be offered by required Licenses, Hardware and Softwares.
SIEM.REQ.009	The SIEM should be from a different OEM than the Prevention Security solutions like F/W, IPS, HIPS, AV, DLP and Encryption.
SIEM.REQ.0010	The solution should enable the Information Security Team to quickly prioritize it's response to help ensure effective incident handling.
SIEM.REQ.0011	The SIEM system should have the ability to normalize data from different sources and translate them into a common format for analysis and correlation.
SIEM.REQ.0012	Event correlation: The SIEM should have the ability to correlate security events from different sources to identify threats and attacks. It should use advanced algorithms to identify patterns and anomalies in log data. The SIEM should correlate between Log, Netflow and endpoint data to provide a complete analysis.
SIEM.REQ.0013	The SIEM system should have advanced analytics and correlation capabilities to

S. No.	Minimum Specifications
	identify patterns, anomalies, and threats across different data sources.
SIEM.REQ.0014	The system should support rule-based and behavior-based analysis to detect known and unknown threats.
SIEM.REQ.0015	The SIEM system should provide a centralized dashboard for security analysts to monitor events, investigate incidents, and respond to alerts. The Solution should have role-based access control mechanism and handle the entire security incident lifecycle.
SIEM.REQ.0016	The SIEM system should integrate with external threat intelligence feeds to enrich its data sources and improve detection capabilities.
SIEM.REQ.0017	The system should have the ability to detect and analyze various types of threats such as malware, phishing, insider threats, and advanced persistent threats (APTs) by taking feeds.
SIEM.REQ.0018	Real-time alerting: The system should be able to generate real-time alerts based on predefined rules and policies. The alerts should be sent to the appropriate personnel/ role for further investigation and remediation.
SIEM.REQ.0019	Data retention: The system should be able to store log data for a predefined period of time. The retention period should be configurable based on the organization's requirements and compliance standards. Initially, solution should be sized to provide live storage for 6 months and archival data for 2 years
SIEM.REQ.0020	User access control: The system should provide granular access control to users based on their roles and responsibilities. It is desirable to support single sign-on (SSO) and two-factor authentication (2FA) for secure access if required.
SIEM.REQ.0021	The offered solution should be equipped with integration capabilities with offered active network & security devices from Day1
SIEM.REQ.0022	SIEM should be able to accept and process logs received from an external sources including offline media.
SIEM.REQ.0023	Reporting: The system should provide customizable reports on security events, threats, and compliance. The reports should be available in various formats such as XML, PDF, CSV, HTML etc.
SIEM.REQ.0024	The SIEM system should provide customizable reporting capabilities to meet specific organizational needs.
SIEM.REQ.0025	Threat intelligence: The system should have the ability to integrate with external threat intelligence sources such as feeds, databases, and APIs. The SIEM should be able to use this intelligence to identify potential threats and reduce the false-positive rate.
SIEM.REQ.0026	The SIEM system should support compliance requirements and reports as per the ISMS policy and industry standards like PCI-DSS, ISO 27000
SIEM.REQ.0027	The solution must have ability to add Asset Inventory details.
SIEM.REQ.0028	The system should generate reports and alerts for compliance and audit purposes.
SIEM.REQ.0029	The monitoring should be cross device and cross vendor and be both out of the box and scalable to cover additional devices and applications as required. All the Logs from all the sources should be managed and monitored from SIEM solution
SIEM.REQ.0030	SIEM Solution should have a common interface with UEBA solution to give analyst a consolidated view of investigation.
SIEM.REQ.0031	The solution should provide a data store using compression engine. The solution should compress the logs/ events by at least 90% for archival or the solution should be provided with suitable storage in order to store the logs for the duration mentioned in scope of work in RFP. In case the storage is found insufficient at a later stage for both options, an additional storage have to be provisioned to meet the requirements without an additional cost to the purchaser.
SIEM.REQ.0032	The solution should provide pre-defined report templates. The reports should

S. No.	Minimum Specifications
	also provide reports out of the box such as PCI- DSS, HIPAA, SOX, FISMA, ISO, SANS Critical Controls.
SIEM.REQ.0033	Reliability: The system should have high availability and fault tolerance to ensure continuous monitoring and protection. It should have built-in redundancy and failover mechanisms.
SIEM.REQ.0034	The SIEM system should have minimal impact on network performance.
SIEM.REQ.0035	Performance: The system should be able to process and analyze log data in real-time with minimal latency. It should support high throughput and low latency processing.
SIEM.REQ.0036	Scalability: The system should be able to scale to meet the organization's growing log volume and log sources. It should support distributed architecture and horizontal scaling. The device should be scalable to 150% of required performance of the scope considering future requirements
SIEM.REQ.0037	SIEM can be either a purpose build appliance / Software base / VM based. In any case, the OEM to provide all the required licenses, storage, infrastructure and all features without degrading the performance.
SIEM.REQ.0038	The solution should have an exhaustive incident tracking system that can track, investigate and resolve events in work- flow like environment
SIEM.REQ.0039	SIEM can be either a purpose build appliance / Software base / VM based. In any case, the OEM to provide all the required licenses, storage, infrastructure and all features without degrading the performance.
SIEM.REQ.0040	The solution should have an exhaustive incident tracking system that can track, investigate and resolve events in work- flow like environment
SIEM.REQ.0041	The SIEM system should be interoperable with different operating systems and environments such as cloud, on-premise, and hybrid.
SIEM.REQ.0042	SIEM should be able to connect the SAN storage to extract/forward to log archives using HBA/FC/SFP+ dedicated ports.
SIEM.REQ.0043	The solution should have a scalable architecture, catering multi-tier support and distributed deployment.
SIEM.REQ.0044	The solution should have capability of displaying of filtered events based on event priority, event start time, end time, attacker address, target address etc. The solution should support configurable data retention policy. The solution should provide capability for configuration backup and should support normalization of real time events.
SIEM.REQ.0045	The solution should provide a facility for logging events with category information to enable device independent analysis. The solution should ensure the integrity of logs. Compliance to regulations should be there with tamper-proof log archival.
SIEM.REQ.0046	No Events are dropped during Spikes (to sustain peak/ burst defined in the RFP), even If the License has been exceeded: The proposed solution must not, under any circumstances, drop incoming events. This is essential to ensure compliance/audit integrity and preserve necessary data to detect and mitigate threats during an attack or other unforeseen spikes in event volumes.
SIEM.REQ.0047	The solution should support collection of logs from all the devices quoted in HSDC network in the heterogenous environment. The Solution should be able to identify ports and services not necessary for normal government operations.
SIEM.REQ.0048	The solution should have native audit capability for end to end incident management. Complete audit trail of incident life cycle (like incident alerting, action taken by each user, final outcome of incident, closing of incident) should be maintained.
SIEM.REQ.0049	The solution should allow a wizard / GUI based interface for rules (including correlation rules for logs and packets) creation as per the customized requirements. The rules should support logical operators for specifying various conditions in rules.

S. No.	Minimum Specifications
SIEM.REQ.0050	The solution should support the following co- relation: Statistical Threat Analysis – To detect anomalies, Susceptibility Correlation - Raises visibility of threats against susceptible hosts, Vulnerability Correlation - Mapping of specific detected threats to specific / known vulnerabilities
SIEM.REQ.0051	The solution should also support historical correlation and have capability to analyse historical data using a new correlation rule and carry out trend analysis on collected data.
SIEM.REQ.0052	Solution should have capability to correlate based on the threat intelligence for malicious domains, proxy networks, known bad IP's and hosts. Proposed SIEM solution should have capabilities to collaborate core platform by bi-directional integration with SOAR . Desirable : Bidirectional Integration EMS/ ITSM etc.
SIEM.REQ.0053	The solution should offer a user interface that is capable of providing the Information Security team an intuitive way of using recognized network Solutions e.g. who is, nslookup, ping etc. to assist in analysis and response work.
SIEM.REQ.0054	The solution should have the capability to send notification messages and alerts through email, Syslog and Scripts, etc. The Solution should provide facility for separate alerting and reporting console for different asset groups.
SIEM.REQ.0055	The solution should be customizable to accept and process unknown log formats, the system should provide the ability to write a custom parser or filter for an unknown new event and a new log source. SIEM should have the ability to natively collect logs from logs sources.
SIEM.REQ.0056	The system should support, not restricted to, the following log and event collection methods: # Syslog – UDP and TCP # Flat file logs such as from DNS, DHCP, Mail servers, web servers etc. # Windows events logs – Agent-based or agent- less. # FTP, S/FTP, SNMP, ODBC
SIEM.REQ.0057	To avoid generating too many false positives, solution must provide a mechanism to deploy new correlation and evaluating them thoroughly before deploying in production mode. The solution should allow a wizard-based interface for rule creation. The solution should support logical operations and nested rules for creation of complex rules.
SIEM.REQ.0058	The proposed solution must have a software tool to allow customers to create integration with unsupported legacy or internally developed event sources. The software tool must allow customers to integrate with Syslog, log files, databases etc. and support the ability to parse multi -line log files.
SIEM.REQ.0059	The solution should be able to conduct agent less collection of logs except for those which cannot publish native audit logs. SIEM should have the ability to natively parse JSON formatted logs.
SIEM.REQ.0060	UEBA solution or equivalent solution should be able to natively/through API integrate with proposed SOAR & SIEM solution for monitoring users and reporting anomalies and It should take input from solutions such as SIEM, SOAR and other security solutions in Data Center. Should display RAW and Normalized packet headers or relevant data basis on which anamoly behaviour observed.
SIEM.REQ.0061	Solution should be ability to correlate identity information maintained in Identity Management System with the events generated in the network
SIEM.REQ.0062	Events should be enriched with contextual user information, such as: i. Which Identity caused the event to be generated? ii. What is their business or IT roll? iii. Do they have had the permissions to perform such activities?
SIEM.REQ.0063	Solution should be able to perfom/detect Privileged User Monitoring Suspicious activity User Activity Monitoring

S. No.	Minimum Specifications
	Shared Accounts Monitoring assign risk and credibility rating to events.
SIEM.REQ.0064	Monitor and report on role changes within the Identity Management System including when privileges are added or revoked.
SIEM.REQ.0065	Solution should be able to detect but not limit to Policy violations, Role violations, Location anomalies, Security Breach, Database access, etc.
SIEM.REQ.0066	Solution should be able to detect traffic from area of concern and risk user activity.
SIEM.REQ.0067	Solution should be ability to correlate identity information maintained in Identity Management System with the events generated in the network
SIEM.REQ.0068	Solution should be able to identify communication channel established between a compromised asset and an attacker-controlled server.
SIEM.REQ.0069	Proposed SIEM solution should consist un-obfuscated parsers natively available with SIEM to modify existing parser as when required by security operations team without any license or service challenges.
SIEM.REQ.0070	SIEM should have integrated GUI Dashboard for complete correlation, analysis and response from various source like UEBA and SOAR and other security solutions etc.. However, solution should be equipped with integration capabilities with offered network & security devices from Day1 to offer a common dashboard
SIEM.REQ.0071	The proposed SIEM solution must have at least 2 successful deployments in SOC/ Data Centre environments in India in Government/ Public Sector/ Scheduled Banks, monitoring with the capacity of 15,000 EPS+ in each of such deployments Customer Signoff/ satisfaction report required
SIEM.REQ.0072	Proposed SIEM solution should have capabilities to collaborate core platform by bi-directional integration with SOAR and UEBA.
SIEM.REQ.0073	OEM to provide training to HSDC team for complete solution management.
SIEM.REQ.0074	Proposed solution should ingest logs with sensitive information/ Personal Identification Information in secure way and should have options to selectively secure only requisite fields in logs only while preserving the format of the data.
SIEM.REQ.0075	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.31 APPLICATION PERFORMANCE MONITORING (APM)

S.No.	Minimum Specifications
APM.REQ.001	The proposed solution should be able to support 50 Web Servers , may have average 10 Application /DB instances in Data Centre environment.
APM.REQ.002	The proposed solution should be able to provide for each individual SQL statement, fired in a transaction, the count of average Rows returned and fetches. It should be able to baseline the performance of every SQL alert on deviation
APM.REQ.003	Solution should have a User Interface to present intuitive application dashboards presenting key metrics and easy navigation from Incidents to Events to relevant application traces
APM.REQ.004	Proposed solution should be able to measure every transaction along with count and response time for each step of the transaction flow and classify in buckets of response time.
APM.REQ.005	It should support end to end tracing for all major software like IBM WAS, AppConnect, MQ, WebLogic, Oracle DB, .NET, WebSphere, etc.
APM.REQ.006	It should support monitoring of all standalone java /Node.JS/Angular/etc. programs as well.
APM.REQ.007	Proposed solution should be able to allow creation of dashboards to show business transaction health and application response time for each and every transaction. The teams must be able to drill down to each of these transactions to see breakup of time spent on web server, application server, middleware, external components, and database tiers (whatever is part of the individual transaction). There should be no sampling. The monitoring tool must be able to capture the business KPIs from POST parameters, Method Arguments (as data objects or variables) Return Values, SOL Bind variables, etc.
APM.REQ.008	The solution should be able to perform post deployment auto discovery of all technology stack/ components and their dependencies. Without manual intervention. (i.e., It should be able to auto-instrument the applications and middleware (web and app servers, and Messaging Queues etc.).
APM.REQ.009	The solution should not make any functional change to application for capturing end user traces. The solution should not compromise any application security .
APM.REQ.0010	Proposed solution should provide full context across the applications and should automate monitoring, tracing and profiling for all applications and services.
APM.REQ.0011	Proposed solution should support monitoring of monolithic as well as cloud/virtualize native applications.
APM.REQ.0012	Proposed solution should provide event correlation of any service impact using a combination of dependency mapping and expert knowledge and should enable administrator to work on the fix right away without wasting valuable time filtering through numerous discrete events.
APM.REQ.0013	For alerting and notifications, proposed solution should support methods/ technologies such as email, Microsoft teams, Office365 etc.
APM.REQ.0014	Solution should expose all inter-dependencies between cloud/virtualize, infrastructure, and application components. Operators can immediately understand the upstream and downstream dependencies whenever an application or component has an issue.
APM.REQ.0015	Proposed solution should be an enterprise observability platform that should be capable to:
APM.REQ.0016	1. Continuously discover and maps all services
APM.REQ.0017	2. Ingest all performance metrics,

S.No.	Minimum Specifications
APM.REQ.0018	3. Trace all requests and profiles every process
APM.REQ.0019	4. Map all application dependencies automatically.
APM.REQ.0020	The solution should be able to provide application memory leak analysis, lock contentions, process crash analysis/process level visibility.
APM.REQ.0021	The proposed solution should be able to provide online auto analysis to identify which component or tier is contributing to slowness of the monitored transaction.
APM.REQ.0022	All required licenses should be PERPETUAL in nature and should have NO dependency on underlying hardware with 5 years On-site comprehensive Annual Technical Support from respective OEM

5.32 SECURITY ORCHESTRATION AUTOMATION AND RESPONSE (SOAR)

S.No.	Minimum Specifications
SOAR.REQ.001	SOAR platform must have at least 25+ ready Playbooks/ Runbooks/ templates out of the box playbooks with Manual Tasks, Automated Tasks and Conditional Tasks and reusable at same time there must be scope to customize and create new Runbooks. SOAR must integrate with SIEM to achieve the functionality of the desired solution as per RFP for SOC . SOAR capabilities within SIEM must not require any separate license and with no restriction on number of analysts. In case SOAR is not native or from different OEM, License should be proposed for 7 analysts. Solution licenses should facilitate the testing/ development separately without any additional cost. The solution must be a fully on-premise solution and should be provided with required Server Hardware in HA mode at DC and NL BCP. Hardware may be having 16 core CPU, 128 GB RAM, 1 TB SSD, NL-SAS Disk 4 TB and required OS or better in order to meet the desired parameters and SLA defined in this RFP. In case the required hardware is found slow or insufficient, the SI shall upgrade/augment in order to meet desired parameter without additional cost to purchaser.
SOAR.REQ.002	Proposed SOAR technology should have Threat intel platform inbuilt with OEM threat intel feeds and support for both commercial and open-source threat intel feeds both structured and unstructured. SOAR solution should collect real time global threat intel data, dedupe, aggregate, normalize, enrich, and process threat intelligence in a holistic and actionable manner.
SOAR.REQ.003	SOAR solution should have an inbuilt threat indicator repository which can be used for active threat hunting using automated playbooks. Threat indicator repository should be able to integrate with third party intelligence sources.
SOAR.REQ.004	Solution should have security orchestration and automated response engine bi-directionally integrated to reduce security incident MTTR (Mean Time To Respond) and automate L1/L2 security activities.
SOAR.REQ.005	Solution must track more than just IOCs, it focuses on attributes that are relevant to advisories/ alerts by Indian government regulatory bodies like CERT-in etc.
SOAR.REQ.006	SOAR solution should have an inbuilt threat indicator repository which can be used for active threat hunting using automated playbooks. Threat indicator repository should be able to integrate with third party intelligence sources.
SOAR.REQ.007	Solution should be equipped with reports which provide a comprehensive view of how threats operate, IOCs, key takeaways for the board, CISO, SOC, IT Ops, and Internal Auditing team.
SOAR.REQ.008	Runbook/ Playbook should be customizable, should be able to run automatic/ manual, listing exceptions. debugging, recording, adding adhoc tasks, versioning, scheduling etc. Solution should support updates for Playbooks
SOAR.REQ.009	Solution should have ability to suggest connections between incidents using machine learning like ability to suggest malicious phishing emails, analyst assignment, phishing incident prediction etc.
SOAR.REQ.0010	There should not be any restriction in number of remedial or response actions in the provisioned license.
SOAR.REQ.0011	Solution should be based on integration with feeds and should be configured with the used cases with automation for response to the basic threats like: 1 Blacklisted IP Communication 2 Possible Penetration Testing Activity 3 Connection to Known Malicious Actor in Published Host List

	4 DDOS Attack 5 Vulnerability scan detection 6 Phishing detection 7 Brute force attack 8 Malware /threat activity monitoring 9 Ransomware 10 Port & vulnerability Scans 11 Password cracking 12 Worm/virus outbreak 13 File access failures 14 Unauthorized server/service restarts 15 Unauthorized changes to firewall rules 16 Unauthorized ITSI access to systems
SOAR.REQ.0012	Solution should have capability to standardize/scale SLA management.
SOAR.REQ.0013	Solution should have capability to know and display which incidents are open, closed and neglected.
SOAR.REQ.0014	Solution should have capability to send the notifications to other team members.
SOAR.REQ.0015	Solution should have capability to generate, map / group the incidents its should be imported manually or Automatically (e.g. REST API, Syslog, email…)
SOAR.REQ.0016	Solution must provide tickets management.
SOAR.REQ.0017	Solution must enable to delegate tasks to another user and to assign due dates
SOAR.REQ.0018	Solution should support- documentation of evidence along with time stamping, tasks information, and searching.
SOAR.REQ.0019	Solution should support collaboration within the platform in the defined workflow.
SOAR.REQ.0020	The solution must be web based
SOAR.REQ.0021	Solution should support integration with but not limited to the following technologies: Incidents Forensics, IT (e.g. AD, SAML...) Communication tools (e.g. email, Slack, Hipchat…) SIEM tools Endpoint Security Network Security Active Directory Threat Intelligence Dynamic malware analysis
SOAR.REQ.0022	Solution should provide role-based access control for all the data & modules to have different access for different members of the team
SOAR.REQ.0023	Should support multi-factor authentication
SOAR.REQ.0024	Solution should have capabilities to automatically harness the critical IOC and map it back to MITRE ATT&CK navigator relevant TTP.
SOAR.REQ.0025	Solution must support Threat Intelligence sharing format/protocols such as STIX/TAXII but not limited to.
SOAR.REQ.0026	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.33 ELEMENT MANAGEMENT SYSTEM/ NETWORK MANAGEMENT SYSTEM (EMS/NMS)

S.No.	Minimum Specifications
EMSNMS.REQ.001	The proposed EMS solution should be an integrated, modular, and scalable solution : 1. Fault & Performance Monitoring (Network, Server, Cloud, VMs, Wi-Fi, all IP network) 2. Network configuration & Change management 3. Traffic analysis 4. Assets Management 5. Reporting & Dashboarding with integration 6.. Helpdesk ITSM Tool
EMSNMS.REQ.002	The system should be accessible via a Web based GUI console/portal from intranet as well as from internet.
EMSNMS.REQ.003	The required hardware and software solution should include the required licenses with update and upgrades in DC & NLBCP in Active Passive mode. The required hardware, software, OS etc.(along with appropriate license) to run the solution in order to meet the performance parameters defined in the scope to be provided as part of solution
EMSNMS.REQ.004	OEM/OEM authorised implementing partner should customize and configure for onsite deployment of proposed solution as per the project and requirement of the organization and onsite support of 3 months should be provided for smooth functioning of the solution. OEM /OEM authorised implementing partner to provide onsite training to HSDC team for complete solution management.
EMSNMS.REQ.005	The proposed EMS solution should be an integrated and scalable solution, accessible from a single pane of glass for KPI insights across the entire IT environment. This dashboard will provide service status, performance view, response-time data etc based on role-based access. Since the operations manager solution provides a single framework for streaming metrics across systems, applications, networks, topology & event data, the operations manager must be FIPS 140-2 /FIPS/ STQC certification for trusted supply chain compliance complaint, which ensures that cryptographic-based security systems are to be used to provide protection for sensitive or valuable data. In case, offered EMS solution has no requisite certification, the product with same configuration/size must be running in atleast 5 state data centre and the OEM must also submit customer satisfactory report for the same along with contact details of the customer.
EMSNMS.REQ.006	To ensure the mature security standard of proposed EMS solution, SI must ensure that the proposed EMS solution is recognised and certified in industry.
EMSNMS.REQ.007	All the management modules shall be customized to be accessed from a common unified dashboard to provide a single pane of glass view for KPI insights. This dashboard will provide service status and restricted views, along with drill down navigation capability. This Business Service Dashboard should also embedded capabilities to display real-time status of Infrastructure (NOC) metrics such as response time, service availability, health, SLA violations, Incident and more for quick insights.
EMSNMS.REQ.008	The proposed solution should have at least 3 deployments (in

S.No.	Minimum Specifications
	state/central Government/ PSU/National BFSI/ National TSPs) in India with two deployments of 2500+ (50%) devices and one deployment of 5000+ (100%) being monitored in each of these deployments in last seven years. Customer names, solution details and copy of Implementation completion/sign-off for all the projects must be submitted by the OEM.
	Performance Monitoring Management
EMSNMS.REQ.009	The proposed Enterprise Management tools must be able to monitor end to end performance of Server Operating Systems & Databases and Should be able to manage distributed, heterogeneous systems – Windows, UNIX & LINUX from a single management station.
EMSNMS.REQ.0010	There should be a managed node that provides the system performance data, and for event management and 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
EMSNMS.REQ.0011	The proposed Enterprise Monitoring Solution must also be integrated with SMS Gateway as well as Email.
EMSNMS.REQ.0012	Solution should provide alarm correlation and facilitate reduction of total number of alarms displayed by means of intelligent alarm correlation, suppression and root cause analysis techniques built into the system. The system must ensure reduction in MTTR by means of advanced event correlation, filtering, and root cause analysis.
EMSNMS.REQ.0013	The proposed Alarm Correlation and Root Cause Analysis system shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network components. The current performance state of the entire network & system infrastructure shall be visible in an integrated console.
EMSNMS.REQ.0014	It should have capability to perform cross domain correlation with alarm correlation from Network Monitoring tool, Systems monitoring tool, application performance monitoring tool and other domain monitoring tools.
EMSNMS.REQ.0015	The proposed solution should provide out of the box root cause analysis.
	Automation and Patch Management
EMSNMS.REQ.0016	The proposed solution should provide unified lifecycle management across heterogeneous virtual & physical servers and network, in the most diverse IT environments including provisioning(by Adding,Modifying the devices), compliance audit and closed-loop remediation and patch management (either as a single OEM solution or by having third party tool to have a integated solution).
EMSNMS.REQ.0017	The solution must support remote desktop connections in the heterogenous environment and provide direct connections to servers ,network and security using communications channel with enhanced security features, audit logs, and access control policies in Data Center either out of box or supplied with third party integrated software.
EMSNMS.REQ.0018	Will support audit and remediation against industry best practice content and should havebuilt-in audit and compliance policies for industry best practices/ Gov. regulations.
EMSNMS.REQ.0019	Workflow Automation - The proposed orchestration solution provide at least 1000 workflows for automation use cases
	Network Fault Monitoring & Performance Management

S.No.	Minimum Specifications
EMSNMS.REQ.0020	The Network Management function must monitor performance across heterogeneous networks from one end of the enterprise to the other.
EMSNMS.REQ.0021	The solution should allow for discovery to be run on a continuous basis which tracks dynamic changes near real-time; to keep the topology always up to date. This discovery should run at a low overhead, incrementally discovering devices and interfaces.
EMSNMS.REQ.0022	NMS should provide integrated fault, performance Monitoring, Configuration & compliance Management together in one tool.
EMSNMS.REQ.0023	NMS should support Industry-leading support for physical, virtual, and SDN-enabled devices
EMSNMS.REQ.0024	NMS should support out of the box monitoring of at least 5000+ devices in the enterprise network. Tentative classification of devices and respective tentative quantities may be considered as under which may vary at the time of installation and commissioning : SNMP/ICMP Devices- 3200 (Approx) Physical Servers -200 (Approx) Virtual Servers - 1000 (Approx) Databases - 50 (Approx) Remaining - for future use
EMSNMS.REQ.0025	Diagnostic Analytics providing change-Correlated Performance Views and should show the difference either in either a side-by-side, or line-by-line presentation
EMSNMS.REQ.0026	The solution should provide discovery and topology capability along with role based /profile based access thus enabling network administrator to get complete respective view of the nodes and network(Topology Diagram).
EMSNMS.REQ.0027	It should support various discovery protocols to perform automatic discovery of all L2, L3 Network devices across Network.
EMSNMS.REQ.0028	The tool shall be able to discover IPv4 only, IPv6 only as well as devices in dual stack. In case of dual stack devices, the system shall be able to discover and show both IPv4 and IPv6 IP addresses.
EMSNMS.REQ.0029	The tool shall be able to work on SNMP V-1, V-2c & V-3 based on the SNMP version supported by the device. It shall provide an option to discover and manage the devices/elements based on SNMP as well as ICMP.
EMSNMS.REQ.0030	The proposed solution must provide a detailed asset report, organized by vendor name, device type, listing all ports for all devices. The Solution must provide reports to identify unused/dormant Network ports in order to facilitate capacity planning
	Network Configuration Management
EMSNMS.REQ.0031	The system should be able to clearly identify configuration changes / policy violations / inventory changes across heterogenousenterprise network.
EMSNMS.REQ.0032	The system should support secure device configuration capture and upload and thereby detect inconsistent configurations and alert the administrators.
EMSNMS.REQ.0033	The proposed system should be able to administer configuration changes to network elements by facilitating to automate the following administrative tasks of effecting configuration changes to network elements: a) Capture running configuration; b) Capture start-up configuration; c) Upload configuration; d) Write start-up configuration; e) Upload firmware

S.No.	Minimum Specifications
EMSNMS.REQ.0034	The proposed fault management solution must be able to perform real-time or scheduled capture of device configurations.
EMSNMS.REQ.0035	NMS should provide unifies incident information, detailed performance troubleshooting data, and change data for configurations and running state diagnostics all in a single operational dashboard.
EMSNMS.REQ.0036	The propose solution should have diagnostic analytics capability that able to visually correlate performance and configuration changes of all network issues.
	Service/ Helpdesk
EMSNMS.REQ.0037	Should be able to support and handle large volume of incident, service requests, changes, etc. and be able to integrate with third party IVR or CTI.
EMSNMS.REQ.0038	The solution should have a single CMDB across ITSM and Asset Management system.
EMSNMS.REQ.0039	The solution should have a Single Architecture and leverage a single application instance across ITIL processes, including unique data and workflows segregated by business unit, cost centre, and user role for Incident, Problem, Change, Release, Knowledge Management, Asset Management and CMDB.
EMSNMS.REQ.0040	Solution should support multi-tenancy with complete data isolation as well as with ability for analysts based on access rights to view data for one, two or more organizational units.
EMSNMS.REQ.0041	The solution should provide to browse through CMDB which should offer powerful search capabilities for configuration items and services, enabling to quickly find CIs as well as their relationships to other CIs.
EMSNMS.REQ.0042	Beyond mobile iOS and Android apps, Self Service App should be available on any device with an HTML5 browser.
EMSNMS.REQ.0043	Should provide data analysis methods for insight and value to service desk by leveraging unstructured as well as structured data.
EMSNMS.REQ.0044	Tool Analytics should be completely configurable in terms of source data and results, enabling Process Managers and other IT Users to proactively identify trends that can be used to drive action. Multiple instances shall be allowed to be configured in different ways in different modules for different outcomes.
EMSNMS.REQ.0045	The tool should allow the user to take a screenshot of the error message and sends it to the service desk. The user can type in a couple of text lines to describe the error in simple language. The service desk agent then can pick up the ticket with the information already filled in (category, impact, and assignment).
EMSNMS.REQ.0046	The tool should have the knowledge management OOB – knowledge databases to support investigations, diagnoses, root cause analysis techniques, and creating / updating workarounds, temporary fixes and resolutions.
EMSNMS.REQ.0047	Integrates with any underlying ITIL and ITSM services including Service Desk, Change Management, Service Level Management and CMDB for request fulfilment.
EMSNMS.REQ.0048	The solution should have the ability to operate all functionality available in the incident, problem/change /request, assets etc. via a mobile app on iPhone or Android phone.
	Inventory Management
EMSNMS.REQ.0049	Discovery should work agentless (that is, agent-less discovery) while

S.No.	Minimum Specifications
	discovery Layers 2 through Layers 7 of OSI model.
EMSNMS.REQ.0050	Should use Industry-standard protocols such as WMI, SNMP, JMX, SSH to perform discovery without requiring the installation of an agent.
EMSNMS.REQ.0051	Discovery system should have the ability to capture configuration for the purposes of comparison and change tracking.
EMSNMS.REQ.0052	Discovery system should be capable of supporting role-based access to various aspects of CMDB administration.
EMSNMS.REQ.0053	Discovery should be object-oriented, allowing specific CIs and relationships to be discovered using a library of discovery patterns.
EMSNMS.REQ.0054	Discovery engine should gather detailed asset and configuration item (CI) information for specific servers and the applications running on them.
EMSNMS.REQ.0055	Solution should dynamically discover and continuously map IT hardware inventory and service dependencies.
EMSNMS.REQ.0056	Discovery system should have ability to discover any device connected to. If not detected, it must have the capability to create/modify discovery scripts as per requirement of the organization
EMSNMS.REQ.0057	Solution should provide a portal to search Configuration Items using natural language understanding.
EMSNMS.REQ.0058	Proposed Tool should support discovery of virtual environment
EMSNMS.REQ.0059	Solution should maintain the discovery of historical data as well as up to date information and also detect the asset changes.
	Asset Management
EMSNMS.REQ.0060	The proposed Asset Management solution should evolve on a common, expandable platform - IT Service Management, Asset Management, Software Asset Management
EMSNMS.REQ.0061	The proposed Asset Management solution should consolidate, end-to-end lifecycle management of IT hardware and software assets.
EMSNMS.REQ.0062	The proposed Asset Management solution should provide Software Asset Management Compliance Dashboards.
EMSNMS.REQ.0063	The proposed Asset Management solution should provide Software Asset Management feature and be configurable on both Vendor specific predefined and other third party/custom license rules and metrics , Vendor audits risk avoidance and Compliance management though dashboards and reporting
EMSNMS.REQ.0064	The proposed Asset Management solution should have hardware, portfolio, contract, vendor, procurement, and financial management–all included.
EMSNMS.REQ.0065	The proposed Asset Management solution should have natively built-in CMDB and IT discovery as OEM solution.
EMSNMS.REQ.0066	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support
EMSNMS.REQ.0067	15 concurrent user shall be required as part of EMSNMS and provision to add multiple users working in shift. Note : EMSNMS.REQ.0024 : EMS& NMS should support out of the box monitoring of at least 5000+ devices in the enterprise network

Note : SMS GateWay and Email Gate Way will be provided by CRID

5.34 DISTRIBUTED DENIAL-OF-SERVICE (DDOS)

S.No.	Minimum Specifications
DDOS.REQ.001	Proposed Solution should provide protection from both State-full and Stateless DDOS attack at HSDC and NL BCP site. Solution should support inbuilt /External Fail-Open (pass-through mode) options for Hardware and Software Bypass feature for all interfaces to achieve faster network convergence in Resilient Deployment. Solution must be supplied with sufficient RAM to meet and sustain the specified performance parameters along with minimum 240GB Hard disk capacity and the solution to have the capacity to store complete logs for minimum 3 months period from day1.
DDOS.REQ.002	Proposed appliance must be purpose built DDoS prevention system and should be stateless technology not having any kind of state limitation such as TCP connections etc. Proposed appliance should be a dedicated appliance based solution.
DDOS.REQ.003	System should have a Scalable Clean/ legitimate Throughput License approach for Legitimate Traffic. System should support Clean/legitimate Throughput License of 20 Gbps from day 1 and scalability with a license upgrade upto 40 Gbps over next 5 years without changing the appliance
DDOS.REQ.004	Solution should inspect ,detect and mitigate IPV4 & IPv6 Attacks and Solution should Detect and Mitigate DDoS on application protocols in the network like HTTP/DNS/VoIP/Mail/VPN/File/Login along with Layer 3 and Layer 4 Protocols including L3 Floods, Sate Exhaustion, Reflection and Amplification and Low and Slow attacks. Solution should inspect ,detect and mitigate IPV4 & IPv6 Attacks
DDOS.REQ.005	Solution should be transparent bridge to pass 802.1Q tagged frames and other control protocols like VLAN and In inline mode system must not modify MAC or IP addresses of passed frames
DDOS.REQ.006	System should support Multiple Segment protection for up to 4 Segments
DDOS.REQ.007	The device operating system should be hardened and the responsibility shall fall on OEM to ensure the same
DDOS.REQ.008	Proposed appliance should support minimum of 24 Million packet per seconds on the same appliance should support latency less than 90 microseconds. Latency should be documented in datasheet/ public portal
DDOS.REQ.009	System should support minimum 8 x 10/1 G, 2x 100 G Fibre protection ports from day 1. All the protection ports should support inbuilt/ external Hardware and Software Bypass with Fail-Open mode.
DDOS.REQ.0010	Should Support dual redundant Hot-Swappable AC power supplies from day one
DDOS.REQ.0011	Solution should support SNMP v2/v3 MIB and Traps and Solution must support REST API management and Integration with RADIUS and TACACS+ along with Device should integrate with DCs existing SIEM engine seamlessly through Syslog messages (CEF,LEEF).
DDOS.REQ.0012	System should provide and use its own threat intelligence feeds with capability to consume and integrate with 3rd Party feeds (IOCs)
DDOS.REQ.0013	The system must have a dedicated management port/ console port for Out-of-Band management; Management interfaces must be separated from traffic interfaces. System management must not be possible on traffic interfaces, management interfaces must not switch traffic. Proposed solution should have inbuilt GUI based monitoring, configuration management, diagnostics and reporting.
DDOS.REQ.0014	The system must support configuration via standard up to date web browsers. System user interface must be based on HTML. Solution should support Configuration and Login Audit trails and Solution should support Role/User Based Access Control and reporting functionality.System should have mechanism to upgrade the firmware and application
DDOS.REQ.0015	Quoted OEM should have Technical support in India and the organization should be

S.No.	Minimum Specifications
	able to raise TAC support with/without the involvement of partner.The proposed DDoS solution should not reach End of Support within 5 years from the date of submission of bid.
DDOS.REQ.0016	OEM Anti-DDoS Solution should have been deployed and used in at least 3 State Data Centers/ Data Centers in Government/ PSU/BFSI/ ISP in India.
DDOS.REQ.0017	The solution shall provide real time dashboard displaying statistics on data such as total traffic, passed/blocked, top IPs/services/domains, attack types, top sources by IP location (Geo IP) and blocked sources, etc.
DDOS.REQ.0018	OEM should have their own Threat Research Team that should provide a Threat Intelligence feed as part of the solution. Threat Intelligence Feed should contain IOC to block Emerging Threats, Active DDoS vectors, Cyber Threats like Malware, APTs, Botnet C&C, Scanning and Brute-force attacks. This feed should be automatically updated in the appliance at a configurable interval.
DDOS.REQ.0019	Should support user customizable/user defined Signature or Filters or Payload/Header based regular expressions and System should allow to write manual ACL's to block IP's
DDOS.REQ.0020	System should restrict the IP address from specific segment like from TOR network and Proposed appliance should be able to block traffic based on Geo location feed that is updated automatically at configurable intervals
DDOS.REQ.0021	The system must be able to block invalid packets (including checks for Malformed IP Header, Incomplete Fragment, Bad IP Checksum, Duplicate Fragment, Fragment Too Long, Short Packet, Short TCP Packet, Short UDP Packet, Short ICMP Packet, Bad TCP / UDP Checksum, Invalid TCP Flags, Invalid ACK Number) and provide statistics for the packets dropped. Solution should also support packet Anomaly Protection.
DDOS.REQ.0022	System should support suspension/dynamic suspension of traffic from offending source based on a signature detection, host behavioural analysis, malformed packets, payload expression matching
DDOS.REQ.0023	The system must support Connection limit option to limit number of new connection on per source basis or in range or equivalent.Solution should support Automatic adaptive thresholds estimation for critical L3, L4 and L7 parameters
DDOS.REQ.0024	System should have capabilities for immediate mitigation of flood attacks—protecting against known and unknown DDoS attacks without manual intervention.
DDOS.REQ.0025	System must be able to detect and mitigate any type of Spoofed SYN Flood attacks and should support different mechanisms or equivalent for the same.
DDOS.REQ.0026	Solution should support deployment for all DNS flood detection and mitigation (especially for random sub-domain attack),Should support IOC Types - IP Address, Fully Qualified Domain Names, URLs
DDOS.REQ.0027	System must be able to detect and block HTTP and HTTPS GET/POST Flood and should support mechanisms like: a) HTTP and HTTPS Header Regular Expressions b) HTTP and HTTPS Rate Limiting c) Rate-based Blocking
DDOS.REQ.0028	Solution should support mitigation of Burst Attacks using mechanisms like source Rate-Based Blocking, Flexible Rate-based blocking, Signature or equivalent and The system must limit number of simultaneous TCP connections on a per-client basis
DDOS.REQ.0029	The system must support the dropping of idle TCP sessions if client does not send a user-configurable amount of data within a configurable initial time period and should dynamically blacklist the offending sources.
DDOS.REQ.0030	System protects from DDoS attacks behind a CDN by surgically blocking the real source IP address
DDOS.REQ.0031	System should Mitigate Encrypted attacks and should support traffic with minimum of 50,000 SSL CPS measured with RSA 2K keys or 33,000 TPS with ECC ECDSA P-256. System protects against SSL/TLS Encrypted DoS and DDoS threats both at the

S.No.	Minimum Specifications
	SSL/TLS Layer and HTTPS layer
DDOS.REQ.0032	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.35 ENDPOINT PROTECTION SOLUTION (EPP)

S. No.	Parameter	Minimum Specifications
EPP.REQ.001	**Security Modules**	Firewall, Application Control, Anti-Malware, Ransomware Protection, Behavioral Protection, ML Models for Static Analysis, Anti-Bot, Web Browsing Protection, Exploit Prevention, EDR 1.The Forensics Analysis component and clauses requirements (Req.0064 to Req.0071) stands deleted. 2. Specifications related to sandboxing (Req.0078,80,81,82) stands deleted
EPP.REQ.002	**Supported OS**	Supported OSs: Windows clients: Windows 10 and higher versions; Mac OS: 10.15 and higher versions, Linux
EPP.REQ.003	**Deployment Platform**	Solution must support on-prem and remote clients regardless of network Solution must use provide modern and easy remote deployment/installation/uninstallation methods. The solution must have the ability for remote Installation and client deployment. The solution must securely register a new client installation to the management server. The solution must allow to manage the agent version and components from the management interface. The management solution should support either a full client or thin web based client The solution must support authentication for administrator login. The solution should be able to provide real time email alerts
EPP.REQ.004	**Anti Malware Security Feature**	Proposed solution should defends endpoints against malware, ransomware, malicious scripts also support Pre-execution and runtime machine learning to detect and mitigate threats along with File reputation - Variant protection - Census check - Web reputation
EPP.REQ.005		Proposed solution should have True file type scan along with proactive outbreak prevention and Command & Control callback detection supporting IPv4 and IPv6 environments
EPP.REQ.006		Defends endpoints - on or off the corporate network - against malware, Trojans, worms, spyware, ransomware, and adapts to protect against new unknown variants and advanced threats like crypto malware and fileless malware.
EPP.REQ.007		Ransomware rollback: Detects ransomware with runtime machine learning and rules to block encryptionprocesses. Rollback/restores any files by taking backup of ransom ware encrypted files and restoring the same before detection.
EPP.REQ.008		The proposed solution should be able to detect the vulnerabilities in any file and assure analysis precision and analysis efficiency.
EPP.REQ.009		Should detect from Targeted and known ransomware attacks, malware and document exploits, Attacker behavior and network activity, Web threats, including exploits and downloads, Phishing, and other email threats, Data

S. No.	Parameter	Minimum Specifications
		exfiltration, Bots, Trojans, worms, keyloggers and Disruptive application
EPP.REQ.0010		Should have capability to do retrospective scan on CnC, Script Analyzer, automatically send executable to virtual analyzer and can crack password protected compressed files
EPP.REQ.0011	**Data Leakage Prevention**	Should have data loss prevention capability with pre-defined templates complying to IT Act 2000 and other MeitY/ CERT-IN guidelines and should have capability to create policies on basis of regular expression, key word and dictionary based
EPP.REQ.0012		Should empower to impose policies for the use of file attributes, removable media with device control for devices like USB drive, Bluetooth, WI-FI/mobile hotspot, USB attached mobile devices etc.
EPP.REQ.0013		Should have granular device control with the following control actions: Read only, Read and write, Read, write and execute
EPP.REQ.0014		Should offers visibility and control of data in motion of sensitive information—whether it is in email, webmail, instant messaging (IM), and most networking protocols such as FTP, HTTP/HTTPS and SMTP.
EPP.REQ.0015		Detect data-stealing malware: Identify botnets, hidden FTP processes, keyloggers, spyware, and Trojans that attempt to collect and send data.
EPP.REQ.0016	**Application Control**	Prevents potential damage from unwanted or unknown applications (executables, DLLs, Windows App store apps, device drivers, control panels, and other Portable Executable (PE) files).
EPP.REQ.0017		Should allow users to install valid and safe applications with policy deployed at Administrator level.
EPP.REQ.0018		Whitelisting and blacklisting of approved applications in Data Center environment (with regular updates)
EPP.REQ.0019	**Vulnerability Protection**	Endpoint vulnerability protection should scan the machine and provide CVE number visibility and accordingly create rule for virtual patch against vulnerability or Endpoint vulnerability protection and malware scanning engine should protect the systems from the vulnerabilities and exploits introduced in the endpoint systems.
EPP.REQ.0020		Should be capable of recommending/ creating rules based on vulnerabilities on endpoint and create dynamic rules automatically based on System posture and endpoint posture
EPP.REQ.0021		Blends signature-less techniques, including high-fidelity machine learning, behavioral analysis, variant protection, exploit prevention, and good file check with other techniques like file reputation, web reputation, and command and control (C&C) blocking.
EPP.REQ.0022		Should performs static and dynamic analysis to identify an object's notable characteristics: Auto start or other system configuration, Anti-security and self-preservation, Deception and social engineering, File drop, download, sharing, or replication, Hijack, redirection, or data theft, Malformed, defective, or with known malware traits, Process, service, or memory object change and Rootkit, cloaking, Suspicious network or messaging activity
EPP.REQ.0023		Should protect storage devices, Data Systems storage

S. No.	Parameter	Minimum Specifications
		systems etc.
EPP.REQ.0024		Solution should support encryption of data indisk, file folder, USB, and removable media to protect from any kind of ransomeware infections.
EPP.REQ.0025		Should have common management console to manage all EPP capabilities defined in the RFP.
EPP.REQ.0026	**Endpoint Detection and Response**	• Investigation and IOC Sweeping • Patient Zero ID / Root Cause Analysis and IOA Behaviour Hunting/Detection • API's for query / automation and Unknown file guidance • Variant Protection to detects mutations of malicious samples by recognizing known fragments of malware code • Packer Detection to Identifies packed malware in memory as it unpacks, prior to execution • Runtime Machine Learning scores real-time behaviour to detect previously unknown threats • IOA Behavioural Analysis detects behaviour that matches known indicators of attack (IOA), including ransomware encryption behaviours, script launching • In-memory runtime analysis malicious script detection, malicious code injection, runtime un-pack detection • Isolation, Quarantine, Process kill, Execution block • Provides context-aware endpoint investigation and response (EDR), recording and detailed reporting of system-level activities to allow threat analysts to rapidly assess the nature and extent of an attack. Custom detection, intelligence, and controls • Record detailed system-level activities and perform multi-level search across endpoints using rich-search criteria such as Open IOC/ Yara, and suspicious objects. • Detect and analyse advanced threat indicators such as fileless attacks. • Root cause analysis for simple or full "kill chain • Search by multiple parameters by OpenIOC rule for disk scans and Yara rules for memory scans
EPP.REQ.0027	**Firewall**	The solution will enforce system Firewall rules to allow or block network traffic to endpoint computers based on connection information, such as IP addresses, ports, and protocols.
EPP.REQ.0028		The solution should also support IPV6 network.
EPP.REQ.0029		The solution must include an option for Host Isolation to isolate or allow a specific host (access to network) that is under malware attack and poses a risk of propagation.
EPP.REQ.0030	**Detection**	Solution must continuously collect system events necessary for detection and analysis.
EPP.REQ.0031		Solution must continuously monitor and report findings as quickly as possible. If an endpoint cannot immediately report findings, results must be stored locally until they can be uploaded to the solution's central management system
EPP.REQ.0032		Solution must allow for real-time alerting or logging of notable events based on custom content (behaviours) or indicators of compromise
EPP.REQ.0033		Solution must provide a way to ensure process information, metadata, network connections, binaries etc.
EPP.REQ.0034		Solution must be able to graphically demonstrate system

S. No.	Parameter	Minimum Specifications
		activity (process trees or other type of mapping interface) to aid in investigations
EPP.REQ.0035		Solution must capture detailed metadata around binaries and processes that are executed on endpoints.
	Forensics	
EPP.REQ.0036		Forensic report will automatically identify the malicious activity entry point and highlight the potential damage, remediation action and the entire chain of attack.
EPP.REQ.0037		The solution will enhance third-party anti-malware or security detections by automatically building and visualizing an incident report
EPP.REQ.0038		The Forensics report will log, present and un-obfuscate PowerShell scripts used during an attack.
EPP.REQ.0039		The solution will list reputation analysis on files, URLs and IPs used during an attack. The solution will show IP Geolocation as part of the reputation information.
EPP.REQ.0040		The solution will be able to follow indirect methods of execution used by malware like WMI calls and Injections to be able to trace the activity of more advanced malware.
EPP.REQ.0041		The solution will create an incident report that will display the incident in terms of the Mitre ATT&CK Matrix.
EPP.REQ.0042	**Reports**	The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behaviour, Lateral Moment, Asset and data discovery and data Exfiltration.
EPP.REQ.0043		Proposed solution should be able to provide access information about Affected Hosts on the following views: Displays a summary of affected hosts by attack phase, provides access to Host Details views and Displays host event details in chronological order
EPP.REQ.0044		Should provide Threat execution and evaluation summary and In-depth tracking of malware actions and system impact, including the following: Network connections initiated, System file/registry modification and System injection behaviour detection
EPP.REQ.0045	**Support**	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support
EPP.REQ.0046	**Implementation**	The OEM should implement/configure management platform of proposed Endpoint Security solution following best practices considering current threat landscape and desired features.
EPP.REQ.0047		The solution should showcase affected process, affected registry keys & affected files in OS environment
EPP.REQ.0048	**Logs**	The solution should be able to log the C&C communication from the emulated BOT file.
EPP.REQ.0049	**Web Browsing Protection**	The solution must block the user from browsing to a known malicious URLs or domains.
EPP.REQ.0050		The solution must provide URL filtering/ web reputation services with additional Black/White listing
EPP.REQ.0051		The solution must ensure safe searching with the Google, Bing and Yahoo search engines
EPP.REQ.0052		The user must not be able to tamper any kind of settings deployed from the management server/ Administrator server in any way
EPP.REQ.0053		The solution must be able to identify zero-days files even if

S. No.	Parameter	Minimum Specifications
		they are not familiar with any reputation service
EPP.REQ.0054		Any ML models used by the endpoint should be frequently updated in order to protect against fresh, zero-days attacks
EPP.REQ.0055	**ML Models for Static Analysis**	The solution's Static Detection Engine must monitor the access to files
EPP.REQ.0056		The solution must check the reputation of files based on ssdeep / Fuzzy hashing or equivalent.
EPP.REQ.0057		The solution will leverage multiple sensors to effectively and uniquely identify generic malware behaviours as well as malware family specific behaviours.
EPP.REQ.0058		The solution will immediately prevent or detect on malicious behaviours regardless if the machine is online or offline
EPP.REQ.0059		The solution will detect and prevent fileless attacks only utilizing Windows processes.
EPP.REQ.0060	**Behavioural Protection**	The solution should detect malicious LNK (Windows Shortcut) files.
EPP.REQ.0061		5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.36 NETWORK DETECTION AND RESPONSE (NDR)

S.No	Minimum Specifications
NDR.REQ.001	Solution should provide visibility on historical attacks up to 1 months. It should perform contact tracing for the attack cycle up to the paitent zero. It should provide packet level back in time investigation up to 5 days.
NDR.REQ.002	Proposed solution should support open/restful APIs for integration with security stacks.
NDR.REQ.003	Should provides a powerful and scalable frontline defense mechanism that protects networks from known threats and relies on full packet capture from various segment including north-south and east-west communication.
NDR.REQ.004	Should support deployment of multiple sensors/probes to acquire data from multiple sources in the network, multiple systems/appliances running analytics engine components for better assessment of traffic to security profiles, multiple systems/appliances with deep-learning/machine-learning components for anomaly detection and, multiple systems/appliances with web-UI components supporting high-availability and scalability needs. Data should not be shared to cloud outside the organization for any security analytics.
NDR.REQ.005	Should utilize full packet capture to perform the behavioural analysis, heuristic analysis and should support its own intelligence feed along with third party intelligence feed (if required) support.
NDR.REQ.006	Solution should be scalable DPI supporting multiple protection group/ security profiles for monitoring critical assets of the oragnization including servers, host, IP addresses etc.
NDR.REQ.007	Solution should have real-time packet capture with following options for security analytics purpose • Capture the entire packet • Slicing the size of packet • Packet Truncation • Exclude specific packets • Capture only headers • Deep Parsing • correlation of the collated traffic data from different sources • Categorization of traffic based on source/destination IP, Ports and Applications • User Defined criteria
NDR.REQ.008	The Network Capturing System can be a Purpose Build Hardware Appliance with Application and required Licenses Loaded or a software based solution in order to meet all the performance parameters including the ports/ storage defined below as a part of the solution: > Should have at least 02 Nos Ports of 10GbE Packet Capturing ports loaded with High Performance SFP+ > Atleast 02 Nos of Gigabit Ethernet Ports for Management and Network Connectivity (Ready to use) and provide feature for remote management > Should able to receive packets aggregated from the SPAN/TAP/Packet broker etc. > Storage should be sufficient to store the Packet level information (required for investigation & forensics as per specifications) for a period of at least 05 Days at the packet flow bandwidth/ handling utilization of 10 Gbps Tapped / Mirrored / SPAN from various network points.

S.No	Minimum Specifications
NDR.REQ.009	Solution should look for potential risks in the organization and provide continuous audit of the network. For example, known insecure application such as Rlogin, telnet, risks for various certificated installed on the servers. It should be able to provide insight if the certificate is self-signed or third-party certificate and also should be able to alert if any certificate is going to expire.
NDR.REQ.0010	Solution should be detecting threats, trace interconnected devices, view historical usage, and assist in orchestrating mitigation through API and should be able to utilize protection groups to classify networks, servers, and services based on risk, allowing for very rapid and concise verification of zero trust adoption.
NDR.REQ.0011	Solution should be able to quickly identify reconnaissance, look back in time within minutes through a detailed history of both good and nefarious activity and contact trace where the network traffic came from
NDR.REQ.0012	Should be pre-built with hundreds of reports, graphs, and charts, which are all customizable. should be able to spot users or devices downloading large volumes of data, bandwidth usage by Application.
NDR.REQ.0013	Should be able to monitor from L2 to L7 layer metrics conversations in the network and should integrate with log management tools for sharing of network data in real time and, alerts as they happen. To block/recommend to block any active CnC communication or any ongoing data exfiltration. The offered solution should be equipped with integration capabilities with offered active network & security devices (to block traffic) from Day1.
NDR.REQ.0014	Should include a distributed search engine data-store to ingest various types of textual, numerical, geospatial, structured and unstructured data and should allow for proactive investigation by allowing user to interact with data using visual graphs/charts in interactive dashboards.
NDR.REQ.0015	Should allow for proactive detection by allowing user to interact with data using visual graphs/charts in interactive dashboards. Should enable user to detect network security issues by accessing details about session. The details may pertain to delays, gaps, session initialization or termination reasons, session payload and data enrichments.
NDR.REQ.0016	Should consist of a sensor or probe to acquire network traffic or flow data and generate session metadata from the acquired traffic.
NDR.REQ.0017	Should include an analytics engine component that processes network traffic and/or generated session metadata to detect threats, risks and, anomalies. Should support for reconstruction of session.
NDR.REQ.0018	Should not require an internet connection in support of any of its capabilities. It should be possible to schedule ingestion of OEM supplied updates and third-party threat intelligence (if required) using system console or CLI or scheduling checks with a locally hosted repository.
NDR.REQ.0019	Should support anomaly detection without any threat intelligence in place by using its deep-learning/machine-learning /programmable logic capabilities. Operating system should be security hardened and embedded with kernel for high speed packet processing
NDR.REQ.0020	Protocols like HTTP, SMB, RDP, SSL, DNS, SMTP, LDAP, etc. should be detected by the solution.Should be able to generate and retrieve reports within the appliance itself without the use of any additional database server.
NDR.REQ.0021	The Proposed Solution should support STIX /TAXI/OpenIOC protocols or RESTful APIs allowing it to receive and share threat intelligence information from 3rd party devices if required.
NDR.REQ.0022	Perform deep packet inspection, meta data extraction, meta- indexing, anomaly detection and data enrichment into Antimalware / Dynamic Analysis and various threat intelligence.

S.No	Minimum Specifications
NDR.REQ.0023	Solution should have Risk assessment analysisit should have on attack surface analysis to focus on the risk not just the threat. any new IP, host, server or application exposing to internet in the last 24 hours should be reported with geolocation dashboard
NDR.REQ.0024	Solution should be able to proactively build a picture of the attack surface from the network perspective (e.g., networks, front end servers, backend databases, users etc.) that need to be continuously monitored and analyzed for security vulnerabilities and unauthorized services and can feed this this information to the SIEM.
NDR.REQ.0025	Perform deep packet inspection, meta data extraction, meta- indexing, anomaly detection and data enrichment into Antimalware / Dynamic Analysis and various threat intelligence.
NDR.REQ.0026	Solution should have Risk assessment analysis, It should have on attack surface analysis to focus on the risk not just the threat.
NDR.REQ.0027	Solution should be able to proactively build a picture of the attack surface from the network perspective (e.g. networks, front end servers, backend databases, users etc.) that need to be continuously monitored and analyzed for security vulnerabilities and unauthorized services and can feed this this information to the SIEM.
NDR.REQ.0028	The solution shall include minimum 4 x fiber network taps and any other type of ports / tap aggregator supporting filtering to limit specific data forwarding as a part of solution in order to achieve all required functionality of NDR.
NDR.REQ.0029	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.37 SSL ORCHESTRATOR (SSLO)

S.No.	Parameter	Minimum Specifications
SSLO.REQ.001	General	The Proposed SSL Visibility Device should be a Purpose-built Appliance with dual power supply
SSLO.REQ.002	Hardware	Device should not be more than 2U hardware appliance
SSLO.REQ.003		The Proposed SSL Visibility Appliance should have a minimum of 2*40 G fiber ports (QSFP+) and 8*10G fiber ports(SFP+). The appliance should have dedicated Out-of-band Management Port.
SSLO.REQ.004	Solution	The modules should be dedicated card based for 1024 & 2048 bit certificates and should support 4096 bit.
SSLO.REQ.005	General	The Proposed SSL Visibility Appliance should have Dedicated Hardware Acceleration for SSL /TLS. The Proposed SSL Visibility Appliance should have a minimum capacity of minimum 45 Gbps of SSL throughput. The Proposed SSL Visibility Appliance should support minimum 50K New SSL Transaction per second with RSA 2K key and minimum 35K TPS using ECCshould be deployed in high availability using open standard VRRP or equivalent. The appliance should provide Minimum 128GB RAM, minimum 500 GB hard disk and at least 1*SSL ASICS/ FGPA/ cards.
SSLO.REQ.006	Solution	The solution should support at least 3 million layer 7 requests per second
SSLO.REQ.007	Features	The Proposed SSL Visibility solution should intercept all SSL/TLS based flows, also on other ports and protocols (not only HTTPS) E.g. SFTP, IMAPs, POP3S etc.
SSLO.REQ.008	Features	The Proposed SSL Visibility Solution should support Public Key Algorithms RSA, DHE, ECDHE
SSLO.REQ.009	Features	The Proposed SSL Visibility Solution should support Symmetrical key algorithms AES, AES-GCM, DES, RC4, Camellia
SSLO.REQ.0010	Features	The Proposed SSL Visibility Solution should support Hashing algorithm SHA-2, SHA256, SHA384
SSLO.REQ.0011	Features	The Proposed SSL Visibility Solution should support Solution should support 512/ 1024 through 4096 bit key lengths
SSLO.REQ.0012	Features	The Proposed SSL Visibility
SSLO.REQ.0013		Solution should have the ability to do certificate signing request
SSLO.REQ.0014	Features	The Proposed SSL Visibility Solution should have the ability to cache dynamically generated certificates for reuse on subsequent connections
SSLO.REQ.0015	Features	The Proposed SSL Visibility Solution should support multiple self-signed, internal (organizational) and external CA's and PKI structures can be used simultaneously in the rule base
SSLO.REQ.0016	Features	Solution should have the ability to customize trusted CA lists.
SSLO.REQ.0017	Features	The Proposed SSL Visibility Solution should integrate with any existing CA solution and current PKI structure
SSLO.REQ.0018	Features	The Proposed SSL Visibility Solution should be able to customize trusted CA list
SSLO.REQ.0019	Features	The Proposed SSL Visibility Solution should be able to do CA revocation management

S.No.	Parameter	Minimum Specifications
SSLO.REQ.0020	Features	The Proposed SSL Visibility Solution should support passing Jumbo Frame IP traffic
SSLO.REQ.0021	General	The Proposed SSL Visibility Appliance SSL decryption of the Proposed SSL Decryption Solution should be Port and protocol Agnostic: Intercept SSL/TLS on any port over any protocol, maintaining data integrity, including decryption, re-encryption without processing overhead and latency
SSLO.REQ.0022	General	The Proposed SSL Decryption Appliance should decrypt and re-encrypt (full duplex) in all modes in same format
SSLO.REQ.0023	General	The Proposed SSL Decryption Appliance should have the flexibility of sending decrypted traffic to multiple copy ports
SSLO.REQ.0024	Functional	The Proposed SSL Visibility Solution should have the ability to service chain. The solution should decrypt in the SSL traffic and send specific decrypted traffic to selective security solutions as defined. Solution should have the ability to insert or delete security solutions in the service chain.
SSLO.REQ.0025	Functional	The Proposed SSL Visibility Solution should have the capability to automatically send traffic to the passive security device, for those security solutions deployed in an active-passive high availability mode. The SSL Intercept device shall support both outbound SSL traffic (forward proxy) and inbound SSL traffic (reverse proxy). The SSL Intercept device shall able support inline bridge mode, decrypt/encrypt SSL traffic without change the SRC/DST IPs and network IP segment topology. The SSL Intercept device shall support SPAN port functions for external passive security devices
SSLO.REQ.0026	Functional	The Proposed SSL Visibility Solution should have the capability to load balance traffic to security device that support active-active high availability mode.
SSLO.REQ.0027	Functional	The Proposed SSL Visibility Solution should have the capability to support scale-out of existing security solution.
SSLO.REQ.0028	Features	The Proposed SSL Visibility Solution should have the ability to import server-side certificates and private keys for decryption
SSLO.REQ.0029	Features	The Proposed SSL Visibility Solution should be able to feed multiple devices with a single decryption stream in sequence as a service chain
SSLO.REQ.0030	Features	The Proposed SSL Visibility Solution should support multiple active-inline devices simultaneously
SSLO.REQ.0031	Features	The Proposed SSL Intercept Appliance should have the Encryption support for TLS 1.1, TLS1.2, TLS1.3 SSLV3
SSLO.REQ.0032	Features	The Proposed SSL Visibility Appliance should have the ability to decrypt and re-encrypt traffic within the same appliance
SSLO.REQ.0033	Features	The Proposed SSL Visibility Solution should support Extended Validation (EV) certificates
SSLO.REQ.0034	Features	The Proposed SSL Visibility Solution should have the ability to configure encryption/decryption policy (incl. block/pass-through) based on source/destination ip/port
SSLO.REQ.0035	Features	The Proposed SSL Visibility Solution should have the ability to configure encryption/decryption policy (incl. block/pass-through) based on host/URL categorization
SSLO.REQ.0036	Features	The Proposed SSL Visibility Solution should have the ability to configure encryption/decryption policy (incl. block/pass-through)

S.No.	Parameter	Minimum Specifications
		based on Subject / Domain Name
SSLO.REQ.0037	Features	The Proposed SSL Visibility Solution should support OCSP stapling
SSLO.REQ.0038	Features	The Proposed SSL Visibility Solution should allow TCPDUMP / Packet capture
SSLO.REQ.0039	Features	The Proposed SSL Visibility Solution should have the ability to decrypt once and feed many active inline and passive security solutions and re-encrypt the traffic before transmitting it on the network
SSLO.REQ.0040	Features	The Solution should decrypt traffic for analysis and filtering by multiple traffic analysis devices. In an in-line configuration, and should do this in both directions using a single box, so that encrypted traffic exiting the data center can also be screened for suspect traffic that in some cases is recorded in the SSL log.
SSLO.REQ.0041	Features	The Proposed SSL Visibility Solution should have ability to allow blocking notification (generated by a security device for E.g. IPS in the active loop) to be passed through the SSL Visibility appliance so they are visible to clients.
SSLO.REQ.0042	Features	The Proposed SSL Visibility solution should detect and evaluate connections from servers having invalid certificates.
SSLO.REQ.0043	Features	The Proposed SSL Visibility Solution should have the ability to maintain headers in regenerated TCP stream.
SSLO.REQ.0044	Features	The Proposed SSL Visibility Solution should have the ability to inspect and manage SSL traffic on multiple network segments on the same device.
SSLO.REQ.0045	Features	The Proposed SSL Visibility Solution should block unwanted SSL/TLS: weak protocols and ciphers, untrusted certificate authorities, expired certificates, custom block lists and also should have the ability to customize trusted CA lists.
SSLO.REQ.0046	Features	The Proposed SSL Visibility Solution should support majority of cipher suites and even the draft versions
SSLO.REQ.0047	Features	The Proposed SSL Visibility solution should Support both certificate resign and known server key operations simultaneously i.e. The solution shall decrypt inbound web traffic to external facing web servers and shall decrypt outbound web traffic generated by Internal network user community or others
SSLO.REQ.0048	Hardware	Should support device management using local console, CLI (SSH), GUI (HTTPS)
SSLO.REQ.0049	Solution	The Proposed SSL Visibility Solution should have CLI interface with all functionalities and configuration capabilities through CLI
SSLO.REQ.0050	Solution	The Proposed SSL Visibility Appliance should have Access Control Lists (ACL) on management interface
SSLO.REQ.0051	Solution	The Proposed SSL Visibility Appliance should support IPv6 and solution should be IPv6 certified to ensure all features of IPv6
SSLO.REQ.0052	Solution	Should support sending of logs to centralized Syslog Server.
SSLO.REQ.0053	Solution	System must have Web-based Graphical User Interface (GUI)
SSLO.REQ.0054	Solution	Should support authentication, authorization and accounting (AAA) integration with external authentication support providers such as RADIUS and TACACS+ and support RBAC to help ensure security. Should support role based access.
SSLO.REQ.0055	Solution	The SSL Intercept device shall support secured RESTful API or XML-RPC for simple 3rd party remote management. The SSL Interception device shall support secured WebUI (HTTPS) access. No HTTP. The SSL Interception device admin access shall be supported by local DB,

S.No.	Parameter	Minimum Specifications
		external Radius/TACACS
SSLO.REQ.0056	Solution	Should supports mirroring packets (HTTPS/TCPS) to specified network interfaces.
SSLO.REQ.0057	Solution	Should be high-performance purpose-built hardware with multicore CPU support and not a part of UTM/ Firewall/ Router or any other device. Proposed appliance should support virtualization and support up to 16 Virtual instances with minimum 2 virtual instances from Day1
SSLO.REQ.0058	Solution	The SSL Intercept device shall able support explicit Forward Proxy functions. For privacy policies, the SSL Intercept shall support URL bypassing by static configuration. For compliance, the SSL Intercept shall support selective URL bypassing by reputable online URL classification services.
SSLO.REQ.0059	Solution	For outbound, the SSL Intercept device shall use the same SSL version and SNI options as client, re-encrypt application data, which may be modified by the external security devices (such as WAF, DLP) to the original destination.
SSLO.REQ.0060	Solution	Should support certificate parser and solution should integrate with client certificates to maintain end to end security and non-repudiation. The appliance should support Certificate format as "Open SSL/Apache, *.PEM", "MS IIS, *.PFX",*.Cer and "Netscape, *.DB" etc.. Should support OCSP protocol to check the validity of the certificates online. Certificate bases access control, CRL's (HTTP, FTP, and LDAP) support.
SSLO.REQ.0061	Solution	Should support SNMP v2 & v3 traps, email alerts and SNTP/ NTP. Device should be able to send SNMP traps to centralized server and should provide login/ logout, configuration changes, dumps information.
SSLO.REQ.0062	Support	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.38 DATA LEAKAGE PROTECTION

S.No.	Minimum Specifications
DLP.REQ.001	Solution must have the following to support atleast 1000 users/licenses: 1) Discovering sensitive data on the network. Ability to discover and control all your data at rest and in motion. 2) Solution should provide data classification based on its type. Should be able to classify data workflows implemented based on the data's characteristics and level of sensitivity. 3) Fast-acting remediation. To protect data and prevent data loss, solution should be capable of doing more than just monitoring. It should also be able to act and remediate, which includes replacing, modifying, cleansing, or deleting data as needed.
DLP.REQ.002	Support the solution including future upgrades of all components of the solution, without any exception for a minimum period of 5 years from the date of go live (Extendable for another 2 years upon CRID's discretion)
DLP.REQ.003	Support for application version / hardware-cum-software infrastructure
DLP.REQ.004	Solution must Safeguard employee privacy – balancing the needs of Government data protection along with the need for employee privacy, Visibility and control over data including: a) Encrypted data; b) Image files etc.
DLP.REQ.005	Summarize the similar incidents, Incident workflow and case management.
DLP.REQ.006	Role based administration for internal administrative tasks and monitoring and enforcement.
DLP.REQ.007	Ensure no unwarranted, illegal, and fraudulent misuse of data shared by HSDC. Partner / Bidder to categorically indemnify HSDC against any direct losses that HSDC may suffer on account of any such fraudulent and illegal act by the Company or its employees.
DLP.REQ.008	Solution should provide for built-in/predefined policies/templates for government and geographies, and can be accessed, used, and applied simultaneously solution that provides content, context and destination awareness, allowing administrators to manage who can send what information where and how.
DLP.REQ.009	The proposed DLP solution should have central web-based management console and incident repository. HSDC administrators shall use the console to define, deploy and enforce data loss policies, respond to the incidents, analyse and report violations, and perform system administration.
DLP.REQ.0010	The proposed DLP solution should block, quarantine or relocate the channel containing sensitive data. DLP must support implementing policies on sensitive data like copy and paste, printing, saving content in local folders, remote , removable drives etc.
DLP.REQ.0011	Enabling Processes: Develop processes that are required to support the use of the tool/ technology: Admin Guide, Policy creation, Policy Fine Tuning, Incident management, classification, incident response/ reporting.
DLP.REQ.0012	Define Key performance indicators (KPI), which are aligned with overall data protection strategy, such as number of data leakage incidents, network coverage, Rules configured, reduction of false positives, Incidents closed within SLAs etc.
DLP.REQ.0013	Perform Configuration of Policies: Provide assistance to configure the tool with required rules.
DLP.REQ.0014	Should man a resource having 2-3 years of DLP experience to assist with routine operations and support continuous improvement of system:
DLP.REQ.0015	Evaluate the incidents, escalations and responses. Exclusion of the authorized list in data protection policies based on the responses, feedback and management directives.

S.No.	Minimum Specifications
DLP.REQ.0016	Evaluate false positives and false negatives; fine tune the data protection policies to correct the errors.
DLP.REQ.0017	Review overall feedback and exceptions.
DLP.REQ.0018	Full documentation of the project is to be included in the deliverables by the successful Vendor.
DLP.REQ.0019	Configure relevant reports as required by HSDC
DLP.REQ.0020	Train the HSDC administrators on usage and configuration of the policies and rules
DLP.REQ.0021	Train HSDC Users for administration, management and implementation of the solution
DLP.REQ.0022	All the resources provided for implementation of the solution should be OEM certified OR have sufficient levels of experience in implementing the solution at various other clients.
DLP.REQ.0023	Installation of the supplied products to be done by OEM only. All required hardware for above implementation shall be provided by Department.
DLP.REQ.0024	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.39 GOVERNANCE, RISK, AND COMPLIANCE TOOL

S. No.	Parameter	Minimum Specifications
GRC.REQ.001	GRC Tool Basic Features	The solution should be deployed on-premises (Organization provided infrastructure) with support upto 100 users base factoring all licenses together.
GRC.REQ.002		The solution should be deployed and running in more than 3 Indian government organizations
GRC.REQ.003		The solution should be deployed and running in more than 20 Indian companies (Government and Private)
GRC.REQ.004		The system should be able to integrate with systems such as Active Directory and LDAP seamlessly.
GRC.REQ.005		The system support SAML 2.0/ two factor authentication protocols.
GRC.REQ.006		The system provides a variety of layout options enabling a business user to alter the user interface.
GRC.REQ.007		The system should support attachments
GRC.REQ.008		Record or field level formulas or calculations should be easily changeable by the local administrator, without the assistance of the OEM or professional services.
GRC.REQ.009		The Solution should provide a variety of layout options enabling a business user to alter the user interface.
GRC.REQ.0010		Use cases should be configurable to add additional fields without requiring professional services for customizations.
GRC.REQ.0011		The Communication between various components of solution & with other integrated systems should be using encrypted channels.
GRC.REQ.0012		The Solution should document the business infrastructure including products/services, business processes, information assets, facilities and personnel and hierarchy of the Department.
GRC.REQ.0013		The Solution should capture history of a record for all changes done on it and the user who made them.
GRC.REQ.0014		The Solution should provide a workflow engine that easily allows users to set up and maintain defined and customized workflow management processes.
GRC.REQ.0015		The solution should have the features of schedule bulk updates and scheduled bulk create based on defined parameters
GRC.REQ.0016		The Solution should support advanced workflow capabilities such that multiple simultaneous paths and return back to earlier steps, phases or stages. The workflow configuration should be driven via a graphical user interface and not configured via customized code.
GRC.REQ.0017		The solution enables you to expand and extend existing use case implementation to additional risk and compliance use cases as the program grows.
GRC.REQ.0018		The solution enables you to expand and extend existing Risk use case implementation to enable risk quantification features such as Bow -Tie Analysis, Monte Carlo Simulation, FAIR analysis etc.
GRC.REQ.0019		The system includes an IT policy and IT controls library.
GRC.REQ.0020	IT Security Policy Program Management	The system supports importing/exporting of IT policies and IT controls.
GRC.REQ.0021		The system includes default content libraries that provide

S. No.	Parameter	Minimum Specifications
		broad coverage across industries.
GRC.REQ.0022		The system includes built-in weighting/scoring capabilities to allow for easy prioritization of business-critical compliance requirements.
GRC.REQ.0023		The system includes pre-defined mappings to industry best practices, framework, regulations and standards.
GRC.REQ.0024		The system supports IT policy and IT control mapping for custom or existing policies and controls.
GRC.REQ.0025		The system supports IT policy authoring with approval workflow.
GRC.REQ.0026		The system supports IT policy and controls versioning.
GRC.REQ.0027		The system supports linking IT policy and controls to supporting documents and files.
GRC.REQ.0028		The system supports easy addition of new regulations and requirements and has interfaces to feeds that provide for and update regulations, legislation and self-regulating bodies.
GRC.REQ.0029		The system provides discreet capabilities to capture and track regulatory changes.
GRC.REQ.0030		The system includes workflow and stakeholder ownership assignment to ensure changes to the business are properly reviewed.
GRC.REQ.0031		The system allows users to filter and view policies by statically or dynamically defined criteria such as Department unit, geography, impact area, role, etc.
GRC.REQ.0032		The system allows users to perform keyword searches to quickly find specific information among various IT policies.
GRC.REQ.0033		The system provides multiple viewable and printable reporting options to provide flexibility in matching report formats to audience needs.
GRC.REQ.0034		The system offers a library of technical baseline configuration procedures mapped to various technologies. (List specific baselines offered.)
GRC.REQ.0035		The system provides top-down or bottom-up approaches to developing key control procedures aligned with corporate compliance requirements.
GRC.REQ.0036		The system provides advanced technical baselines written against control standards and mapped to regulatory requirements, best practices, and international standards.
GRC.REQ.0037		IT Policies and controls are assigned: Individually to entities, globally to groups, automatically based on attributes and dynamically when attributes change
GRC.REQ.0038		The platform should support the identification and criticality definition of business processes and assets.
GRC.REQ.0039		The system should have a built-in method of defining the business process criticality as well as provide the flexibility to accommodate our calculation method.
GRC.REQ.0040		Ability to capture the relevant data for each business process as well as underlying assets, application, information assets, products and services, business unit, devices, etc.
GRC.REQ.0041		The system should support and provide a Contacts application that maintains details (such as Name, email, contact number, Business Unit, Manager etc.) of all the employee that have access to the system.

S. No.	Parameter	Minimum Specifications
GRC.REQ.0042		Ability to import data related to employees from an export from systems such as an HRMS system Or an Excel sheet.
GRC.REQ.0043		Ability to document and maintain external benchmarks, frameworks, laws and regulations identified for meeting the corporate objectives.
GRC.REQ.0044		Ability to document unique and comprehensive control standards identified and documented from the internal policies for meeting the corporate objectives.
GRC.REQ.0045		Provide built in workflow (basic and advanced) for the current follow-up and escalation process.
GRC.REQ.0046		Ability to define frequency of review and reporting for the tasks assigned.
GRC.REQ.0047		Pre-mapped controls that are maintained by vendor on a periodic basis. Specify which of these frameworks are supported (NERC, ISO, ISF, COBIT, NIST, FFIEC, HIPAA, GLBA, PCI, SOX, HITRUST CSF).
GRC.REQ.0048	IT Controls Assurance	Compliance requirements can be mapped to a business hierarchy.
GRC.REQ.0049		The system records the consequences (financial and non-financial) of non-compliance with different requirements.
GRC.REQ.0050		Compliance programs have the ability to create compliance-related assignments or tasks to track responsibility and expected completion dates.
GRC.REQ.0051		Each owner has signoff ability to close out a compliance period, archive their compliance program data and begin the cycle for the next period.
GRC.REQ.0052		The system has the ability to link to supporting external requirements from compliance programs.
GRC.REQ.0053		Ability to define / modify preconfigured compliance questionnaires/surveys
GRC.REQ.0054		The survey functionality includes the ability to assign multiple recipients from a single template and reporting across different statutory entities.
GRC.REQ.0055		The system allows the ability to view, print and report on all compliance-related surveys.
GRC.REQ.0056		Content (policies, controls, report templates, reference documentation) is available as part of the standard solution.
GRC.REQ.0057		The system supports bidirectional policy and control/sub control mapping to all relevant regulations and mandates.
GRC.REQ.0058		The system employs predefined and customizable assessment templates (based upon standards/ frameworks).
GRC.REQ.0059		The system supports a master library of questions that can be used in multiple questionnaires and are mapped to standards/frameworks.
GRC.REQ.0060		The system supports applying weight to questions and responses.
GRC.REQ.0061		The system automatically generates findings for incorrect answers and allows the management of findings through remediation tasks or exception requests.
GRC.REQ.0062		The system's compliance scores seamlessly combine survey-based and automated testing results and data from third-party tools.
GRC.REQ.0063		The system can flag result discrepancies (e.g., between survey-based and automated test results).

S. No.	Parameter	Minimum Specifications
GRC.REQ.0064		The system can be used to perform a gap analysis.
GRC.REQ.0065		The system calculates compliance scores for each regulation.
GRC.REQ.0066		The system calculates compliance scores for any group, including dynamically defined groups.
GRC.REQ.0067		Ability to document control activities and capture details like control owners, testing requirements, mapping with compliance, risk, business unit etc..
GRC.REQ.0068		The system provides the built-in ability to document control activities currently in scope and perform validation testing such as Control Self Assessments, Design Efficiency and Operating Efficiency testing, etc.
GRC.REQ.0069		Ability to integrate automated test results from technical controls like Qualys Guard, Nessus out of the box.
GRC.REQ.0070		Ability to provide built-in assessments and questionnaires as well as manually create assessments and questionnaires per defined guidelines for conducting compliance testing.
GRC.REQ.0071		Provide an automated and rule driven mechanism for reporting test results on a frequency via data driven events and conditions.
GRC.REQ.0072		Provide a mechanism to track and remediate control deficiencies identified during testing.
GRC.REQ.0073		The system provides the ability to define and report the full scope of the information security management system (ISMS).
GRC.REQ.0074	Information Security Management System (ISMS)	The system provides the ability to report on ISO 27001 conformance in conjunction with a certification effort.
GRC.REQ.0075		System captures robust details about each risk element / item including objectives, products and services, business processes, risks, controls, physical facilities, technology assets, policies and procedures.
GRC.REQ.0076	IT Risk Management	System enables a holistic understanding of the interrelationship of each risk element / item elements and provides the ability to traverse these relationships and drill into the details of each framework element
GRC.REQ.0077		Ownership of each risk element / item record can be established by individual and by organizational entity (business unit, division, company, etc.)
GRC.REQ.0078		System provides a means to roll-up risks from a detailed level to a summary, enterprise-wide view appropriate for executive reporting
GRC.REQ.0079		System supports a risk register approach to risk assessments
GRC.REQ.0080		Risk assessments are performed on both inherent and residual risk
GRC.REQ.0081		Risk assessments can be performed for each risk category associated with a risk register record
GRC.REQ.0082		Risk assessments support both qualitative and quantitative approaches and both approaches can be applied consistently and harmonized in one risk assessment view
GRC.REQ.0083		Risk thresholds can be established by risk and by organizational hierarchy and risks outside thresholds can be routed to stakeholders on a timely basis
GRC.REQ.0084		The system provides a means to capture and assess the risks associated with new or changed products and services, business processes, or ventures

S. No.	Parameter	Minimum Specifications
GRC.REQ.0085		Risk register records can be catalogued as scenarios and reports of enterprise scenario analysis generated
GRC.REQ.0086		Risk register records in development or de-commissioned can be catalogued as such so that they are not reflected in risk roll-up calculations but are retained for further development and / or audit trail reference
GRC.REQ.0087		The system integrates the concepts of strategic planning, operational management and internal controls.
GRC.REQ.0088		The system provides the ability to create a risk summary report that describes key risks, how they are being managed and monitored, remediation of key issues and accountability.
GRC.REQ.0089		The system offers graphical, color-coded reports of strategic objectives and the evaluation of risk where specific criteria are accessed.
GRC.REQ.0090		System provides a means to reaffirm existing risks and risk assessments with risk owners and to capture and report on changes in risk profile of each organizational unit including missing and emerging risks, changes in products, processes, organizational structure, technology and externally driven events. The system automatically distributes work to impacted users and tracks it to completion, including the ability to automatically send reminders.
GRC.REQ.0091		The system allows for aggregation of risks across the organization.
GRC.REQ.0092		Automated questionnaires can be utilized to target and assess any risk element and to capture business contextual information about each element:
GRC.REQ.0093		The system calculates, displays, and reports risk scores.
GRC.REQ.0094		Risk calculations are transparent (no "black box" magic).
GRC.REQ.0095		The system gives users full control over risk calculation parameters, weightings.
GRC.REQ.0096		The system supports custom risk assessment methodologies and algorithms.
GRC.REQ.0097		Required fields and field names can be easily configured by the customer to match the customer's unique risk taxonomy.
GRC.REQ.0098		The system supports risk assessment processes and workflow.
GRC.REQ.0099		The system supports online assessments.
GRC.REQ.00100		The system enables a methodology to assign security resources to threat related projects, tracks the projects and facilitates a process that includes threat identification, analysis and counter measure plans.
GRC.REQ.00101		The system provides a method to gather threat scenarios for business representatives via a questionnaire function.
GRC.REQ.00102		Ability to manually or automatically calculate the criticality of information assets (Applications, It Infra., devices etc) which are defined.
GRC.REQ.00103		Ability to reflect the current risk assessment process conducted for the IT Assets (applications, devices, etc.)
GRC.REQ.00104		Provide the capability to document and capture details of stakeholders identified like asset owner, risk owner, control owners etc.
GRC.REQ.00105		Capability to define and automate the frequency of conducting the IT risk assessment and automatically

S. No.	Parameter	Minimum Specifications
		generating reports across various levels such as business unit head / manager, asset owner as well as board and management levels.
GRC.REQ.00106		Provide an out of the box risk register in order to capture currently maintained and tracked risks as well as ability to configure the application via no coding to accommodate our requirements.
GRC.REQ.00107		Ability to capture and document risk response procedures as well as mitigating controls that are maintained and linked to within the same platform.
GRC.REQ.00108		Ability to link and map identified risk to Authoritative Sources, departments, asset, divisions as well as other elements via cross reference and mapping capabilities without coding etc.?
GRC.REQ.00109		The solution provides a centralized system to catalogue IT assets for incident prioritization and provide business context for prioritization of events
GRC.REQ.00110	Cyber Incident & Breach Response Management	Core functions of the solution should include a catalogue of IT assets, central repository and taxonomy for security alerts, integration to SIEM, log and packets, full lifecycle support for incident management, incident investigation, incident response and issues management
GRC.REQ.00111		Solution manages end-to-end security incident lifecycle as a consistent/predictable business process
GRC.REQ.00112		Solution centralizes security incident management with integrated business context
GRC.REQ.00113		Solution can align and help customers deploy incident response best practices aligned with industry standards
GRC.REQ.00114		Solution provides a repository to document SOC procedures based on threat category
GRC.REQ.00115		Solution will help in the overall investigation process and forensic analysis for security incidents
GRC.REQ.00116		Solution has the Incident Journal to summarize key points about the security investigation so if a security incident is escalated security analysts will have details about the key points
GRC.REQ.00117		Solution has terminology specifically catering to security incidents
GRC.REQ.00118		Solution can map incidents to security controls and provide a view of how effective security controls are in capturing security incidents
GRC.REQ.00119		The solution provides a centralized system to catalogue IT assets for incident prioritization and provide business context for prioritization of events
GRC.REQ.00120		Solution manages end-to-end security incident lifecycle as a consistent/predictable business process
GRC.REQ.00121		Solution centralizes security incident management with integrated business context
GRC.REQ.00122		Centralized catalogue of IT assets and repository and taxonomy for vulnerability data
GRC.REQ.00123	IT Security Vulnerability Program Management	The system should support ability to research known vulnerabilities helps prioritize efforts for IT operations
GRC.REQ.00124		System should support ingestion of vulnerability detections to support large enterprise environments

S. No.	Parameter	Minimum Specifications
GRC.REQ.00125		System should enable creation of vulnerability tickets for tracking of remediation actions by scanner
GRC.REQ.00126		System should support rules-based issues management
GRC.REQ.00127		System should have built-in integration to the leading scanning technologies including Qualys and Tenable
GRC.REQ.00128		System should apply business context to detections to help analysts prioritize remediation efforts based on the role, criticality and CVSS environmental score
GRC.REQ.00129		System should provide an end-to-end process to address vulnerabilities from detection to remediation according to business risk
GRC.REQ.00130		All the quoted components must be IPv6 ready from day one and should be supplied with 1 Year comprehensive OEM on-site support/ services for S/w and One Year OEM onsite manpower Support for the S/w.
GRC.REQ.00131	Licenses and support	Installation of the supplied products to be done by OEM only. All required hardware for above implementation shall be provided by Department. The licenses shall be for enterprise wide license and license should be perpetual in nature
GRC.REQ.00132		The respective OEM must provide comprehensive training to SDC Officials on the Solution for an appropriate period or 15 days at Chandigarh split in following sessions. Sessions can be as Under 1. Session 1: At the time of installation and commissioning for implementing best practices with the experience of OEM keeping in view over all architecture of project. CRID shall be part of this process. 2. Session 2: Administration, Management and Performance Tuning. The session must be instructor lead and may be conducted physical or online as on need basis. This may be repeated in first year after Go-Live as per the requirement of CRID.

5.40 VULNERABILITY ASSESSMENT TOOLS

S.No.	Parameter	Minimum Specifications
VAT.REQ.001	Architecture	The Solution should be 100% on-premises with no dependency on the cloud and shall not rely on component /service hosted outside the Organization's premise for any feature functionality or product capability. It should cater to perform vulnerability scan of all IP devices present in their environment.
VAT.REQ.002		The Solution should have inbuilt/out of box 100s dash boarding and reporting capability with an option of customization as per the customers requirement.
VAT.REQ.003		The Solution should have an option of defining the data retention period so to retain results for a defined and configurable period of time after which the results are expired and archived into another query-able database automatically. The data retention period will be as per Government guidelines issued time to time.
VAT.REQ.004		The product must provide flexible licensing of scanner deployment with the ability to deploy additional scanners at no additional cost.
VAT.REQ.005	Role Based Access Control	The solution should allow the Organisation to create multiple profiles based on department, asset type, platforms, users, geographies, network zones, applications etc.
VAT.REQ.006		The product must provide role-based access control with enough granularity to control users access to specific data sets and functionality that is available to those users.
VAT.REQ.007	Integration	The Solution should provide mechanism to integrate with SIEM, SOAR, PAM, IT Ticketing systems, NACs etc. Please describe the out of box use cases that will be supported by the solution.
VAT.REQ.008	Discovery, VA Scan, Remediation and Analysis	The solution must have capability to perform active and passive asset discovery scan, network VA, database VA etc.
VAT.REQ.009		The solution should have the capability to accurately discover and classify assets connected in the network and auto comparing the total count with the previously discovered assets scan to report newly discovered assets. Post discovery the system should automatically determine the criticality of the asset so as to help in prioritization.
VAT.REQ.0010		The solution should provide views of active and mitigated vulnerabilities with automatic migration of vulnerabilities from active to mitigated, flag re-opened vulnerabilities with recurrence count.
VAT.REQ.0011		The solution should provide remediation views that are automatically prioritized and streamlined for providing insight to management and application owners
VAT.REQ.0012		The solution support provides an option of uploading the custom audit policies to meet organization's requirement
VAT.REQ.0013		The solution should be able to prioritize scanned based on risk and shall be able to reduce the remediation efforts by more than 90%.
VAT.REQ.0014		The solution should perform Intelligent port scanning for service identification running on non-standard ports and support scanning throttling/ rate limiting speed.

S.No.	Parameter	Minimum Specifications
VAT.REQ.0015		The product must support PCI, CIS, SCAP etc. Compliance vulnerability scanning. The product must include pre-defined PCI scan profiles that meet current PCI DSS criteria for network scanning. Functionality must exist to filter all other non-PCI relevant vulnerabilities.
VAT.REQ.0016		Tool should provide unique Vulnerability Priority Prediction apart from CVSS framework.
VAT.REQ.0017		The product must fully integrate scanning and compliance to include combined licensing and consolidation of data, analysis, and querying. The Vulnerability Scanner should be capable of performing agent less and agent based scans. The Vulnerability Scanner should be capable of performing agent less and agent based scans.
VAT.REQ.0018		Dashboard elements must be fully customizable by filtering to display data based on asset list, vulnerability or compliance checks, time, key word search, IP address, etc.
VAT.REQ.0019	Support	The OEM must provide comprehensive training to SDC Officials on the Solution for a period of 15 days. Supplier should provide training to use, configure and operate the services created using supplied Stack as per purchaser's intimation

5.41 DYNAMIC APPLICATION SECURITY TESTING (DAST) TOOLS

S.No.	Minimum Specifications
DAST.REQ.001	Should detect web application OWASP and SANS vulnerabilities, via crawl/ application analysis, universal translator, normalization, pre-attack analysis, attack and generating reports after the scan. Describe explicitly how many vulnerabilities are identified with details for help
DAST.REQ.002	The solution should have capability to scan web & mobile applications.
DAST.REQ.003	The solution should be capable to automate / schedule scans.
DAST.REQ.004	The solution shall support simultaneous Crawl/ application analysis & Audit during scans.
DAST.REQ.005	The solution allows for real-time review and investigation of vulnerabilities found while a test is still in progress.
DAST.REQ.006	The solution offers the capability to schedule a single or multiple recurring scans in advance.
DAST.REQ.007	The solution supports Web Services security testing.
DAST.REQ.008	The solution provides REST/URL Rewriting (Variable) detection and support.
DAST.REQ.009	The solutions allow custom checks to be added
DAST.REQ.0010	The solution comes with an array of out-of-the-box scan policies and all major compliance reports which may be further added to and customized.
DAST.REQ.0011	The solution allows for a re-run of the entire scan with the same settings
DAST.REQ.0012	The solution provides a shortcut to quickly re-test all vulnerabilities
DAST.REQ.0013	Must support CAPTCHA/OTP/Composite Login process configuration in the proposed solution.
DAST.REQ.0014	Solution should support Swagger API Scan.
DAST.REQ.0015	Solution should generate rules to send to WAF.
DAST.REQ.0016	Integration with tools like POSTMAN and BURP.
DAST.REQ.0017	License should support concurrent users and should be sized for 5 User / Tester
DAST.REQ.0018	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.42 SYSTEM SOFTWARE'S

Operating System & Database software will be procured separately by CRID and will be provided to the MSI based on the requirement as per project plan submitted by MSI.

5.43 VIRTUALIZATION SOFTWARE

S.No.	Minimum Specifications
VIRT.REQ.001	The solution should include bare metal hypervisor with functionality of HA and proactive HA, Zero Downtime & Zero Data-loss without any clustering solution, Encrypted Live Migration of VMs, Hot Add (vCPU, vMemory, vStorage & vNetwork) , Horizontal, Vertical Scaling (vCPU, vMemory, vStorage & vNetwork) without disruption or downtime of working VMs for both windows and Linux base VMs, distributed switch, VM level encryption, Network and Storage I/O Control, VM based replication not more than 5 mins RPO, resource scheduling for storage and VMs
VIRT.REQ.002	The solution should provide in-built enhanced host-level packet capture tool which will provide functionalities like SPAN, RSPAN, ERSPAN and will capture traffic at uplink, virtual switch port and virtual NIC level
VIRT.REQ.003	Virtualization software shall allow heterogeneous Guest OS support and certification for namely Windows, Red hat & SUSE Linux Enterprise (SLES)- This support and certification should be from OS as well as hypervisor vendor listed
VIRT.REQ.004	Virtualization software should provide quick boot and reduce patching and upgrade times by rebooting the hypervisor without rebooting the physical host, skipping time-consuming hardware initialization
VIRT.REQ.005	The solution should enforce security for virtual machines at the Ethernet layer. Disallow promiscuous mode, sniffing of network traffic, MAC address changes, and forged source MAC transmits
VIRT.REQ.006	Virtualization software/solution should allow seamless migration across different CPUs across the hybrid cloud by persisting the hot migration with zero downtime per-VM during migrations across clusters. The solution should also provide the cross-cloud Cold and Hot Migration to further enhance the ease of management across and enabling a seamless and non-disruptive hybrid cloud
VIRT.REQ.007	Virtualization software should provide secure boot for protection for both the hypervisor and guest operating system by ensuring images have not been tampered with and preventing loading of unauthorized components
VIRT.REQ.008	The solution should provide functionality to automate and simplify the task of managing hypervisor installation, configuration and upgrade on multiple physical servers.
VIRT.REQ.009	Virtualization software should have the provision to provide zero downtime, zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure, without the cost and complexity of traditional hardware or software clustering solutions
VIRT.REQ.0010	Virtualization software should provide integration of 3rd party endpoint security to secure the virtual machines with offloaded antivirus, anti-malware solutions with/without the need for agents inside the virtual machines
VIRT.REQ.0011	The solution shall pre-emptively rebalance workloads in advance of upcoming demands and spikes, eliminating resource contention before it happens thus ensuring that workloads get the resources that they need at all times and also provide smart Alerts, guided remediation, self-learning analytics with dynamic thresholds to deliver recommendations, or trigger actions, that optimize performance and capacity and enforce configuration standards.
VIRT.REQ.0012	Virtualization software should provide simple and effective centralized management for virtual machine templates, virtual appliances, ISO images, and

S.No.	Minimum Specifications
	scripts.
VIRT.REQ.0013	Virtualization software should have the ability to live migrate VM files without any VM downtime, it should have capability of native backup and restoration of the virtualization management server
VIRT.REQ.0014	Virtualization software should support TPM 2-0 hardware modules and adds a virtual TPM device to shield guest OS from Operator or in-guest attacks
VIRT.REQ.0015	Hypervisor management software should support user role and permission assignment (RBAC) and shall provide capability to monitor and analyse virtual machines, and server utilization and availability with detailed performance graphs.
VIRT.REQ.0016	Hypervisor management software console shall maintain a record of significant configuration changes and the administrator who initiated them and shall provide a single view of all virtual machines, allow monitoring of system availability and performance and automated notifications with email alerts.
VIRT.REQ.0017	The virtualization software should provide in-built or integrated Replication capability which will enable efficient array- agnostic replication of virtual machine data over the LAN or WAN. This Replication should simplify management enabling replication at the virtual machine level enabling RPOs as low as 5 minutes
VIRT.REQ.0018	Hypervisor should have capability similar of Virtual Volumes which enables abstraction for external storage (SAN, NAS and Object Storage) devices making them Virtualization aware and it should allow common management across storage tiers and dynamic storage class-of-service automation via a policy-driven control plane
VIRT.REQ.0019	OEM should provide direct support for 5 years i.e. 24x7x365x5 with unlimited incident support and 30 mins or less response time including the unlimited upgrades and updates.
VIRT.REQ.0020	The virtualization software should support Isolation between Virtual Machines. In case one VM is infected/defaced then the attack may not penetrate to other VM/Network
VIRT.REQ.0021	The virtualization software should have control to enable/disable ports/services/ACL or a Network based Firewall.
VIRT.REQ.0022	The virtualization software should support live/hot Backup/Snapshot and Restoration facility.
VIRT.REQ.0023	Virtualization software should support Multi-User Access/role based authentication for VMs.
VIRT.REQ.0024	Virtualization software should be Scalable.
VIRT.REQ.0025	Virtualization software should support Multi IP Pool / LAN segments.
VIRT.REQ.0026	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.44 DISASTER RECOVERY MANAGEMENT SOFTWARE/SOLUTION

Sl.No.	Minimum Specifications
DRMS.REQ.001	DR solution should allow centralized creation and management of recovery plans directly from Virtualization Manager Console/equivalent functional manager console in GUI mode. Automatically discover and display virtual machines protected.
DRMS.REQ.002	DR solution should support the extension of recovery plans with custom scripts and also able to Control access to recovery plans with role-based access control.
DRMS.REQ.003	DR solution should receive automatic alerts about possible site failure and allow execution of recovery plan directly from virtualization manager with a single click and also support automated boot of protected virtual machines with pre-specified boot sequence.
DRMS.REQ.004	DR solution should manage and monitor execution of recovery plans from virtualization manager / DRM portal or independent reporting Portal and support automated reconfiguration of virtual machine IP addresses at failover site.
DRMS.REQ.005	DR solution should automate failback to original production site using original recovery plan and also automatically re-protect virtual machines by reversing replication to the original site without any additional hardware appliance.
DRMS.REQ.006	DR solution should use storage snapshot/VM snapshot to perform recovery tests without losing replicated data and also provide multiple point-in-time recovery which will allow reversion to earlier known states.
DRMS.REQ.007	DR solution should connect virtual machines to an existing isolated network to avoid impacting production applications while doing a testing and automate clean-up of testing environments after completing tests.
DRMS.REQ.008	DR solution should store, view and export results of test and failover execution from virtualization manager/DRM portal/reporting manager.
DRMS.REQ.009	DR solution should automate planned migrations with graceful shutdown of protected virtual machines at the original site thus ensuring no data loss and application-consistent migrations.
DRMS.REQ.0010	DR solution should manage replication directly through the common virtualization manager, at a granular virtual-machine level and ensure complete replication of virtual machine data in an application-tier and storage based replication/storage to storage replication through DR tool prior to initiating migration.
DRMS.REQ.0011	DR solution should be possible for the same site to serve as a protected site and recovery site when replication is occurring in both directions and protecting virtual machines at both sites.
DRMS.REQ.0012	From initial setup to ongoing management, DR solution should deliver simple and policy-based operations: • Centralized recovery plans to create and manage recovery plans for thousands of VMs directly from the intuitive user interface. • Policy-based management to utilize storage profile protection groups to identify protected datastores, automate the process of protecting and unprotecting VMs, and adding and removing datastores from protection groups. • Self-service provisioning to allow application tenants to provision DR protection using blueprints in Automation layer.
DRMS.REQ.0013	DR solution should offer: a. Application-agnostic protection eliminates the need for app-specific point solutions b. Automated orchestration of site failover and failback with a single-click reduces recovery times. c. Frequent, non-disruptive testing of recovery plans ensures highly predictable recovery objectives d. Centralized management of recovery plans from the virtualization manager console/equivalent functional manager console in GUI mode replacing the

Sl.No.	Minimum Specifications
	manual runbooks. e. Planned migration workflow enables disaster avoidance and data centre mobility. f. Reduce the DR footprint through hyper-converged, software defined storage infra. g. VM/ Hypervisor based replication integration to deliver VM-centric, replication that eliminates dependence on storage any discrete infra. h. Support for array-based replication or through any other equivalent method(Hardware/Software based) to offer choice and options for replication with zero data loss.
DRMS.REQ.0014	DR solution should Map virtual machines to appropriate resources on the failover site a. Option to customize the shutdown of low-priority virtual machines at the failover site to get more resources or proper utilization of resources" b. Option to recover multiple sites into a single shared recovery site d. The solution should provide technology so that live migration/replication of virtual machine disks would be supported between different storages.
DRMS.REQ.0015	DR solution should be storage-agnostic replication that supports use of low-end storage, including direct-attached storage and also provides host based replication which will replicate only changed blocks to increase network efficiency.
DRMS.REQ.0016	DR solution should provide integration with hypervisor/ VM based Replication and should support to achieve RPO/RTO as defined in the scope of this RFP.
DRMS.REQ.0017	DR solution should provide automatic generation of history reports after the completion of workflows such as a recovery plan test and clean-up are performed in DR solution. These reports should document items such as the workflow name, execution times, successful operations, failures, and error messages which are useful for internal auditing, proof of disaster recovery protection for regulatory requirements, and troubleshooting. Reports can be exported to any of below formats: HTML, XML, CSV, Microsoft Excel, Word document.
DRMS.REQ.0018	OEM should provide direct support 24x7x365 with unlimited incident support (Telephonic, Web & Email) and 30mins or less response time including the unlimited upgrades and updates for a period of complete project.
DRMS.REQ.0019	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

5.45 HYPER CONVERGED INFRASTRUCTURE (HCI) SOLUTION

Sl. No.	Component / Performance / Utility	Minimum Specification
A	**HCI Architecture**	
HCI.REQ.001	**HCI Architecture**	The proposed HCI solution should include software, hardware, networking, licenses (storage, compute and network virtualization, cloud orchestration, automation, management and monitoring etc.) and any other components required to create an integrated solutionfrom day 1, License proposed should have flexibility to decouple the HCI software from hardware, in order to run HCI software on any certified hardware. The plan, design, architecture and implementation of the HCI solution to be carried out by the SI should be compliant with global best practices and reference architecture of respective HCI OEMs.
B	**General**	
HCI.REQ.002	General	Proposed HCI solution must have been implemented in at-least one State Data Centre/PSU Data Centre/ TIER 3 Data Center in India.
HCI.REQ.003	General	The complete HCI solution must include complete software suite for virtualization, cloud orchestration, provisioning, management, monitoring and reporting etc.
HCI.REQ.004	General	The proposed HCI solution should be fully software defined and should not leverage any specialized (proprietary) hardware for providing data services such as deduplication and compression
HCI.REQ.005	General	a. The proposed solution should independently scale storage and compute as and when needed without any downtime. b. HCI should support storage expansion without any virtualization license implication for "only storage " expansion.
HCI.REQ.006	General	The proposed HCI software solution and all required licenses should be PERPETUAL / Subscription (If Subscription, It must be supplied for duration of scope of the project in this RFP + 2 years)in nature and should have NO dependency on underlying hardware.
HCI.REQ.007	General	The proposed solution must offer the ability to add nodes independent of form factor, RAM, Storage and Cores etc. for future expansions.
HCI.REQ.008	General	The proposed HCI solution must support Data Compression, De-duplication & Erasure coding natively and licenses for this feature should be factored in the bill of material.
C	**Management**	

Sl. No.	Component / Performance / Utility	Minimum Specification
HCI.REQ.009	Management	The proposed solution must be managed through an web based console that provides a single pane of glass view for the entire environment
HCI.REQ.0010	Management	The solution should provide prebuilt & customizable operations dashboards & reports to provide real time insight into infrastructure behaviour (like what-if scenarios, root cause analysis etc.), upcoming problems & opportunities for efficiency improvements.
HCI.REQ.0011	Management	The solution should provide explanations, recommended solutions to performance, capacity & configuration problems. It should also associate workflows with alerts to automatically initiate corrective measures at critical thresholds.
HCI.REQ.0012	Management	The solution should provide capacity analytics which can identify over provisioned resources so they can be right sized for most efficient use of virtualized resources.
HCI.REQ.0013	Management	The solution shall provide assistance in troubleshooting and operational management in the virtualized environment.
HCI.REQ.0014	Management	The solution should have the capabilities for configuration and change management workflows
D	**Reporting**	
HCI.REQ.0015	Reporting	The solution should provide dashboard capabilities and customization, capabilities for meta-tagging, ability to customize report time periods, capabilities to export the reports to multiple formats, to automate and distribute reports and display resources utilization
E	**SW Feature**	
HCI.REQ.0016	SW Feature	The HCI storage must have integrated wizard to schedule snapshot for hourly / daily / weekly / monthly snapshot policies. Any additional software or license must be provided on day 1.
HCI.REQ.0017	SW Feature	The Solution should allow for taking clones of individual Virtual Machines for faster provisioning. Any additional software or license required must be provided on day 1.
HCI.REQ.0018	SW Feature	The Solution should allow for taking snapshots of individual Virtual Machines to be able to revert back to an older state, if any additional software license is required, it must be provided on day 1.
HCI.REQ.0019	SW Feature	Must support Instant space optimized point- in-time Snapshots. Should support atleast 24 snapshots.

Sl. No.	Component / Performance / Utility	Minimum Specification
HCI.REQ.0020	SW Feature	The proposed solution must support the automated rolling upgrades of hypervisor, storage software, and firmware with no VM or storage down time without requiring the VMs to be relocated to other cluster or storage platform to accomplish these non disruptive upgrades, all from a single GUI interface
HCI.REQ.0021	SW Feature	The solution design should have features like zero data loss and near zero downtime in case of disk, host, network, rack and site failure.
HCI.REQ.0022	SW Feature	No Single Point of Failure with complete redundancy at all levels. Nodes should be configured to have at least two copy of data available in cluster, in order to support data & cluster availability in event of One Node Failure
HCI.REQ.0023	SW Feature	The solution should be able to work on latest x86 server hardware available from all the leading OEMs in the industry and should not be restricted to a particular OEM.
HCI.REQ.0024	SW Feature	All servers in the HCI cluster must contribute Compute & Storage.
HCI.REQ.0025	SW Feature	The proposed solution must offer "native File Services" / "integration with File Services", supporting NFS 3.0/4.0, and SMB 2.0/3.0 with the ability to scale-out. if additional license needs to be factored for replication, factor the same from day-1
HCI.REQ.0026	SW Feature	Integration with backup solution proposed in this RFP to Backup and restore all type of configurations with rollback and recovery.
F	**Virtualization**	
HCI.REQ.0027	Virtualization	The proposed virtualization software shall provide a virtualization layer that sits directly on the bare metal server hardware with no dependence on a general purpose OS for greater reliability and security
HCI.REQ.0028	Virtualization	The solution shall provide the ability to expand vCPUs, memory , storage and vNICs (provided the same is supported by the guest operating system) without the need to reboot the workload
HCI.REQ.0029	Virtualization	The solution should provide capability to migrate existing physical/Virtual workloads to the proposed HCI solution with minimal disruption
HCI.REQ.0030	Virtualization	The solution shall provide zero-downtime/near zero down-time, zero-data loss continuous availability against physical host failures. This should be offered without any dependency on the guest operating system. The solution should also store a redundant copy of the data which is accessible immediately by the Hypervisor and application.

Sl. No.	Component / Performance / Utility	Minimum Specification
HCI.REQ.0031	Virtualization	The solution shall provide capabilities to limit I/O for virtual workloads to ensure that business critical VMs are not affected due to congestion by other VMs on the same host
HCI.REQ.0032	Virtualization	The proposed solution's Hypervisor(s) must offer "Live VM Migration", "High Availability" and intelligent placement of workloads on nodes best suited to their execution.
HCI.REQ.0033	Virtualization	Hypervisor shall provide automated live migration for initial placement and balancing of available resources with the rules to define affinity and / or anti-affinity of workloads
HCI.REQ.0034	Virtualization	The solution shall provide hyper converge software that allows delivery of enterprise class storage services using x86 server infrastructure without dependence on a separate SAN & associated component such as SAN switches & HBAs
G.	**Replication**	
HCI.REQ.0035	Replication	Proposed solution should support synchronous and asynchronous, local and remote replication to any x86 platforms as long as HCI SW is same and solution must support RPO of upto 5 minutes.
HCI.REQ.0036	Replication	The solution should provide orchestration layer to have automated disaster recovery. Unlimited VMs licenses should be provided for covering all the available compute & storage.
HCI.REQ.0037	Replication	The solution must allow changing of IP address and name of recovered Virtual Servers to match target data center.
H	**Disaster Recovery**	
HCI.REQ.0038	**Disaster Recovery**	The solution should have capability to test DR failover to separate network with no impact to production workloads.
HCI.REQ.0039	**Disaster Recovery**	The solution should have feature to assist in failback process to Primary data centre.
HCI.REQ.0040	**Disaster Recovery**	License not required on day 1, however, may require in future
I	**Security**	
HCI.REQ.0041	Security	Proposed solution should have the feature of encrypting data-at-rest at Software Defined Storage/ Hard disk level, using native or Third Party Key Management solution, which should be provisioned from Day 1
HCI.REQ.0042	Security	The proposed solution must offer Micro segmentation for VM-level security (at the vNIC).

Sl. No.	Component / Performance / Utility	Minimum Specification
J	**Cloud Management Platform**	
HCI.REQ.0043	Cloud Management Platform	Capacity Planning must be integrated into the proposed solution, showing both efficiency savings available to the deployed system (such as right-sizing workloads) and the predicted time remaining for RAM, CPU and Storage on the cluster (given "current" demand). Additionally, the planning should advise on what resources need to be added and allow administrators to model the behavior of the platform given additional (configurable) workloads
HCI.REQ.0044	Cloud Management Platform	The solution should have catalogue of private cloud services , ability to extend to public cloud services from day1, and should support self-service provisioning capabilities not limited to only HCI based solution but also for legacy architecture on X86 platform.
HCI.REQ.0045	Cloud Management Platform	The proposed solution should support application lifecycle management with automated orchestration across major hypervisor and cloud.
HCI.REQ.0046	Cloud Management Platform	The solution should provide authentication, authorization and accounting (AAA) out of the box like VM Access rights, Edit Rights, Delete Rights etc.
HCI.REQ.0047	Cloud Management Platform	The solution should provide ability to orchestrate third-party integrations via APIs to simplify the use of complementary IT service management tools and products likeload balancing and Firewall API
HCI.REQ.0048	Cloud Management Platform	The solution should have Life Cycle Management Work flows: Provisioning
HCI.REQ.0049	Cloud Management Platform	The Solution should have the capabilities for customization of dashboards
HCI.REQ.0050	Cloud Management Platform	The solution should provide capability of generating reports for usage & performance
HCI.REQ.0051	Cloud Management Platform	The proposed solution should have capability to create VPC (virtual private cloud) with capability to use same /different subnets/CIDR in different VPC's
HCI.REQ.0052	Cloud Management Platform	The solution shall provide an orchestration engine with ready workflows and ability to create custom workflows based on SOAP, REST operations and PowerShell scripts
K	**Nodes**	
HCI.REQ.0053	**Nodes**	Proposed cluster should have minimum 5 Nodes with single node failure.

Sl. No.	Component / Performance / Utility	Minimum Specification
HCI.REQ.0054	**Nodes**	CPU per Node: Minimum 2 Nos. x86 64 or higher Core processors with minimum 2.0 GHz clock speed of each processor
HCI.REQ.0055	**Nodes**	RAM per Node: Minimum 1 TB DDR5 min. 4800 MT/s or more PCI Gen5
HCI.REQ.0056	**Nodes**	**Network Ports per Node** 4 Nos. 25/10 Gbps with SFP+ 1 No. IPMI (Management Port)
HCI.REQ.0057	**Nodes**	**Power Supply and fans per node** Redundant and hot swappable power supplies and fans
L	**Storage Space**	
HCI.REQ.0058	**Storage Space**	Proposed solution should be configured with min 250 TB usable Storage (All Flash NVMe) with RF2/FTT1 and should tolerate 1 Node Failure, the proposed storage should have data savings features like compression, de duplication and erasure coding. Should have redundant Boot drives
M	**Firmware Code and Patch Management**	
HCI.REQ.0059	**Firmware Code and Patch Management**	The solution should provide seamless upgrade for (but not limited to) Firmware, Hypervisor, Storage OS, SDS software, BIOS and other such functions which are required in the solution.
HCI.REQ.0060	**Firmware Code and Patch Management**	All patches for the complete hardware and software solution must come from respective OEMs' authorized source and should be manageable/ upgradeable using GUI based console.
N	**Proactive Maintenance and Support**	
HCI.REQ.0061	Proactive Maintenance and Support	Proposed HCI solution should come with a proactive incident reporting and alerting which covers both Hardware components and full Software stack.
HCI.REQ.0062	Proactive Maintenance and Support	Proactive Maintenance feature should automatically have the ability to alert all hardware and hypervisor related alerts to the 24 x 7 Call centre of the DC without the need of external web access
HCI.REQ.0063	Proactive Maintenance and Support	Original Equipment manufacturer should have online 24 x 7 support for any hardware or software related issue
HCI.REQ.0064	Proactive Maintenance and Support	HCI solution must have direct OEM, L1, L2 and L3 support, 24x7x365 days with unlimited incident support (Telephonic / Web / Email) and technical contacts / contract with 30 minutes or less response time.

Sl. No.	Component / Performance / Utility	Minimum Specification
HCI.REQ.0065	**Warranty**	5 Years onsite comprehensive warranty including all other accessories related to smooth proposed HCI infrastructure from the date of successfully installation, commissioning, integration and final acceptance

5.46 CLOUD MANAGEMENT & ORCHESTRATION SOLUTION (CMOS)

Sl No..	Minimum Specifications
CMOS.REQ.001	The solution should provide simple and flexible deployment model with easy installer, automated environment replication and validation process, automated management of configurations, certificates, licenses, passwords, and users. Source control and version content with GitHub, GitLab or equivalent. Automate deployment of cloud content across multiple users and different environments.
CMOS.REQ.002	The solution should be able to automate and provision data-center services such as compute, storage, networking, container, backup, replication, load balancing, NAT, fault tolerance, security, virtual firewall, etc.It should have templates/bluprint that manage cloud resources to achieve infrastructure as code (IaC). Should support bare metal server provisioning through automation tool or via lifecycle management software.
CMOS.REQ.003	The solution should deliver a comprehensive, integrated product and lifecycle management solution for entire cloud to speed up deployments and updates, optimize and automate ongoing product and content management, and apply operational best practices across all components of cloud.
CMOS.REQ.004	The solution shall provide Unified, web-based, multi-tenant self-service IaaS, PaaS and XaaS, service catalog. Each tenant needs to be able to create their ownprofiles/blueprints, share them to a public catalog, and not be able to see other tenant's build profiles, compute resources, or managed machines
CMOS.REQ.005	The solution should provide flexibility in deployment with having cloud-independent VM/application profile coupled with its cloud-specific logic that abstracts the application from the specific cloud, interprets the needs of the application, and translates those logical needs to cloud-specific services and APIs. The tool should eliminate the need of cloud specific scripting/IaaS to prevent cloud lock-in.
CMOS.REQ.006	The solution should reduce cost and improve efficiency with real-time, ML-based capacity and cost metering parameters. Deliver optimal consolidation and proactive planning using a real-time, forward-looking capacity analytics engine, predict future demand and provide actionable recommendations that include reclamation, procurement and cloud migration planning options.
CMOS.REQ.007	The solution should provide support third-party/inbuilt agentless/agent guest introspection services like Antimalware/ Antivirus, HIPS/ HIDS and Stateful firewall etc. without requirement of installing agent inside Virtual Machine of windows and linux.
CMOS.REQ.008	The solution should be able to provide auto scale cloud resources based on resource utilization of VMs. The solution should provide horizontal and vertical auto scale. The software must allow the designer to create custom action for the team to use.
CMOS.REQ.009	The solution should automate the application and infrastructure delivery process with release pipeline management, including visibility and analytics into active pipelines and their status for troubleshooting and leverage existing tools and processes with out-of-the-box integration such as Ansible, Bitbucket, Github, Gitlab, IPAM, Puppet, Openshift, salt, terrafomr, bamboo, Docker, Docker Registry, Gerrit, GIT, Jenkins, Jira and TFs etc
CMOS.REQ.0010	The solution should have inbuilt orchestrator platform to build the custom workflow for complex tasks like cloning, re-sizing, snapshot, deletion etc. There should be zero manual intervention in this entire process across Cloud and also integrated configuration management capabilities to build the custom states for complex tasks for OS and Applications. Onboard the existing resources already running in environment including their resource dependencies.
CMOS.REQ.0011	Cloud Management Platform should provide out of the box compliance management for virtual/ cloud environments. Create custom compliance and enforce them through automatic remediation. Enforce IT regulatory standards with integrated compliance & automated drift remediation and adherence to common requirements out-of-the box compliance templatesas per applicable similar regulatory standards from Government of India, and creating own custom templates.

CMOS.REQ.0012	The solution should have ability for work flows to include business approvals
CMOS.REQ.0013	The solution should have capabilities around Configuration and Change Management work flows. Should have intend based workload balancing across clusters and ability to automatically take corrective action or call to external systems to effect change (workflow), open/close tickets or wait for approvals etc.
CMOS.REQ.0014	The solution should have Life Cycle Management Work flows: Extensible Capabilities to allow "Self-Management" work flows (Reboot/Restart, Migrate/Upgrade, Scale etc.)
CMOS.REQ.0015	The solution should integrate with any Software Defined Network (SDN) and provide simplified, programmable, application of network & security policy to deploy virtualized network functions (like switching, routing, stateful firewall, VPN, NAT, DHCP, container network & security and load-balancing) and allow for on-demand creation of security groups and policies.
CMOS.REQ.0016	The solution should provide out-of-the-box monitoring and troubleshooting for Packaged applications with Open-Source agentsto gather operating system metrics and monitor availability of remote platforms and applications. Capable of integrating with any application performance management tool.
CMOS.REQ.0017	Should be able to add all types of structured and unstructured log data, enabling administrators to troubleshoot quickly, without needing to know the data beforehand, perform long term Log retention and Log archival for future access and centralize log storage and analytics feature with Dashboards, Reports and Alerts with API integration for Automated Remediation.

5.47 VIDEO WALL& VIDEO WALL CONTROLLER

5.48 VIDEO WALL

S.No.	Parameters	Minimum Technical Requirements (either option 1 or option 2 to be complied)	
		Option **For Seamless single screen bezel less with external system controller**	**Option 2)** **Seamless single screen (bezel less) with embedded controller**
VW.REQ.001	Screen Size	Min "3000 mm (w) X 1687.5 mm (h) available in 5X5 tiles	Min 136" or higher, Bezel less (All-in-one) LED with Embedded System Controller
VW.REQ.002	Video Wall & Controller	Video Wall & Controller, Software should be from the Same OEM	Video Wall & Controller, Software should be from the Same OEM
VW.REQ.003	Native Resolution	Full HD (1920x 1080) pixels in 16:9 aspect ratio	Full HD (1920x 1080) pixels in 16:9 aspect ratio
VW.REQ.004	Technology	LED or better	LED or better
VW.REQ.005	Pixel pitch	1.56 mm or better	1.56 mm or better
VW.REQ.006	Light Source	LED light source with a minimum life time of 1,00,000 hrs. in Normal Mode & Eco Mode; Individual tile should be equipped with multiple LED banks and each LED bank should have an array of diodes. Single or multiple diode failure should not impact image display on the screen	LED light source with a minimum life time of 1,00,000 hrs. in Normal Mode & Eco Mode
VW.REQ.007	Refresh Rate	3840 Hz or higher for flicker free experience	3840 Hz or higher for flicker free experience
VW.REQ.008	Brightness on screen	500 nits or better	500 nits or better
VW.REQ.009	Brightness Uniformity	>95%	>95%
VW.REQ.0010	Colour	Should provide auto colour adjustment function and should be sensor based, automatic calibration system which works with an advanced colour sensor. The sensor continuously measures the	Should provide auto colour adjustment function and should be sensor based, automatic calibration system which works with an advanced colour sensor. The sensor continuously measures the primary levels of the entire wall and adjusts white point and colour when

S.No.	Parameters	Minimum Technical Requirements (either option 1 or option 2 to be complied)	
		Option **For Seamless single screen bezel less with external system controller**	**Option 2)** **Seamless single screen (bezel less) with embedded controller**
		primary levels of the entire wall and adjusts white point and colour when needed.	needed.
VW.REQ.0011	Screen	Min 160°or higher for both horizontal and vertical viewing angle	Min 160°or higher for both horizontal and vertical viewing angle
VW.REQ.0012	Contrast	3000:1 or more	3000:1 or more
VW.REQ.0013		System must be modular in installation; Dark box type stacking model is not acceptable	System must be modular in installation; Dark box type stacking model is not acceptable
VW.REQ.0014	IP Protection	IP20 or better	IP20 or better
VW.REQ.0015	Control	IP Based control; old IR based control should not be acceptable	IP Based control; old IR based control should not be acceptable
VW.REQ.0016	Remote	IP based control should also be provided for quick access; old IR based control should not be acceptable	IP based control should also be provided for quick access; old IR based control should not be acceptable
VW.REQ.0017	Screen to Screen Gap	Less than 0.5 mm Gap between 2 screens	Bezel-less
VW.REQ.0018	Terminal	Min 2x Input (DP1.2) Min 2x Input (HDMI2.0) Min 2x LAN Min 2x USB Min 1x Output (DP1.2)	Min 3 x HDMI Min 1X DP Min 1x LAN Min 1 x USB Control Port Audio out for Terminal
VW.REQ.0019	Power Consumption in Full Bright	Power Consumption for each VDU/Rear Projection Modules should be up to 320 Watts. This should be supported by datasheet.	Power Consumption for each VDU/Rear Projection Modules should be up to 320 Watts. This should be supported by datasheet.
VW.REQ.0020	Power Supply	100 – 240 VAC, 50-60Hz;	100 – 240 VAC, 50-60Hz; Power supply

S.No.	Parameters	Minimum Technical Requirements (either option 1 or option 2 to be complied)	
		Option **For Seamless single screen bezel less with external system controller**	**Option 2)** **Seamless single screen (bezel less) with embedded controller**
		Power supply	
VW.REQ.0021	Max Power consumption per unit area	336 W/m^2, 1146 BTU/h/m^2	336 W/m^2, 1146 BTU/h/m^2
VW.REQ.0022	Cooling Inside Tile	Any advanced cooling mechanism	Any advanced cooling mechanism
VW.REQ.0023	Maintenance Access	Tile should be accessible from the rear side for maintenance only	Maintenance access should also be available from the rear side
VW.REQ.0024	Control & Monitoring	Video wall should be equipped with a Tile control & monitoring system. It should provide options to view control layouts on remote devices such as tab, laptop, etc through web browsers	Video wall should be equipped with a control & monitoring system. It should provide options to view control layouts on remote devices such as tab, laptop, etc through web browsers
VW.REQ.0025		Should be able to control & monitor individual tile, multiple tiles and multiple video walls	Should be able to control & monitor individual or multiple views on a single screen
VW.REQ.0026		Should provide a virtual remote GUI over the IP to control the video wall	Should provide a virtual remote GUI over the IP to control the video wall
VW.REQ.0027		Status log file should be downloadable as per user convenience	Status log file should be downloadable as per user convenience
VW.REQ.0028	Sharing & Collaboration	It should be possible to share the layouts over LAN/WAN Network with Display in Meeting room or on Remote Workstations connected on LAN/WAN Network	It should be possible to share the layouts over LAN/WAN Network with Display in Meeting room or on Remote Workstations connected on LAN/WAN Network
VW.REQ.0029	Speakers	External	In-built
VW.REQ.0030	Support	5 years On-site comprehensive warranty with 24x7x365 hardware support	5 years On-site comprehensive warranty with 24x7x365 hardware support
VW.REQ.0031	Safety	India ETA/BIS	India ETA/BIS

S.No.	Parameters	Minimum Technical Requirements (either option 1 or option 2 to be complied)	
		Option **For Seamless single screen bezel less with external system controller**	**Option 2)** **Seamless single screen (bezel less) with embedded controller**
	Certifications		

5.49 VIDEO WALL CONTROLLER

S. No.	Parameters	Minimum Technical Requirements(Option 1)	Minimum Technical Requirements (Option 2)
VC.REQ.001	Display controller	Controller to be able to control mentioned video wall and should be based on the latest architecture.	For All-in-one single screen with embedded system controller, the same functionally should be achieved as specified in option 1.
VC.REQ.002	OS	Windows 10 or better, 64-bit	
VC.REQ.003	Processor	Xeon with 2 GHz or higher end processor	
VC.REQ.004	Cores	Octa core	
VC.REQ.005	RAM	Minimum 32 GB expandable to 64 GB	
VC.REQ.006	Chassis Type	19" or better Rack mount industrial chassis	
VC.REQ.007	Network	2 x 1Gb/s LAN	
VC.REQ.008	DVI/HDMI Inputs	4	
VC.REQ.009	Resolution Support for Outputs	Each o/p should have 4K support	
VC.REQ.0010	Hard disk	R.A.I.D-1 redundant setup with 2x 1000GB	
VC.REQ.0011	Tampering Alarm	Controller cover opening alarm	
VC.REQ.0012	Control	The system should have the capabilities of interacting (Monitoring & Control) with various applications on different network through the single Operator Workstation. It shall be possible to launch layouts, change layouts in real time using Tablet	
VC.REQ.0013	Keyboard & Mouse Extension	Keyboard and Mouse along with mechanism to extend them to 20mtrs. Operator desk from display controller to be provided	
VC.REQ.0014	24 x 7 operation	The controller shall be designed for 24 x 7 operation	
VC.REQ.0015	Redundancy	HDD, LAN, Power Supply	
VC.REQ.0016	Others	The Video Wall and the Controller should be of the same make to ensure better performance and compatibility	

S. No.	Parameters	Minimum Technical Requirements(Option 1)	Minimum Technical Requirements (Option 2)
VC.REQ.0017	OEM Certification	All features and functionality should be certified by the OEM.	
VC.REQ.0018		The Display Modules, Display Controller & Software should be from a single OEM.	
VC.REQ.0019	Operating System	Windows 10 64-bit IoT Enterprise	
VC.REQ.0020	Tampering Alarm	Controller cover opening alarm	
VC.REQ.0021	Output	DP/DVI/HDMI	
VC.REQ.0022	Input	H.264, MPEG2/4, MxPEG, MJPEG, V2D, H.263	
VC.REQ.0023	Dimensions	19" Rack mount	
VC.REQ.0024	Operating Conditions	100-240V ,10-5A, 50/60Hz, Redundant Power supply	
VC.REQ.0025	Operating Temperature	0° to 40°C | 32° to 104°F	
VC.REQ.0026	Humidity	Max. 80% Rh(non-condensing) at 40°C	
VC.REQ.0027	Noise Level	Max. 50dbA (measured at 1m/3.28ft distance at 22°C/72°F)	
VC.REQ.0028	Regulation Compliance	UL, CB, BIS, FCC, CE, IEC 60950, IEC 62368. This should be furnished along with bid documents	
VC.REQ.0029	Wireless	The operator should be also possible to show Laptop or Android/iOS phone over the video wall without disturbing the existing network over wireless	
VC.REQ.0030	Software	The software should be able to preconfigure various display layouts and access them at any time with a simple mouse click or schedule/timer based. Also, software has feature to show maximum, minimum and current brightness / colour values of all the projectors.	
VC.REQ.0031	Software	The software should be able display multiple sources anywhere on video wall in any size.	

S. No.	Parameters	Minimum Technical Requirements(Option 1)	Minimum Technical Requirements (Option 2)
		Key features of Video Wall management Software • Central configuration database • Browser based user interface • Auto-detection of network sources • Online configuration of sources, displays and system variables	
VC.REQ.0032	Software	Video Wall Control Software shall allow commands on wall level or tile level or a selection of tiles: • Switching the entire display wall on or off. • Setting all projection modules to a common brightness target, which can be either static (fixed) or dynamic to always achieve maximum (or minimum) common brightness between projection modules. • Fine-tune colour of each tile	
VC.REQ.0033	Software	Should support Multiple clients / Consoles to control the Wall layouts	
VC.REQ.0034	Software	The Software should be able to share layouts b/w available different videowalls on same network as well as preview of sources on the workstation	
VC.REQ.0035	Software	Software should enable the user to display multiple sources (both local & remote) up to any size and anywhere on the display walls (both local & remote).	
VC.REQ.0036	Software	The software should be able to create layouts and launch them as and when desired	
VC.REQ.0037	Software	The Display Wall and sources (both local & remote) should be controlled from Remote PC through LAN without the use of KVM Hardware.	
VC.REQ.0038	Software	Software should support display of Alarms	
VC.REQ.0039	Software	The software should provide at	

S. No.	Parameters	Minimum Technical Requirements(Option 1)	Minimum Technical Requirements (Option 2)
		least 2 layers of authentication	
VC.REQ.0040	Software	Software should able to Save and Load desktop layouts from Local or remote machines	
VC.REQ.0041	Software	All the Layouts can be scheduled as per user convince. Software should support auto launch of Layouts according to specified time event by user	
VC.REQ.0042	Software	It should be possible to create layouts comprising of screen scrapped content of Workstations, DVI inputs, Web sources, URLs configured as sources. Layouts can be pre-configured or changed in real-time.	
VC.REQ.0043	Software	It should be possible to schedule specific Layout based on time range It should be possible to share the layouts over LAN/WAN Network with Display in meeting room or on Remote Workstations connected on LAN/WAN Network	
VC.REQ.0044	Software	System should have a quick monitor area to access critical functions of the video wall User should be able to add or delete critical functions from quick monitor area Full featured Web services-based API supports Legacy RS-232 and TCP/IP. All software communication should be encrypted, Secure user Management with AD and LDAP Support Zero Maintenance, automatically saves the user's work.	
VC.REQ.0045	Software	Integrated Embedded & External Audio formats with Audio decoding of video streams also possible Software also supports UMD, IDC, Source name, Time (time zone aware), Date, text, Logo, Message Ticker, Source Status	
VC.REQ.0046	Software	The system shall include complete	

S. No.	Parameters	Minimum Technical Requirements(Option 1)	Minimum Technical Requirements (Option 2)
		Bi-directional Soft KVM to permit operators to take mouse & keyboard control of Displays, Screen Scrapped applications and DVI source	
VC.REQ.0047	Software	It should be possible to create two separate Tickers which run concurrently. These can be positioned at top or bottom and can run independently. The Ticker can be picked from data source through screen scrapping or through typing specific incidence, manually	
VC.REQ.0048	Software	The system should have the capabilities of interacting (Monitoring & Control) with various applications on different network through the single Operator Workstation. It shall be possible to launch layouts, change layouts in real time using Tablet	
VC.REQ.0049	Software	The control of the wall shall be possible via a network. All tiles shall have their own IP address, and the control software can access all of them at the same time. The available features shall be: On/Off, Brightness and Colour, Input control. Separate hardware server for monitoring features Wall or Panel On/Off, Brightness and Colour, Input control, health monitoring. Also, software has feature to show maximum, minimum and current brightness / colour values of all the projectors.	
VC.REQ.0050	Software	Central setup & Connection management, Central configuration database, fully distributed & modular component technology, Browser based UI, Auto-detection of network sources	
VC.REQ.0051	Software	Online configuration of sources, backup & restore, Scheduled backup, fully features web services-based API covering all legacy and	

S. No.	Parameters	Minimum Technical Requirements(Option 1)	Minimum Technical Requirements (Option 2)
		encrypted communications	
VC.REQ.0052	Software	Save and load layouts (complete display presets including perspectives and applications), start stop and position applications & sources freely over the complete desktop, remote keyboard and mouse control from and towards other networked desktops (bi-directional)	
VC.REQ.0053	Software	Supported sources: Analog & digital / streaming video, Analog (RGB) and Digital (DVI-I) Sources, Network desktops, Network multi-channel workstations and applications, Internet & internet sources, Embedded & external audio formats, Localization	
VC.REQ.0054	Modules	The Display Modules, Display Controller & Software should be from a single OEM	
VC.REQ.0055	Support	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support	

5.50 DESKTOP COMPUTER SYSTEMS (INTEL OR AMD)

5.51 INTEL PROCESSOR BASED COMPUTER SYSTEMS

S.No	Type	Parameter	Required Minimum Specification
INTELD.REQ.001	Processor	Generation	Intel® Core™ i7 Processor 11th Generation or higher.
INTELD.REQ.002		CPU Architecture	x64
INTELD.REQ.003		Speed (Min Base Frequency)	1.6 GHz or higher
INTELD.REQ.004		Turbo Frequency	4.9 GHz or higher
INTELD.REQ.005		Cores	Min. 8
INTELD.REQ.006		Threads	Min. 16
INTELD.REQ.007		Cache	16 MB or higher
INTELD.REQ.008	Mother Board	Sound/ Audio System	Integrated
INTELD.REQ.009		Memory	1x16 GB DDR-IV (2933 MHz) or higher expandable up to 64 GB (Min. 2 DIMM) or higher
INTELD.REQ.0010		Video Graphics	Integrated Graphics
INTELD.REQ.0011		PCI Slot	Minimum 1 PCI Express x 16
INTELD.REQ.0012	Hard disk Drive	512 GB SSD + 1 TB SATA (7200 RPM) or 1 TB SSD or higher capacity.	
INTELD.REQ.0013	Display	Screen Size	21" or more TCO 08 certified
INTELD.REQ.0014		Display Technology	Active Matrix TFT LCD (Backlit LED)
INTELD.REQ.0015		Resolution	1600x900 or higher
INTELD.REQ.0016	Keyboard	Standard USB OEM make	
INTELD.REQ.0017	Mouse	Optical/Laser USB OEM make	
INTELD.REQ.0018	Operating System	Preloaded OS	Windows 11 Professional 64 bit OEM or Higher
INTELD.REQ.0019		Additional OS supported	Linux
INTELD.REQ.0020	Miscellaneous	Ports, Security & Misc	Minimum 6 USB Ports (Out of which 3 USB 3.0 ports and minimum 2 USB ports should be at front), 10/100/1000 Ethernet Card, 1x VGA/DP, 1x Display Port/HDMI, Microphone & Stereo Headphone/ Combo port and other standard ports, TPM 2.0 or higher.
INTELD.REQ.0021		Power Supply	260 W or less Power supply (>=85% efficient), Active PFC or higher
INTELD.REQ.0022		Volume	<= 13.5 Liters
INTELD.REQ.0023	Warranty		Min 5 years OEM onsite comprehensive warranty.

5.52 REQUIRED CERTIFICATION

S.No	Category of Standard	Description	Name of Certification
INTELD.REQ.0024	Safety Standards	Safety of Electronics Products against Electrical Hazards	IS 13252(Part1):2010/ IEC 60950 Part1:2005/ UL Certification/ Equivalent Indian Standard
		Certification for Electro Magnetic Interference/ Radiation under control	FCC/Equivalent certification from NABL approved Lab
		Restriction of Hazardous Substances in manufacturing	India WEEE & India RoHS/ International RoHS
INTELD.REQ.0025	Energy Efficiency Standards	Energy Efficiency Standard	Energy Star 7.0 or higher/ Equivalent BEE Star rating
INTELD.REQ.0026	Environmental Standards	Environmental Protection Standard	EPEAT/ Equivalent Indian Standard
INTELD.REQ.0027	ISO standard	ISO 9001	ISO 9001

5.53 AMD PROCESSOR BASED COMPUTER SYSTEMS

S.No.	Type	Parameter	Required Minimum Specification
AMDD.REQ.0001	Processor	Generation	AMD Ryzan 7, 5000 Series or higher
AMDD.REQ.0002		CPU Architecture	x64
AMDD.REQ.0003		Speed (Min Base Frequency)	3.8 GHz or higher
AMDD.REQ.0004		Cores	Min. 8
AMDD.REQ.0005		Threads	Min. 16
AMDD.REQ.0006		Cache	20 MB or higher
AMDD.REQ.0007	Mother Board	Sound/ Audio System	Integrated
AMDD.REQ.0008		Memory	1x16 GB DDR-IV (2933 MHz) or higher expandable up to 64 GB (Min. 2 DIMM)
AMDD.REQ.0009		Video Graphics	Integrated Graphics
AMDD.REQ.00010		PCI Slot	Minimum 1 PCI Express x 16
AMDD.REQ.00011	Hard disk Drive	512 GB SSD + 1 TB SATA (7200 RPM) or 1 TB SSD or higher capacity.	
AMDD.REQ.00012	Display	Screen Size	21.0" or more TCO 08 certified
AMDD.REQ.00013		Display Technology	Active Matrix TFT LCD (Backlit LED)
AMDD.REQ.00014		Resolution	1600x900 or higher
AMDD.REQ.00015	Keyboard	Standard USB OEM make	
AMDD.REQ.00016	Mouse	Optical/Laser USB OEM make	
AMDD.REQ.00017	Operating System	Preloaded OS	Windows 11 Professional 64 bit OEM or Higher
AMDD.REQ.00018		Additional OS supported	Linux
AMDD.REQ.00019	Miscellaneous	Ports, Security & Misc	Minimum 6 USB Ports (Out of which 3 USB 3.0 ports and minimum 2 USB ports should be at front), 10/100/1000 Ethernet Card, 1x VGA/DP, 1x Display Port/HDMI, Microphone & Stereo Headphone/ Combo port and other standard ports, TPM 2.0 or higher.
AMDD.REQ.00020		Power Supply	260 W or less Power supply (>=85% efficient), Active PFC or higher
AMDD.REQ.00021		Volume	<= 15.5 L
AMDD.REQ.00022	Warranty		Min 5 years OEM onsite comprehensive warranty.

REQUIRED CERTIFICATION

S.No.	Category of Standard	Description	Name of Certification
AMDD.REQ.00023	Safety Standards	Safety of Electronics Products against Electrical Hazards	IS 13252(Part1):2010/ IEC 60950 Part1:2005/ UL Certification/ Equivalent Indian Standard

		Certification for Electro Magnetic Interference/Radiation under control	FCC/Equivalent certification from NABL approved Lab
		Restriction of Hazardous Substances in manufacturing	India WEEE & India RoHS/ International RoHS
AMDD.REQ.00024	Energy Efficiency Standards	Energy Efficiency Standard	Energy Star 7.0 or higher/ Equivalent BEE Star rating
AMDD.REQ.00025	Environmental Standards	Environmental Protection Standard	EPEAT/ Equivalent Indian Standard
AMDD.REQ.00026	ISO standard	ISO 9001	ISO 9001

5.54 LAPTOPS (INTEL OR AMD)

5.55 INTEL PROCESSOR BASED LAPTOPS

S.No.	Type	Parameter	Specification
INTELL.REQ.0001	Processor	Generation	Intel® Core™ i7 Processor 12th Generation or higher
		CPU Architecture	x64
		Efficient Core Max Turbo Frequency	3.4GHzorhigher
		Performance-core Max Turbo Frequency	4.7 or higher
		CPU Cores	Minimum 10
		CPU Threads	Minimum12
		Cache	Minimum 12MB or higher
		Wireless Connectivity	IEEE802.11ax (Wi-Fi 6),Integrated Bluetooth 5.1 or higher
INTELL.REQ.0002	Motherboard	Memory	1x16 GB DDR-IV (2933 MHz) or higher expandable up to 64 GB(with one DIMM free)
		Video Graphics	Integrated HD Graphics or better
INTELL.REQ.0003		Sound System	Integrated Stereo Speaker
INTELL.REQ.0004	Hard Disk Drive		(512GB SSD+ 1TB SATA HDD) or (1 TBSSD) Or higher
INTELL.REQ.0005	Display	Screen Size	14.0”orhigher
		Display Technology	Anti-glare LED Backlit Display
		Resolution	1920x1080orhigher
		Web Camera	Integrated HD Web Camera(720porhigher)
INTELL.REQ.0006	Keyboard		Spill Resistant backlit keyboard with Touch pad
INTELL.REQ.0007	Operating System	Preloaded OS	Windows11 Professional 64 bit OEM
		Additional OS Supported	Linux
INTELL.REQ.0008	Miscellaneous	Ports	Minimum 4 USB ports out of which 2 portshouldbeUSB3.0orhigherand1 port shall be Type C port with docking support,10/100/1000EthernetCard,VGA/HDMI, Microphone ,Stereo Headphone ,and other standard ports.
		Weight with Battery	Less than 2Kg
		Battery Backup	Minimum 6 hours
		Security	TPM 2.0 or higher
		Warranty	Minimum 3 years OEM on-site comprehensive warranty including battery
		Carry Case, charging adaptor	Good quality carry case/bag, Charging Adapter

Certification required: -

S.No.	Category of Standard	Description	Name of Certification.

INTELL.REQ.0009	Safety Standards	Safety of Electronics Products against Electrical Hazards	IS13252 (part1):2010/IEC60950Part1: 2005/UL certification/ Equivalent Indian Standard
		Certification for Electrical Magnetic Interference/Radiation under control	FCC/Equivalent Certification from NABL approved Lab,
		Restriction of Hazards Substance in manufacturing	India WEEE & India RoHS/ International RoHS
INTELL.REQ.00010	Energy Efficiency Standards	Energy Efficiency Standard	EnergyStar7.0 or Higher/Equivalent BEE Star rating
INTELL.REQ.00011	Environmental Standards	Environmental protection standard	EPEAT/Equivalent Indian Standard
INTELL.REQ.00012	ISO Standards	ISO9001	ISO9001

5.56 AMD PROCESSOR BASED LAPTOPS

S.No.	Type	Parameter	Specification
AMDL.REQ.0001	Processor	Generation	**AMD Ryzen 7, 5000 Series or Higher.**
		CPU Architecture	x64
		Speed(Min Base frequency)	2.0 GHz or higher
		Boost Clock Frequency	4.5 GHz or higher
		CPU Cores	Minimum 8
		CPU Threads	Minimum16
		Cache	Minimum 16MB or higher
		Wireless Connectivity	IEEE802.11ax (Wi-Fi 6), Integrated Bluetooth 5.1
AMDL.REQ.0002	Motherboard	Memory	1x16 GB DDR-IV (2933 MHz) or higher expandable up to 64 GB(with one DIMM free)
		Video Graphics	Integrated HD Graphics or better
		Sound System	Integrated Stereo Speaker
AMDL.REQ.0003	Hard Disk Drive		(512GBSSD+ 1TBSATAHDD) or (1 TBSSD) Or higher
AMDL.REQ.0004	Display	Screen Size	14.0"orhigher
		Display Technology	Anti-glare LED Backlit Display
		Resolution	1920x1080 or higher
		Web Camera	Integrated HD Web Camera (720p or higher)
AMDL.REQ.0005	Keyboard		Spill Resistant backlit keyboard with Touchpad
AMDL.REQ.0006	Operating System	Preloaded OS	Windows11 Professional 64 bit OEM
		Additional OS Supported	Linux
AMDL.REQ.0007	Miscellaneous	Ports	Minimum 4 USB ports out of which 2 portshouldbeUSB3.0orhigherand1 port shall be Type C port with docking support,10/100/1000EthernetCard,VGA/HDMI, Microphone, Stereo Headphone, and other standard ports.
		Weight with Battery	Lessthan2Kg
		Battery Backup	Minimum 6hours
		Security	TPM2.0orhigher
		Warranty	Minimum 3 years OEM on-site comprehensive warranty including battery
		Carry Case, charging adaptor	Good quality carry case/ bag, Charging Adapter

Certification required: -

S.No.	Category of Standard	Description	Name of Certification.
AMDL.REQ.0008	Safety Standards	Safety of Electronics Products against Electrical Hazards	IS13252 (part1):2010/IEC60950Part1: 2005/UL certification/Equivalent Indian Standard
		Certification for Electrical Magnetic Interference/Radiation under control	FCC/Equivalent Certification from NABL approved Lab,
		Restriction of Hazards Substance in manufacturing	India WEEE & India RoHS/ International RoHS
AMDL.REQ.0009	Energy Efficiency Standards	Energy Efficiency Standard	EnergyStar7.0or Higher/Equivalent BEE Star rating
AMDL.REQ.00010	Environmental Standards	Environmental protection standard	EPEAT/Equivalent Indian Standard
AMDL.REQ.00011	ISO Standards	ISO9001	ISO9001

Note: The Compliance should be submitted as per Minimum Technical Specifications on OEM & Bidder letterhead along with products /items Data Sheet for offered make & model.