e-Tender

for

Selection of System Integrator for Supply, Design, Installation, Commissioning with O&M of IT components for Haryana State Data Centre

Haryana State Electronics Development Corporation Limited
U00000CH1982SGC004963
Regd. Office: SCO 111-113, Sector 17-B Chandigarh-160017
Phone 0172-2704922
Phones (TDS Division): - 0172-2720113

Email: - sandeepv.hartron-hry@gov.in; Hartron.tds@gmail.com; rajeshpandey.ditech@hry.gov.in
Website:- https://etenders.hry.nic.in

INDEX

INTRODUCTION

Haryana State Electronics Development Corporation Ltd. (HARTRON) is a Haryana State Govt. undertaking and is a Nodal Agency of Government of Haryana for the procurement of Electronics & IT related Hardware & Software products.

State Data Center (HSDC) is operational since 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 17-F 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

HARTRON invitee-tender for Selection of System Integrator for Supply, Design, Build, Installation, Commissioning with O&M of IT components for Haryana State Data Centre **,** as per the terms and conditions specified in this tender document.

Please refer "Purchaser" as Citizen Resources Information Department (CRID) instead of Hartron in this RFP in all references. The Hartron is the Nodal department for tendering process.

SECTION 1

IMPORTANT INFORMATION

1.	Tender Inviting Authority Designation and Address	Haryana State Electronics Development Corporation Ltd. (HARTRON). Regd. Office: SCO 111-113, Sector 17B, Chandigarh
2.	Name of the Work	**Selection of System Integrator for Supply, Design, Installation, Commissioning with O&M of IT components for Haryana State Data Centre**
	Tender reference	e-Tender/Hartron/TDS/DC/2025-26/06
	Place of Execution	Chandigarh
3.	Tender document availability	Tender Notice & Tender Document is available at **https://etenders.hry.nic.in** from 9:00 AM onwards
	Approximate tender value	Rs. 50 Crores
	Processing Fee for Tender	The Payment for Tender Document Fee ₹5,900/- (Rupees Five Thousand Nine Hundred Only) i.e. (₹5,000/- + 18% GST) and ₹1,180/- eService Fee i.e. (₹1,000+18% GST)can be made by eligible bidders through Online Mode at NIC Portal in favor of Haryana State Electronics Development Corporation Limited. Scanned copy of Online Payment Receipt should be uploaded with technical e-bid.
	Earnest Money Deposit (EMD)	The Payment for EMD (refundable) of Rs.5,00,000/- (Rupees Five Lacs only) can be made by eligible bidders through Online Mode Available on NIC Procurement Portal). Scanned copy of Online Payment Receipt should be uploaded along with technical bid.
		The Payment of Rs.45,00,000/- (Rupees Forty-Five Lacs only) also will be made by eligible bidders in the form of Bank Guarantee (BG) in favor of Director (Administration), Citizen Resources Information Department, Room no-42, 9th floor, Haryana Civil Secretariat, Sector-1, Chandigarh-160001 and will be submitted along with the technical bid in original.
	Performance Bank Guarantee	The successful bidder(s) will submit total Performance Bank Guarantee (PBG) amounting to the 10% of the total project order value. This 10% PBG shall be split in 5 different PBGs with value as per section 6.7.5 **PBG release schedule** and shall be released in time period mentioned in this schedule. All PBGs to be issued in favor of Director (Administration), Citizen Resources Information Department, Room no-42, 9th floor, Haryana Civil Secretariat, Sector-1, Chandigarh-160001 , a**nd submitted as per timeline mentioned in clause 7.8**.If the rate contract is extended, the PBGs shall also be extended similarly by the successful bidder(s).
4.	Starting date of Tender	**22.07.2025 onwards**
5.	Pre-bid meeting	The pre-bid queries (if any) may be submitted by prospective bidders via email at sandeepv.hartron-hry@gov.in; Hartron.tds@gmail.com; rajeshpandey.ditech@hry.gov.in, , before **01.08.2025** After the due date & time, no pre-bid queries will be entertained.
6.	Pre-bid meeting	The pre-bid meeting will be held on **04.08.2025** at 2:30 PM in conference room HARTRON Bhawan, Bays no. 73-76, Sector-2, Panchkula.
7.	Last date and time for submission of e-Tender	**21.08.2025 by 03.00 PM**
8.	Last date for submission of hard copy of technical bid to HARTRON.	**21.08.2025 by 3:30 PM** (Hard Copy of Technical bid with proper binding and indexing as uploaded on e-procurement portal by the respective bidder must be submitted by bidder in the O/o DGM (TDS) HARTRON Bhawan, Bays No. 73-76, Sector2, Panchkula.)

9.	Date and Time of Opening of Technical Bids	**28.08.2025 by 03.00 PM**
10.	Date and Time of Opening of Commercial Bids	To be intimated later on
i. Eligibility Criteria: Please refer to the Section 4 of the Tender Document. ii. Two Bid System i.e.Stage-1 Prequalification cum Technical Bid; Stage-2 Commercial Bid. iii. Tenders received after due date and time will be summarily rejected. iv. Any Bid not conforming to the format will be summarily rejected.		

Note:

1. Bidders are advised to visit the e-procurement portal i.e.https://etenders.hry.nic.in of Haryana Govt. on regular basis for updates/corrigendum issued by Hartron related to the tender.

2. The bidder shall submit hardcopy of technical e-bid as uploaded on NIC Portal in a properly indexed and page-numbered format, with the document title included. The index and page numbers must be placed at the beginning of the bid document and must comply with the requirements specified in the tender documents.

3. Bidders are required to submit hardcopy of their technical e-bid as uploaded on NIC Portal in a properly bound format to ensure that all pages remain together and in the correct order during handling, review or evaluation.

4. If loose papers in hardcopy of technical e-bid as uploaded on NIC Portal are attached with paper clips / thread will not be accepted, and the bidder shall be solely responsible for any loss or damage that may result from such submission.

SECTION 2

INSTRUCTION TO BIDDERS ON ELECTRONIC TENDERING SYSTEM

1. Bidder should do Online Enrolment in this Portal using the option Click Here to Enroll available in the Home Page. Then the Digital Signature enrollment has to be done with the e-token, after logging into the portal. The e-token may be obtained from one of the authorized Certifying Authorities such as e-Mudhra CA/GNFC/IDRBT/MtnlTrustline/SafeScrpt/TCS.
2. Bidder then logs into the portal giving user id / password chosen during enrollment.
3. The e-token that is registered should be used by the bidder and should not be misused by others.
4. DSC once mapped to an account cannot be remapped to any other account. It can only be inactivated.
5. The Bidders can update well in advance, the documents such as certificates, work order details etc., under My Documents option and these can be selected as per tender requirements and then attached along with bid documents during bid submission. This will ensure lesser upload of bid documents.
6. After downloading / getting the tender schedules, the Bidder should go through them carefully and then submit the documents as per the tender document; otherwise, the bid will be rejected.
7. The BOQ template must not be modified/replaced by the bidder and the same should be uploaded after filling the relevant columns, else the bidder is liable to be rejected for that tender. Bidders are allowed to enter the Bidder Name and Values only.
8. If there are any clarifications, this may be obtained online through the eProcurement Portal, or through the contact details given in the tender document. Bidder should take into account of the corrigendum published before submitting the bids online.
9. Bidder, in advance, should prepare the bid documents to be submitted as indicated in the tender schedule and they should be in PDF/XLS/RAR/DWF formats. If there is more than one document, they can be clubbed together.
10. Bidder should arrange for the EMD as specified in the tender. The original should be posted/couriered/given in person to the Tender Inviting Authority, within the bid submission date and time for the tender.
11. The bidder reads the terms and conditions and accepts the same to proceed further to submit the bids.
12. The bidder has to submit the tender document(s) online well in advance before the prescribed time to avoid any delay or problem during the bid submission process.
13. There is no limit on the size of the file uploaded at the server end. However, the upload is decided on the Memory available at the Client System as well as the Network bandwidth available at the client side at that point of time. In order to reduce the file size, bidders are suggested to scan the documents in 75-100 DPI so that the clarity is maintained and also the size of file also gets reduced. This will help in quick uploading even at very low bandwidth speeds.
14. It is important to note that, the bidder has to click on the Freeze Bid Button, to ensure that he/she completes the Bid Submission Process. Bids Which are not Frozen are considered as Incomplete/Invalid bids and are not considered for evaluation purposes
15. In case of Offline payments, the details of the Earnest Money Deposit(EMD) document submitted physically to the Department and the scanned copies furnished at the time of bid submission online should be the same otherwise the Tender will be summarily rejected
16. The Tender Inviting Authority (TIA) will not be held responsible for any sort of delay or the difficulties faced during the submission of bids online by the bidders due to local issues.

17. The bidder may submit the bid documents online mode only, through this portal. Offline documents will not be handled through this system.
18. At the time of freezing the bid, the eProcurement system will give a successful bid Updating message after uploading all the bid documents submitted and then a bid summary will be shown with the bid no, date & time of submission of the bid with all other relevant details. The documents submitted by the bidders will be digitally signed using the e-token of the bidder and then submitted.
19. After the bid submission, the bid summary has to be printed and kept as an acknowledgement as a token of the submission of the bid. The bid summary will act as a proof of bid submission for a tender floated and will also act as an entry point to participate in the bid opening event.
20. Successful bid submission from the system means, the bids as uploaded by the bidder is received and stored in the system. System does not certify for its correctness.
21. The bidder should see that the bid documents submitted should be free from virus and if the documents could not be opened, due to virus, during tender opening, the bid is liable to be rejected
22. The time that is displayed from the server clock at the top of the tender Portal, will be valid for all actions of requesting bid submission, bid opening etc., in the e-Procurement portal. The Time followed in this portal is as per Indian Standard Time (IST), which is GMT+5:30. The bidders should adhere to this time during bid submission.
23. All the data being entered by the bidders would be encrypted at the client end, and the software uses PKI encryption techniques to ensure the secrecy of the data. The data entered will not be viewable by unauthorized persons during bid submission and not viewable by any one until the time of bid opening. Overall, the submitted bid documents become readable only after the tender opening by the authorized individual.
24. During transmission of bid document, the confidentiality of the bids is maintained since the data is transferred over secured Socket Layer (SSL) with 256-bit encryption technology. Data encryption of sensitive fields is also done.
25. The bidders are requested to submit the bids through online eProcurement system to the TIA well before the bid submission end date and time (as per Server System Clock).
26. The bidders are requested to submit the bids through online eProcurement system to the TIA well before the bid submission end date and time **(as per Server System Clock)**.

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 for Selection of System Integrator for Supply, Design, Installation, Commissioning with O&M of IT component for Haryana State Data Centre 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

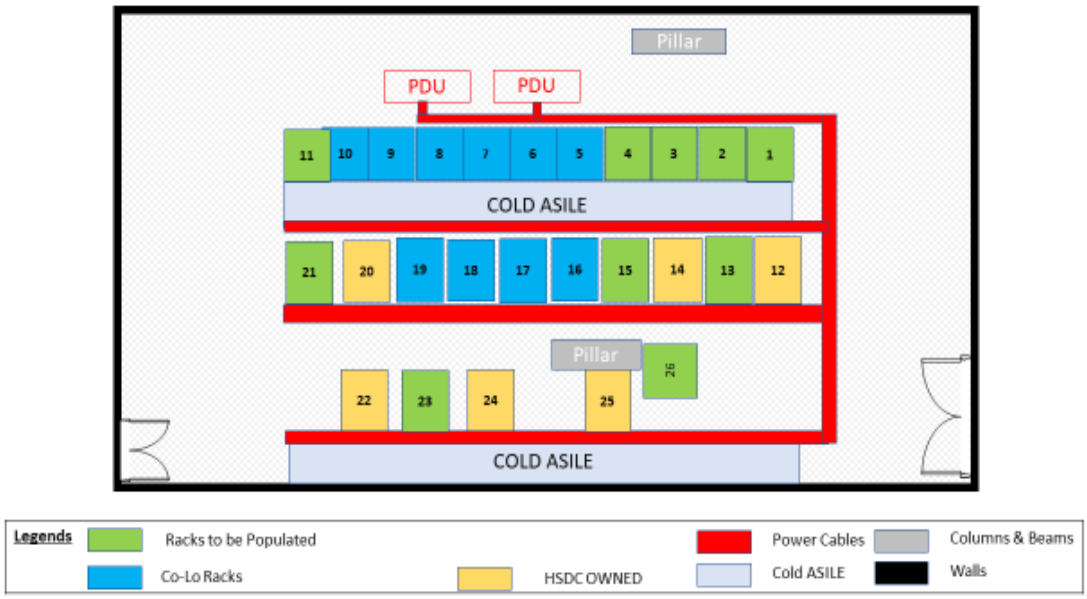
State Data Center (HSDC) is operational since 14-08-2012 and is now managed by CRID, Haryana and MSP RailTel Corporation of India Ltd. ((RAILTEL) a Mini Ratna Category-1 enterprise) Govt. of India undertaking, Ministry of Railways w.e.f. 01.01.2015.Haryana State Data Centre is located in Sector 17F in 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.

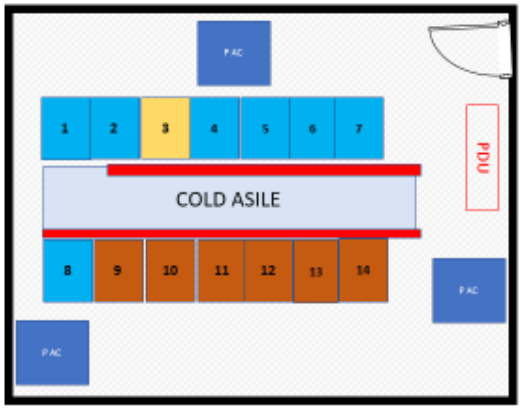
e) * Rest of Racks 7,8 i.e. 2 Racks are in pure colocation in SDC Server farm area.

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 existing ICT infrastructure under the scope of present MSI i.e. M/S Railtel India Corporation Ltd. In this regard, Annexure-18 may be referred along with HOTO process. 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

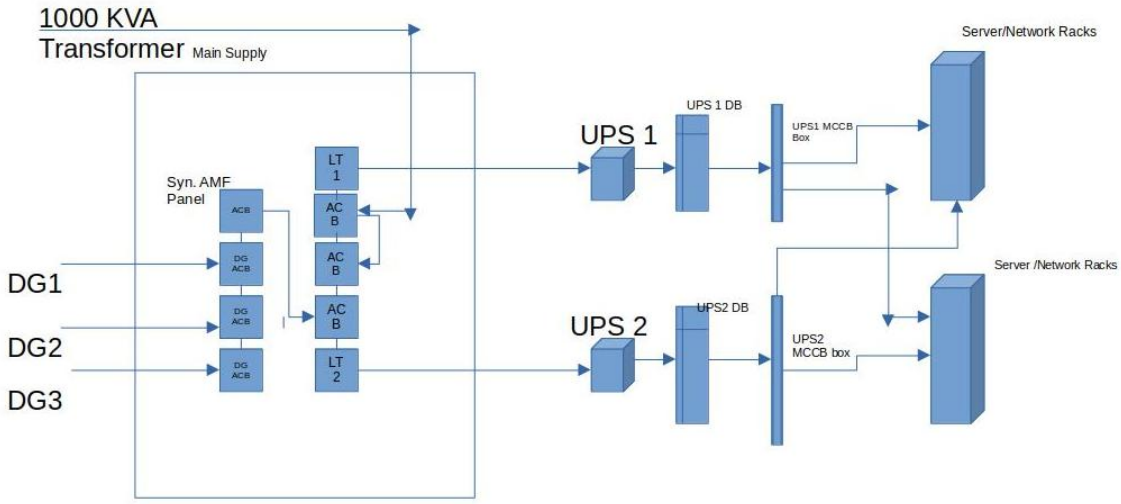


Figure 1: Existing Electrical Architecture of HSDC

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. should be part of the respective solution offered by respective OEM/SI including required.
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 and their integrations will be allowed subject to the approval of the competent authority.
8. 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.

9. 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.
10. 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 of role-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 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 : The Security parameters mentioned for existing infrastructure as per annexure-18 shall also be applicable for new infrastructure installed and commissioned under the scope of this RFP.

    Note: Above value added service will be applicable to scope of MSI when related system software/appliances are covered under BOQ of this RFP or will be provided separately by CRID. For example : EDR for Antivirus and APM. for monitoring services, Operating system etc. may be provided separately while backup software/ backup appliance are covered in this RFP.

Component-wise Migration/ Up gradation Plan:

Hosting Infrastructure

HSDC 1.0 has 100+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 SI by the CRID(SDC team) and application owner for smooth migration.

Step 1: Four 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 .

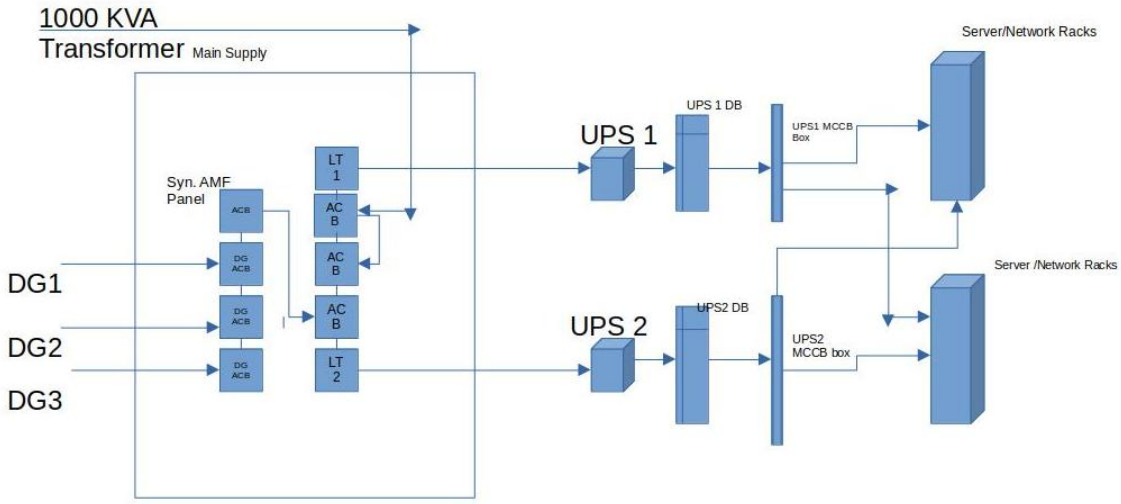


Figure-2 Electrical Architecture for HSDC

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, **25** critical applications need 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 based on availability of infrastructure 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 Co-location 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, NOC services, etc 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 Departments with 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 Go Live 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 by CRID**.**

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

a) BMS and all of its sub-systems as mentioned at Section 1.2.4 are 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. 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 services should contain (but not limited to following), the details of which shall be incorporated at the time of signing of actual agreement:

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

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

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.

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.

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

The MSI would develop an optimum list of services that 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, cooling etc. is available to cater maximum 34 numbers of racks along with the other utility areas like BMS, Staging & NOC etc. In separate connectivity room , respective Telecom racks are also provided by respective ISPs.

The ICT infrastructure for Haryana 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 of supplied ICT infrastructure as per BOQ mentioned in this RFP along with operation and maintenance of entire existing HSDC infrastructure may not go beyond 34(approx) racks for a period of minimum one year after go live and further extendable to one more year, if

required. 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 test the BoQ items

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

b. HCI Cloud node server Infrastructure

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

d. Security infrastructure such as Firewalls, DDOS, WAFetc.,

e. Virtualization and Cloud Management – Orchestration layer (On premise Service offering)

f. SAN switches, Purpose Built Backup Appliance & Backup software etc.

g. Operation and maintenance Services for a period of 1 year 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 SI 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 1 year in order to perform operation and management for all ICT components as per scope of the RFP after go-live. O&M of manpower support is initially for first year and is extendable on annual basis up to the period of 5 years. 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 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

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, WAF,etc.

   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.

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 as per the scope of this RFP. Racks will be loaded with network, security, compute, storage, hypervisor, virtualization, orchestration etc.

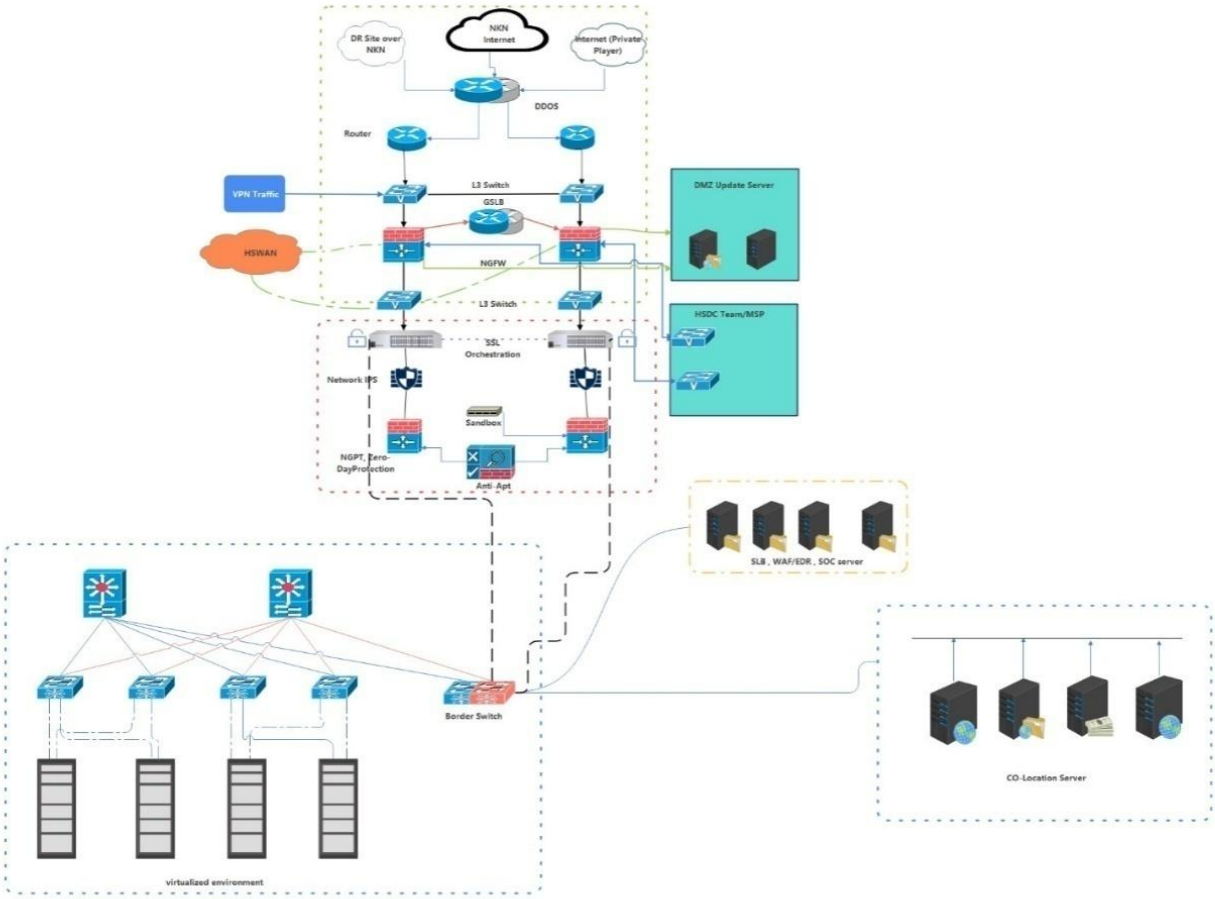


Figure-3 Logical Schematic diagram of transformed HSDC

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 must integrate with minimum of 3 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 next generation 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:

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.

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 scales compute and allocation of available storage as and when needed without any downtime.

l. **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.

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 and related equipment in the Data Centre as per scope of this RFP.
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 minor Civil 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 5 years from Go-live (In case if any product is declared EOS during the mentioned 5 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 and should have no dependency on underlying hardware 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". In case, any item does not come with PERPETUAL licenses, the SI shall provision subscription licenses for scope of work as per this RFP.

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 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 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) 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 on-boarding 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)

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

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.

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.	Service Management	ISO 20000 latest specifications
3.	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
iii. The cost to engage independent auditors or PMU shall be born by CRID.

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 • 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 as per RACI matrix. • 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 IT component of the DC sites. Set-up the services and processes as per the desired standards, Centralized SDC Service Desk & Self-service portal Implementation &Management
c) Phase III: Operations and Maintenance services for the IT component of DC

Phases

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

i) MSI should understand, analyze and examine the current state of the H**S**DC in discussion and knowledge transfer from the current/existing 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" 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 MSI and 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/operator(refer Annexure 18) 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 IT component at DC

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

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.

After successful commissioning and FAT completions of the project, MSI will 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

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 will ensure to continue AMC/CAMC or ATS of usable infrastructure 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 maintenance of all IT components as per this RFP is the responsibility of bidder.
- 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 SetupNetwork & Cyber Security Implementationincluding 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. 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) will be managed by MSI, all expenses will be born by CRID.
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 Authorized 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:

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, 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 implementation plan 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 – III: OPERATION AND MAINTENANCE SERVICES

MSI will operate and maintain all components as per this RFP with 5 years On-site comprehensive warranty support after Go Live acceptance**. O&M of manpower support is initially for first year and is extendable on annual basis up to the period of 5 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.

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 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

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

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 optionshould 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 program 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 15 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
	DC- 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- Cloud solution Expert including HCI	L3(1) L2(1)	2	100%	8x6	1
4.	DBA	L3(1) L2(1)	2	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

The above proposed manpower in Information Security should be well capable of managing all equipment in DC with demonstrable experience in 1 or more domains of security.. 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;"

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.

Apart from the -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.	Project Manager (L4)	Mandatory: Educational Qualification in BE / B. Tech / M.Tech / MCA from recognized Institute, with PGDM/ MBA from recognized 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.	DC-DR Cloud Solution Expert (L3/L2)	Mandatory: Educational Qualification in BE / B. Tech / MCA and 5+(for L3)/4 (for L2) 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
3.	DBA(L3/L2)	BE/B.Tech/MCA with minimum 5(for L3)/4(for L2) 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), Oracle
4.	Network and Security Expert(L3/L2)	BE/B.Tech/MCA with minimum 5(for L3)/4(for L2) Years of Experience in network system provisioning, configuration, and management a. Relevant Firewall OEM related Certification (Mid/Professional Level) as per Bidder's Solution
5.	Storage and Backup Expert (L3/L2)	BE/B.Tech/MCA with minimum 5(for L3)/4 (for L2) Years of Experience in Storage Implementation & Management. a. Relevant Storage OEM related Certification (Mid/Professional Level) as per Bidder's Solution
6.	Server Expert /System Administrator(L3/L2)	BE/B.Tech/MCA with minimum5(for L3)/4(for L2) Years of Experience in Server Administration. a. Windows/Linux Server related Certification (Mid/ Professional Level)
7.	Server Expert /System Administrator(L1)	BE/B.Tech/MCA with minimum 3 Years of Experience in Server Administration / Configuration. a. Windows/Linux Server related Certification (Entry/Associate Level)
8.	BMS Expert (L3)	BE/B.Tech/MCA in Electrical/Electronics/Computer or Post Graduate Diploma or certification in BMS 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
9.	BMS Expert (L2/L1)	a. Diploma/ITI/ Polytechnic Diploma (IT) in Electrical with minimum 4(for L2)/3(for L1) Years of Experience in Electrical Solution Implementation/Monitoring
10.	NOC Engineer (L1)	BE/B.Tech/MCA/Polytechnic Diploma (IT) with minimum 3 Years of Experience in Network/Server Configuration/Performance Monitoring.
11.	Help Desk Engineer (L1)	BE/B.Tech/MCA/Polytechnic Diploma (IT) with minimum 3 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.
vii. MSI to keep supporting/office staff to help deployed manpower in their day-to-day office working.

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

Sl. No.	Activities	CRID	PMC	Present MSI	MSI	Line Department
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
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

Sl. No.	Activities	CRID	PMC	Present MSI	MSI	Line Department
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 shall direct 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. Power supply from multiple grid at HSDC
iii. AMC for servers/storage provided for Co-Lo rack

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- Cloud Solution Expert (L3)						
4		Network and Security Expert (L3)						
5		Storage and Backup Expert (L3)						
6		Server Expert /System Administrator (L3)						
		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**	(List all tasks to be performed under this project)			

	Tasks Assigned	

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	• Agent- Installation, Configuration, Modification, Un-installation • Backup- New Backup	• Adding new devices to fabric • OS installation, Un-installation • Patch- Update, Remove

• 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 • VTL Failure • Virtualisation Network Failure • Virtualisation Infrastructure Failure • Threshold Alarm (Critical)	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 component connecting the above equipment's • Signature Update • Server Reboot Request • User Account Locked • VM Provisioning Failure	• 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 • 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 period of 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 management SLAs on-IT Infrastructure related SLA

Note: O&M SLAs will be applicable for all applications hosted at DC 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+4Weeks to <=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+28 Weeks**	Nil
	>T+28 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 : Delivery of all ICT components (Hardware + Software)	**T+12 Weeks**	Nil
	>T+12 Weeks to <=T+16 Weeks	Penalty at 0.5% shall be imposed on the respective CAPEX value for State Data Center and Far DR
	>T+16 Weeks	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

Go-Live & Integration SLAs

Measurement	Target	Penalty
Milestone-Commissioning, UAT, Go-Live with hands-on training/ hand-holding. Declaration of start of O&M	**T+28 Weeks**	Nil
	>T+28 Weeks to <=T+32 Weeks	Penaltyat0.5%shallbeimposedonthe respective CAPEX value for DC Site & Far DR site
	>T+32 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

Infrastructure Consolidation and Rationalization Study SLAs

Measurement	Target	Penalty
Milestone -Perform SDC Drills to check functionality: Sign-off of consolidation and capacity augmentation plan	**T+ 28 Weeks**	Nil
	>T+ 28 Weeks to <=T+32 Weeks	Penalty at 0.5% shall be imposed on the Total CAPEX value
	>T+ 32 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 Overall UPTIME SLA

Penalty for Service and Equipment Failure (for the Data Centre 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	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: 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: 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 up to 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 5 Cr**
    - **For First to2nd year (as per Schedule) : 16% of PBG value = Rs 80 Lakh.**
    - **If Penalty = 1% of Yearly PBG Value then the Penalty = Rs 8 thousand**
    - **For 3rd year (as per Schedule) : 20% of PBG value = Rs 1 Cr.**
    - **If Penalty = 1% of Yearly PBG Value then the Penalty = Rs 10 thousand**
- **Similarly**
    - **For 4th & 5th Year (as per Schedule) = 24% of PBG value = Rs 1.20 Cr**
    - **If Penalty = 1% of Yearly PBG Value then the Penalty = Rs 12 thousand**

:: 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.	Measurement	Definition	Measurement Interval	Target	Penalty
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 Centre infrastructure or its facilities shall Be communicated	Monthly	100% Incidents to be reported to CRID within 1 hour with the cause, action,	No Penalty

Sl.	Measurement	Definition	Measurement Interval	Target	Penalty
		Immediately to CRID as an Exceptional report Giving details of Downtime, if any.		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 CRID. For e.g. Switch, Servers etc.	Monthly	100% as per the inventory log committed and maintained by MSI.	Rs.10000foreve rynon-compliance
7.	Manpower	Absence of resource	Monthly	100% on site deployment	Inability of MSI to deploy manpower resource/resources as per Manpower requirement specified

Sl.	Measurement	Definition	Measurement Interval	Target	Penalty
					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

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 U**PTIME 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 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
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/NVR system availability, availability of CCTV recording –180days 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	
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	<= 8 hours	No Penalty

	respective ICT components after go-live	> 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 4

A. Bill of Materials:-

1. HSDC Site (CAPEX-BOQ)

Sl	BOQ ITEM	QTY
1	Rack Server 128 Core (14 U)	7
2	HCI Solution for 5 Node	1
3	Core Switch HA	2
4	SAN Switch	2
5	TOR Switch	4
6	L3 Switch	4
7	Server Virtualization Software (Latest version) (for 14 sockets (64core per socket) in 7 server)	1
8	Cloud Automation, Orchestration & Management (for 14 sockets (64core per socket) in 7 server)	1
9	SDN	1
10	Server Load Balancer	2
11	Distributed Denial-of-Service(DDOS)	1
12	SSL Decryptor & SSL Encryptor	2
13	Internal Firewall	2
14	External Firewall	2
15	Web application firewall (WAF)	2
16	Purpose Built Backup Appliance	1
17	Backup Software	1
18	Enterprise Monitoring Solution (EMS), Network Monitoring Solution (NMS)	1
19	DNS Server	4

Note: - The bidder must be submitted Annexure-16 on their letterhead by complying the same in their offer.

2. OPEX BOQ

Sl	BOQ ITEM	QTY
1	Operation & Maintenance	1

B. ELIGIBILITY CRITERIA

4.1 This RFP is open to all firms/companies within India, who are eligible to do business in India under relevant Indian laws as in force at the time of bidding.

4.2 Firm/company declared by GoH to be ineligible to participate for corrupt, fraudulent or any other unethical business practices shall not be eligible during the period for which such ineligibility is declared.

4.3 In case the entity is a defaulter in paying any dues to any of the Government Departments, the entity is not eligible for the tender. The bidder should submit affidavit as placed at Annexure-12 & 13 in the technical bid.

4.4 Breach of any of the conditions of this tender document, work order, arrangement, contract with GoH may attract a proceeding to declare a firm/company ineligible for a certain period or certain number of consecutive tender calls at the option of HARTRON.

4.5 The concessions/benefits to MSEs and medium Enterprise are as per Haryana State Public Procurement Policy for MSMEs-2016, issued by Govt. of Haryana, Department of Industries & Commerce vide G.O. 2/2/2016-4IBII (1) dated 20.10.2016, Amendment Memo No. 2/3/2018-4IB-II dated 23.04.2018 and 2/2/2016-4I-BII dated 13.08.2021 and amendment thereof if any, Manufacturing Micro and Small Enterprises (MSEs including Khadi and Village Industries/Units) who have filed Entrepreneur Memorandum in Haryana in respect of the quoted items participate directly in tender and do not through any intermediaries (their dealers/agents. distributors), will not subcontract to any other firm and to carry the entire manufacturing at their enterprise. Concerned MSE will be required to submit a copy of Entrepreneur Memorandum in respect of its category of Micro/Small issued to the firm by the Industries Department Haryana as a part of technical bid.

4.6 Preference to Make In India criterion as per Notification of Department of Industries & Commerce, Government of Haryana i.e. "Haryana State Public procurement (Preference to Make in India)-2020, will not be applicable.OM for this MII exemption along with the list of items for which this exemption is applicable is given at Appendix 4: Make in India preference exemption order.

4.7 Any Bidder not meeting even one of the qualification criteria as mentioned below shall be summarily rejected. The Bidders shall enclose documentary evidence for fulfilling the Eligibility in the Technical Bid. If a bidder fails to enclose the documentary proof for eligibility, their bid will be summarily rejected.

Minimum Eligibility Criteria:

1. Pre-Qualification Criteria

Sl	Eligibility Requirement	Supporting Documents Required
1.	Processing fee for Tender should be submitted.	The Payment for Tender Document Fee is ₹5,000/- (Rupees Five Thousand only) + ₹1,180/- eService Fee (including 18% GST) can be made by eligible bidders through Online Mode at NIC Portal in favor of Tendering Authority. Scanned copy of Online Payment Receipt should be uploaded with technical e-bid.
2.	EMD fee	The Payment for EMD (refundable) of **Rs. 5,00,000/- (Rupees Five Lacs only)** can be made by eligible bidders through Online Mode Available on NIC Procurement Portal). Scanned copy of Online Payment Receipt should be uploaded along with technical bid.
		The Payment of **Rs. 45,00,000/- (Rupees Forty-Five Lacs only) also will be made by eligible bidders in the form of Bank Guarantee (BG)** in favor of Director (Administration), Citizen Resources Information Department, Room no-42, 9th floor, Haryana Civil Secretariat, Sector-1, Chandigarh-160001 and will be submitted along with the technical bid in original.

2. Eligibility Criteria

Sl	Eligibility Requirement	Supporting Documents Required

Sl	Eligibility Requirement	Supporting Documents Required
1.	The Bidder must be incorporated and registered in India under the Indian Companies Act 1956 or 2013, or a Limited Liability Partnership (LLP) registered under the LLP Act, 2008 or Indian Partnership Act 1932 and should have been in operation in India for a minimum of seven years as on Bid Submission Date.	i) Copy of Certificate of Incorporation / Registration under Companies Act 1956/2013 Articles of Association Partnership Deed for Partnership Firms
2.	The Bidder should have an average annual turnover of at least **Rs 100 Cr** from the IT System Integration or Information Technology Infrastructure Projects Including implementation, operations & maintenance	i) Audited Balance sheet and Profit & Loss account statement or CA Certificate or Statutory Auditor Certificate of the Bidder for each of the last 3 Financial Years FY 2021-22, 2022-23, 2023-24, Considered balance sheet and loss & Profit statement of FY 2024-25 (if audited).
3.	The bidder should have positive net worth (measured as paid up capital plus free reserves) in last 3 Financial Years FY 2021-22, 2022-23, 2023-24, Considered balance sheet and loss & Profit statement of FY 2024-25 (if audited).	i) CA Certificate or Statutory Auditor Certificate of the Bidder confirming the net-worth and profit after Tax for each of the last 3 financial years. ii) The net worth of the Bidder firm (manufacturer or principal of authorized representative) should not be negative and also should have not eroded by more than 30% (thirty percent) in the last three financial years.
3.	The Bidder should possess all below certificationsor latest which are valid as on bid submission date: 1. ISO 9001:2008 or ISO 9001:2015 or 2018 for Quality Management System 2. ISO or IEC 20000: 2011 for IT Service Management 3. ISO 27001:2013 for Information Security Management	i) Copies of the valid certificates from authorized agencies.
5.	The Bidder should have: PAN card GST Registration Number	i) Copies of the valid certificates from authorized agencies a) Income Tax registration or PAN number GST Registration Certificate

Sl	Eligibility Requirement	Supporting Documents Required
6	The Bidder should have experience in Supply, Design, Build, Installation, Commissioning with Operations and Maintenance **of IT components for Data Center** (Tier-IV/ Tier-III / Tier-II) for any Centre or State or UT Govt or PSU or National BFSI or National TSPs from Apr 2018 to till bid submission date (Only ICT Infra, manpower etc. excluding construction of building): a) **Three** (3) completed/ongoing orders each having minimum value of Rs 20 Cr (~40% of the estimated tender value) or more. OR b) **Two** (2) completed/ongoing orders each having minimum value of Rs 25 Cr (~50% of the estimated tender value) or more. OR c) **One** (1) completed/ongoing order of value Rs 40 Cr (~80% of the estimated tender value) or more. In last 7 financial years i.e. 2018-19, 2019-20, 2020-21, 2021-22, 2022-23, 2023-24, 2024-25 **IT components (as per BOQ of this RFP)** which includes Servers and network switching & routing and Security components(Firewall, DDoS, WAF, etc) and Virtualizations, HCI and Backup system, etc	i) Contract signed with client clearly highlighting the Scope of Work, Bill of Material and value of the Contract/order ii) Completion Certificate issued & signed by the competent authority of the client entity on the entity's letterhead (For completed project) iii) Bidder project experience of on-going projects with at least management (IT & Non IT) of minimum 5 racks in O&M phase shall be considered when a) Go Live certificate signed by the authorized signatory of the client entity on the entity's letterhead for in order to ensure that the project is in Go Live phase or b) Certificate signed by the authorized signatory of the client entity on the entity's letterhead for in order to ensure that the project-t is in O&M phase and is being run by the SI (initiated or completed or ongoing since Apr 2017 to till as on bid submission date) iv) In Case the desired tier certificate is not available /expired, the bidder to submit uptime Certificate of 99.74% or above issued & signed by the authorized signatory of the client entity on the entity's letterhead for consideration.
7.	The Bidder should have experience of at least one (1) order of Supply, Design, Build, Installation, Commissioning with Operations and Maintenance of a Data Center (Tier-IV/ Tier-III / Tier-II) site for any Centre or State or UT Govt or PSU or National BFSI or National TSPs in last 7 financial years i.e. 2018-19, 2019-20, 2020-21, 2021-22, 2022-23, 2023-24, 2024-25 as on bid submission date of at least value of Rs 25 Crores (Only in ICT Infra excluding construction of building).	i) Contract signed with client clearly highlighting the Scope of Work, Bill of Material and value of the Contract/order ii) Completion Certificate issued & signed by the competent authority of the client entity on the entity's letterhead (For completed project) iii) In case the project is on-going the Go Live certificate is required issued & signed by the authorized signatory of the client entity on the entity's letterhead iv) In Case the desired tier certificate is not available / expired, the bidder to submit uptime Certificate of 99.74% or above issued & signed by the authorized signatory of the client entity on the entity's letterhead for consideration.

Sl	Eligibility Requirement	Supporting Documents Required
8.	The Signatory signing the Bid on behalf of the Bidder should be duly authorized by the Board of Directors of the Bidding Company to sign the Bid on their behalf.	i) A Certificate from the Company Secretary of the Bidder certifying that the Bid signatory is authorized by the Board of Directors of the Company to do so, with acceptance of board resolution, resolution number and date
9.	Bidder shall have office or local contact available in Tri-city (Chandigarh, Mohali and Panchkula)	i) Copies of rent agreement or proof of ownership of office or address detail of local contact in Tri-city (Chandigarh, Mohali and Panchkula) if available. OR ii) In case there is no existing office or local contact, an undertaking from the authorized signatory to establish the local contact or open the office within one month (30 days) from the date of award of contract in Tri-city (Chandigarh, Mohali and Panchkula)
10.	OEM Criteria 1.The OEM should be in the manufacturing of offered products or equivalent during any 3 out of 5 financial years (2020-21,2021-22,2022-23, 2023-24, 2024-25) 2. The OEM should have executed orders of quantity 300% of required tender quantity of the respective product with nearly similar type or configuration or size. The orders should be executed on behalf of any Central or State Govt or PSUs or National BFSI or National TSPs during the last 5 years as on bid submission date(2020-21,2021-22,2022-23,2023-24,2024-25). 3. OEM of offered products must have their own Technical service & support Centre in India. 4. Authorization from OEM for confirming that the products quoted are not "end of life or end of sale products" shall be available for next 5 years from achieving Go-Live of the project. 5. Undertake that the support including spares, update, upgrades, fixes, patches for the quoted products shall be available for next 5 years from achieving Go-Live of the project. 6. Undertaking from OEM to support directly, if needed, including delivery against defectives also within the scope of project (A certificate from OEM to provide support for the products with pre-qualification bid) 7. Undertaking for the proposed supplied equipment/product in the tender to discharge all responsibilities under warranty for the period indicated in the contract	1. Work orders or contract Agreement or Supply Order. 2. Work Order or Contract Agreement or Supply Order. 3. Documentary evidence for support center in India to be provided. 4 & 5. Documentary evidences such as Authorization letters MAF (Manufacturer's Authorization Form) from all OEMs whose products are being quoted by the Bidder need to be attached in the proposal as per format provided in RFP. 6 & 7. Self-Certification or Declaration Certificate or affidavit duly signed by authorized signatory on company letter head
11.	Compliance from Bidder & OEM for detailed technical specifications of all the Products offered in this bid as per Bill of material (BOM)	i) The bidder must enclose with a self-declaration the item wise compliance for the technical specifications duly vetted by

Sl	Eligibility Requirement	Supporting Documents Required
		the respective OEMs specific to this tender on respective OEM's letterhead. The Model and Make/Version of the offered products should be clearly specified in the compliance document(Bill of material (BOM))
12.	Undertaking by Bidder & its OEMs 1. Not be insolvent, bankrupt or being wound up, not have its affairs administered by a court or a judicial officer, not have its business activities suspended and must not be the subject of legal proceedings for any of the foregoing reasons; 2. Not blacklisted with any of the State or Central Government as on the date of submission of the bid. 3. No Dispute with Bidder or their OEM as on date of submission of bid related to supply/execution/implementation of any item placed by CRID(DITECH) or HARTRON. 4. Undertaking from Bidder or Parent Company or major promoter of the OEMs directly/indirectly shall not be from or belong to the countries sharing land borders with Indian Territory. OR Bidder or its OEM from a country that shares a land border with India will be eligible to bid in this tender only if the bidder is registered with the Competent Authority. Bidder or its OEM has to undertake compliance as per Notification No:02/09/2020 – 4IB – II Dated 10-12-2020 of the Department of Industries & Commerce Govt. of Haryana. Any false declaration and non-compliance of this would be a ground for immediate termination of the contract and further legal action in accordance with the laws 5. Undertaking from Bidder & its OEM that they are registered entity in India & have direct presence in India for more than 5 years as on bid submission date 6. In case of additional purchase, If at any time during the execution of the contract the SI reduces the sale price or sells or offers to sell such scope of work as are covered under the contract, to any person or organization including the purchaser or any department of Central Government/State Government at a price lower than the price chargeable under the Contract, he/she shall forthwith notify such reduction or sale or offer of sale to the purchaser and the price payable	i) Self-Certification or Declaration Certificate or affidavit duly signed by authorized signatory on company letter head and as indicated in MAF (Manufacturer's Authorization Form)

Sl	Eligibility Requirement	Supporting Documents Required
	under the contract for the supplied Bills of Quantity after the date of coming into force of such reduction or sale or offer of sale shall stand correspondingly reduced. An undertaking to this effect must be submitted along with tender.	

Note :

1. PSU : Public Sector Undertaking
2. TSP : Telecom Service Provider
3. BFSI : Banking Financial Services and Insurance
4. UT : Union Territory

3. Project Milestone & Deliverables

T0= WO Date/Contract Agreement signing Date

Sl	Timeline/Milestone	Milestone
1	**T0** = **WO Date/Contract Agreement signing Date** T1=T0+4 Weeks	Submission of Documents: HOTO of existing DC, Requirement Study, Design document (Technical & Functional, Drawings), Project Plan, Implementation plan along with Delivery Schedule for all BOQ Items
2	T2=T1+ 8 weeks	Delivery of all BOQ Items
3	T3=T2+ 2 weeks	Inspection of all BOQ Items
4	T4=T3+ 4 weeks	Installation, Testing, Operationalization of all BOQs at DC Site with Hands-on Training/Hand-holding
5	T5=T4 + 8 weeks	Commissioning, UAT, migration & Go Live with Hands-on Training/Hand-holding. Declaration of Start of O&M
6	T9 = T8 + 2 weeks	Perform DC Drills

Note : The delivery schedule of BOQ Items at respective location should be in line with planned installation and commission sequence as per shared approved plan with purchaser considering the following as :

i. Items which will install first, should be supplied first considering dependency.

ii. If there is requirement of installation of two BOQs items in parallel, both must be supplied together.

iii. Bidder has to require confirmation from purchaser before final delivery/ies as per approved plan.

4. Payment Schedule

Sl	Timeline/Milestone	Milestone	Payment
1	T0 = WO Date/Contract Agreement signing Date T1=T0+4 Weeks	Submission of Documents as per project milestone & deliverables	10% mobilization advance of total contract value excluding OPEX and warranties beyond first year on receipt of 10% PBG of total contract value
2	T2=T1+ 8 weeks	Delivery of all BOQ Items	
3	T3=T2+ 2 weeks	Inspection of all BOQ Items	• 70% of Capex amount of all delivered & inspected BOQs • And submission of 10% additional BG of the CAPEX amount of this phase i.e. all BOQ items (Active & Passive) required to implement this phase for a period of 1 year. Document to be submitted for release of Payment: • Invoices & delivery challans dully signed by the Inspection Committee as per the clause mentioned in section 8.2 Inspection of Items
4	T4=T3+ 4 weeks	Installation, Testing, Operationalization of all BOQs at DC Site with Hands-on Training/ Hand-holding (Phase 1)	
5	T5=T4 + 8 weeks	Commissioning, UAT, migration & Go Live with Hands-on Training/Hand-holding. Declaration of Start of O&M	• 15% of Capex amount of all BOQs commissioned & Go Live • (Release of 10% additional BG submitted under delivery & inspection stage after 1 year or Go live date + 3 months, whichever is later) (exemption only w.r.t migration delays if any can be accorded by the SS IT with defined T&C)
6	T9 = T8 + 2 weeks	Perform DC Drills	TOTAL Go Live Release of balance 5% of Capex amount of all BOQs commissioned & Go Live

<table>
<tr><th>Sl</th><th>Schedule</th><th>Payment</th></tr>
<tr><td>1</td><td>O & M Cost Payable Quarterly basis with equal installment shall be paid quarterly after verification of SLAs.

O&M costs includes deployed man power for first year after Go Live. From first year onwards manpower +warranties of the infrastructure on pro-rata basis shall be considered.

<table>
<tr><th>Sl</th><th>Year 1</th><th>Year 2</th><th>Year 3</th><th>Year 4</th><th>Year 5</th></tr>
<tr><td>Manpower</td><td>Yes</td><td>No</td><td>No</td><td>No</td><td>No</td></tr>
<tr><td>Warranty</td><td>Yes</td><td>Yes</td><td>Yes</td><td>Yes</td><td>Yes</td></tr>
</table>
</td><td>Based on Invoice value applicable for that quarter with deduction of SLA/Penalties if any.</td></tr>
</table>

RFP General Terms & Condition

Right to vary quantity

a. At the time of award of contract, the quantity of goods, works or services originally specified in the bidding documents may be increased or decreased. It shall be without any change in the unit prices or other terms and conditions of the bid and the bidding documents

b. If the purchaser does not procure any subject matter of procurement or procures less than the quantity specified in the bidding documents due to change in circumstances limited to variation up to 25% of the total quantity **(if the quantity is greater than equal tounit of measure)**, the Bidder shall not be entitled for any claim or compensation except otherwise provided in the bidding document. **In case the quantity is less than 4 units, the Purchaser reserves the right to procure 1 unit of measure of the equipment specified.**

c. Repeat orders for extra items or additional quantities may be placed limited to variation up to 25% of tender value (as indicated above) for next 2 years from the date of project Go Live on the rates and conditions given in the contract.

d. In case of delivery of any extra item or additional quantity, dollar or foreign currency hedging clause/ provisions would be applicable. In that case, the bidders would need to indicate the import content(s) and the currency (ies) used for calculating the value of import content(s) in their total quoted price, which (that is, the total quoted price) will be in Indian Rupees. The bidder to also indicate the Base Exchange rate for each such foreign currency used for converting the foreign exchange content into Indian Rupees at the time of bidding. Any increase or decrease in price by reason of the variation in the rate of exchange in terms of the contract will be borne by the bidder, if the prices are within or equal to 15% of variation. However, at the time of additional purchase, if there is a variation beyond 15% of the foreign currency/ dollar value, both parties shall bear 50% of the variation cost beyond 15%.

Any Bid failing to meet the above stated Qualification criteria shall be summarily rejected and will not be considered for Financial Evaluation.

SECTION 5

MINIMUM TECHNICAL SPECIFICATIONS

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. Bidders are required to fill the technical performa at annexure-4 and submit the technical brochures along with the technical bid . 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. 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

COMPUTE AND STORAGE

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	2U Rack Mounted or 1U Rack mounted with all the required features ,redundancy ,functionalities as per RFP
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	1 TB DDR 5 RAM with ECC 4800 Mhz 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
SER.REQ.0013	Power & temperature	Platinum rated redundant Hot plug Power Supplies Should support hot plug redundant power supplies with minimum 89% 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.
		  ○ Encrypted virtual media
		  ○ Server Health Logging
		  ○ Out of Band Management
		• 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/tags for Asset 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

S. No.	Parameter	Minimum Specifications
		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 **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	1000 Or higher

S. No.	Parameter	Minimum Specifications
	(must be available on SPEC dot ORG before evaluation)	
SER.REQ.0021	SPEC fp_rate_2017 for the product (must be available on SPEC dot ORG before evaluation)	1000 Or higher

NETWORKING

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)
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.

S.No.	Parameter	Minimum Specifications
		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

SPINE CORE SWITCH

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 or BGP-EVPN with VxLAN
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

S.No.	Parameter	Minimum Specification
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 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

S.No.	Parameter	Minimum Specification
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

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 48x1G/10G/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
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

S.No.	Parameter	Minimum Specifications
		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 64k 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
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

S.No.	Parameter	Minimum Specifications
		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
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

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 4xQSFP+ (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	Should support QOS 802.1p class of service, marking, classification, policing and shaping and at least eight egress queues.
L3C.REQ.0021	The switch/ switch series and Switch OS should be EAL3/NDPP/NDcPP certified under Common Criteria.
L3C.REQ.0022	All required Cables, Accessories and Licences should be provided from Day-1
Warranty & Post warranty Support	
L3C.REQ.0023	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support
L3C.REQ.0024	Switches supplied/offered must be SDN ready from day 1 & compatible with SDN solution offered under this RFP

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/ISIS 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 SDN controller / Fabric manager 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 SDN controller / Fabric manager Server is not present for any reason. There must not be any relationship between the Central SDN controller / Fabric manager 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 the capability to design (stage) the networking Fabric as one, i.e. not switch-by-switch, through a single interface.
SDN.REQ.0013	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.0014	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.0015	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.0016	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.0017	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.0018	The solution should provide real-time monitoring of various parameter of the network using real-time state streaming telemetry or better technology.
SDN.REQ.0019	The controller/fabric should have centralised dashboard to upgrade the entire fabric with ease without incurring traffic downtime in fabric core. The System must integrate with 3rd-party systems through open APIs for additional reporting, with the minimum of time series databases and graphing applications.

S. No.	Minimum Specifications
SDN.REQ.0020	All the hardware, software and licenses must be included as part of the solution as per the required specification from Day 1
SDN.REQ.0021	Technical support for solution must be directly from single OEM. OEM should have 24x7 available over email and Phone.
SDN.REQ.0022	1. Solution offered for SDN controller / Fabric manager must be compatible with all network devices offered under this RFP & All licenses should be provided with the devices for the mentioned features. The licenses 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 Licenses if Subscription must be supplied for duration of scope of the project in this RFP + 2 years
SDN.REQ.0023	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.0024	SDN controller/ Fabric manager 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.0025	Controller/Fabric should be capable to show in real time congestion hotspots in the network with buffer level utilization info from the network devices or simplify troubleshooting of connectivity and performance problems.
SDN.REQ.0026	The solution is expected to provide real time 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), anamoly/deviation analysis, bug/PSIRT visibility, device resource utilization, traffic flow analytics with streaming telemetry.
SDN.REQ.0027	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

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 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

BACKUP

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	PBBA VTL Appliance should be expandable up to minimum usable 2 PB Front-end capacity from Day 1. The solution 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 or 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 50 TB/hr (at target side) Or more, considering without deduplication compression ratio and encryption. Deduplication and compression must be ensured at target/backup appliance end.
PBBA.REQ.0011	Feature	Scheduling:
PBBA.REQ.0012		Backup software used in PBBA should be able to retrieve data from tape to client server directly.
PBBA.REQ.0013		Audit, logs & reports e.g. de-duplication report, Data growth analysis report, Compute/Network 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		Subsequent Replication should transfer only difference data from previous successful replication.
PBBA.REQ.0016		Replication should provide the flexibility to transfer only dedup data.
PBBA.REQ.0017		Should provide compression of data while replication.
PBBA.REQ.0018		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-in time 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 as per scope of this RFP.
PBBA.REQ.0023	Warranty& Post warranty Support	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

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 or instance 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. 150 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. 100 TB Front End Capacity or required number of instance based license to meet 100 TB 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 or instance 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
BKPS.REQ.007	The software shall be able to Compress and Encrypt data at the Client-side and

<table>
<tr><th>S.No.</th><th>Minimum Specifications</th></tr>
<tr><td></td><td>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/solution shall support file archival 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 or 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 or required instance based license.
BKPS.REQ.0024	Capacity or required instance 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 or required instance 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 or indirectly.
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: Full job completion report. Overview of the full backup jobs that were successful, partially successful and failed for each day.
BKPS.REQ.0039	Full backup data volume report. Overview of the total data volumes that were backed up for each day.
BKPS.REQ.0040	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	Should support source based deduplication while image level backup.

S.No.	Minimum Specifications
BKPS.REQ.0043	Should support granular recovery from image level backup.
BKPS.REQ.0044	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 supportVTL, NFS. CIFS for proposed backup disk appliance
BKPS.REQ.0054	Must support source capacity based licensing or instance 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

S.No.	Minimum Specifications
	control to regulate the level of management
BKPS.REQ.0061	The solution should have the capability to manage and monitor backups at remote 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 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

Cyber Security

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 minimum 20 Gbps of L7 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+
WAF.REQ.0012	HA Deployment	The WAF should support HA deployment (Active/Active or Active/Passive)

S.No.	Parameter	Minimum Specifications
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

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 of DITECH/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 shall not be End-of-support by the OEM for 5 years from the date of bid submission
INTFW.REQ.006	The appliance should not have any active internal or external Wi-Fi, Bluetooth, NFC components.
	Specification
INTFW.REQ.007	The proposed firewall solution/platform shall run on a hardened OS and delivered on purposeful built hardware and security appliance.
INTFW.REQ.008	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.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.
INTFW.REQ.0010	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 Solution shall support configuration of dual stack gateway on a bond interface or on a sub-interface of a bond interface.
INTFW.REQ.0011	Firewall OS, CVE (Common Vulnerabilities and Exposures) must be available/disclosed on public web sites

S.No.	Minimum Specifications
INTFW.REQ.0012	It shall be possible to centrally manage Firewall and all the associated modules/ functionalities/ services over secure channel.
INTFW.REQ.0013	solution/platform shall be supplied with the support for all standard static and dynamic routing protocols.
INTFW.REQ.0014	The solution/platform shall support VLAN tagging (IEEE 802.1q).
INTFW.REQ.0015	Solution/platform shall have integration with Identity Awareness Capabilities on the security appliance via Active Directory or RADIUS.
INTFW.REQ.0016	Solution/platform shall support Application awareness and granular control functionalities for all the commonly available Web 2.0 applications and tools.
INTFW.REQ.0017	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.0018	Solution/platform shall support Link aggregation functionality (LACP/PAGP) to group multiple ports as single Channel.
INTFW.REQ.0019	Solution/platform shall not have any licensing restriction on number of users and shall be supplied for unlimited users unless specified otherwise.
INTFW.REQ.0020	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 day one
INTFW.REQ.0021	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.0022	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.0023	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 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.0024	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 - 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.0025	Proposed appliance/platform must have integrated redundant hot-swappable power supplies
INTFW.REQ.0026	The proposed firewall/solution architecture should have control/management

S.No.	Minimum Specifications
	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.0027	The proposed solution/platform hardware should be a multicore CPU architecture with a hardened 64-bit operating system to support higher memory and should supplied with appropriate/higher RAM to support required performance in this RFP for this Firewall from day 1 considering future scalability without changing the existing hardware.
INTFW.REQ.0028	The firewall/solution must have at least usable 480GB (SSD) storage from day 1.
	Network Protocols/Standards Support Requirements
INTFW.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
INTFW.REQ.0030	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.0031	The proposed firewall/platform shall be able to handle unknown /unidentified applications with actions like allow, block or alert.
INTFW.REQ.0032	The proposed firewall/platform shall have granular application identification technology based upon deep packet inspection.
INTFW.REQ.0033	The proposed firewall/platform shall warn the end user with a customizable page when the application is blocked.
INTFW.REQ.0034	The proposed firewall/platform shall delineate specific instances of instant messaging/Social Network Applications (Facebook Chat, WhatsApp, Telegram, WeChat etc.).
INTFW.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.
INTFW.REQ.0036	The Firewall/platform shall provide stateful engine support for all common protocols of the TCP/IP stack.
INTFW.REQ.0037	The Firewall/platform shall provide NAT functionality, including dynamic and static NAT translations.
INTFW.REQ.0038	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.0039	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 categories for operational efficiency
INTFW.REQ.0040	Solution should support the following authentication protocols: - LDAP - Radius (vendor specific attributes) - Token-based solutions (i.e. Secure-ID) - Kerberos

S.No.	Minimum Specifications
	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.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.
INTFW.REQ.0042	b) Network Address Translation (NAT) shall be configurable as 1:1, 1: many, many: 1, many: many.
INTFW.REQ.0043	c) Reverse NAT shall be supported.
INTFW.REQ.0044	d) Port address translation /Masquerading shall be supported.
INTFW.REQ.0045	Dynamic Host Configuration Protocol (DHCP)& Virtual Private Network (VPN) shall be supported
INTFW.REQ.0046	The firewall/platform shall support Internet Protocol Security (IPsec).
INTFW.REQ.0047	Key exchange with latest Internet Key Exchange (IKE), Public Key Infrastructure PKI (X.509) shall be catered to.
INTFW.REQ.0048	Support Latest Encryption algorithms including AES 128/192/256(Advanced Encryption Standards), 3DES etc.
INTFW.REQ.0049	Support Latest Authentication algorithms including SHA-1(Secure Hash Algorithm-1), SHA-2(Secure Hash Algorithm-2) etc.
INTFW.REQ.0050	IPsec NAT traversal shall be supported.
	Firewall Policy Requirements
INTFW.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 (After Integration with AD) d) Customizable services e) Combination of one or multiple of above mentioned parameters
INTFW.REQ.0052	The Firewall/platform shall be able to filter traffic even if the packets are fragmented.
INTFW.REQ.0053	It shall support the VOIP Applications Security by supporting to filter SIP, H.323, MGCP etc.
INTFW.REQ.0054	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 (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.

S.No.	Minimum Specifications
	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.0055	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.0056	Should have more than 11,000 (excluding custom signatures) IPS signatures or more.
INTFW.REQ.0057	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to security events.
INTFW.REQ.0058	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.0059	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.0060	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.0061	User-developed application & IPS signatures: The application control & IPS function shall allow to create new application & IPS signatures.
INTFW.REQ.0062	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.0063	Solution must have tracking mechanism for the changes done on policy management dashboard and maintain audit trails.
INTFW.REQ.0064	The Firewall Management Solution, log server and reporting server can be either hardware appliance or VM based solution.
INTFW.REQ.0065	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.0066	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

S.No.	Minimum Specifications
	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.0067	PIM-SM, PIM-SSM, IGMP v1, v2, or v3
INTFW.REQ.0068	The offered firewall solution must be a appliance and should be provided with redundant Fans and power supplies
INTFW.REQ.0069	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.0070	Solution should have n Multi-tier engine to detect & prevent Command and Control IP/URL and DNS.
INTFW.REQ.0071	Firewall Policies : 45,000 or more
	Management & Logging/Reporting
INTFW.REQ.0072	The management must be accessible via a web-based interface and ideally with no need for additional client software
INTFW.REQ.0073	The management solution must be capable of role-based administration
INTFW.REQ.0074	The solution must provide multiple report output types or formats, such as PDF, HTML, and CSV.
INTFW.REQ.0075	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.0076	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.0077	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.0078	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.0079	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.0080	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.0081	The firewall should support TLSv1.2 and TLSv1.3 decryption and also supports Outbound and Inbound inspection.
INTFW.REQ.0082	Should support SLAAC Stateless Address Auto configuration
INTFW.REQ.0083	The proposed firewall must have support for mobile protocols like GTP, SCTP.
INTFW.REQ.0084	The proposed solution should support the ability to create QoS or rate-limiting 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.0085	Bidirectional Forwarding Detection (BFD)
INTFW.REQ.0086	The Solution should support DNS security
INTFW.REQ.0087	**Monitoring, Management and Reporting**

S.No.	Minimum Specifications
INTFW.REQ.0088	Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis
INTFW.REQ.0089	Should have built in report templates base on Applications, Users, Threats, Traffic and URLs
INTFW.REQ.0090	Should be able to create report based on SaaS application usage or application usage
INTFW.REQ.0091	Should be able to create reports base user activity
INTFW.REQ.0092	Should be able to create custom report base on custom query base any logging attributes
	Authorization
INTFW.REQ.0093	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.0094	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

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.
EXTFW.REQ.0015	The solution/platform shall support VLAN tagging (IEEE 802.1q).

S.No.	Minimum Specifications
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 6 million concurrent sessions on L4 or at least 1 million concurrent session on L7 and minimum 400,000 new connections per second on L4 from day 1 or minimum 110,000 new connections per second on L7 from day 1 and scalable to at least 12 million concurrent sessions on L4 or at least 2 million concurrent sessions on L7 and minimum 800,000 new connection per second on L4 or minimum 220,000 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#), Security processing (like apps, users, content/URL, policy match, SSL decryption, application identification etc) & Network Processing (like flow

S.No.	Minimum Specifications
	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 supplied with appropriate/higher RAM to support required performance in this RFP for this Firewall from day 1 considering future scalability 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 protocols

S.No.	Minimum Specifications
	- 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.
	Administration, Management, Logging & Reporting
EXTFW.REQ.0069	Solution must have mechanism to track and report the changes done on policy management and maintain audit trails.
EXTFW.REQ.0070	The Firewall Management Solution, log server and reporting server can be either hardware appliance or VM based solution.

S.No.	Minimum Specifications
EXTFW.REQ.0071	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.0072	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.0073	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.0074	Should support Multicast protocols like IGMP, PIM, etc
EXTFW.REQ.0075	The solution must have data loss prevention by defining the categories of sensitive information that is required to filter.
	Management & Logging/Reporting
EXTFW.REQ.0076	The solution should come with a web based administration interface or GUI console.
EXTFW.REQ.0077	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.0078	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.0079	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.0080	The device or any of its family should not have any feature of wireless within its hardware or software.
EXTFW.REQ.0081	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.0082	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.0083	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.0084	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.0085	The firewall supports TLSv1.2 and TLSv1.3 decryption
EXTFW.REQ.0086	Should support SLAAC Stateless Address Auto configuration

S.No.	Minimum Specifications
EXTFW.REQ.0087	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.0088	Bidirectional Forwarding Detection (BFD)
EXTFW.REQ.0089	The Solution should support DNS security
	Monitoring, Management and Reporting
EXTFW.REQ.0090	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.0091	Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis
EXTFW.REQ.0092	Should have built in report templates base on Applications, Users, Threats, Traffic and URLs
EXTFW.REQ.0093	Should be able to create reports base user activity
EXTFW.REQ.0094	Should be able to create custom report base on custom query base any logging attributes
EXTFW.REQ.0095	**Authorization**
EXTFW.REQ.0096	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.0097	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.0098	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

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. 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 authorized 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 authorized 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 solution must be FIPS 140-2 /FIPS/STQC for trusted supply chain /Cert-In certification for OWASP top 10 vulnerability guidelines compliant, 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 or National or State Govt. Data Centre or PSUs Data Center or National BFSI or National TSPs 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 recognized and certified in industry like ISO 27000 or ISO 27034 etc.
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 integrated 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 have built-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 heterogonous enterprise 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, SLA Management, 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 discovery Layers 2 through Layers 7 of OSI model.

S.No.	Minimum Specifications
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 (excluding PO & Invoice generation).
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

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. 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 10 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 1/10G, 2x100 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 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

S.No.	Minimum Specifications
	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/ TSP 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 and 33,000 TPS with ECC ECDSA P-256. System protects against SSL/TLS Encrypted DoS and DDoS threats both at the SSL/TLS Layer and HTTPS layer
DDOS.REQ.0032	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

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 100K New SSL Transaction per second with RSA 2K key and minimum 70K TPS using ECC should 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 Solution should have the ability to do certificate signing request
SSLO.REQ.0013	Features	The Proposed SSL Visibility Solution should have the ability to cache dynamically generated certificates for reuse on subsequent connections
SSLO.REQ.0014	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.0015	Features	Solution should have the ability to customize trusted CA lists.
SSLO.REQ.0016	Features	The Proposed SSL Visibility Solution should integrate with any existing CA solution and current PKI structure
SSLO.REQ.0017	Features	The Proposed SSL Visibility Solution should be able to customize trusted CA list
SSLO.REQ.0018	Features	The Proposed SSL Visibility Solution should be able to do CA revocation management
SSLO.REQ.0019	Features	The Proposed SSL Visibility Solution should support passing Jumbo Frame IP traffic

S.No.	Parameter	Minimum Specifications
SSLO.REQ.0020	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.0021	General	The Proposed SSL Decryption Appliance should decrypt and re-encrypt (full duplex) in all modes in same format
SSLO.REQ.0022	General	The Proposed SSL Decryption Appliance should have the flexibility of sending decrypted traffic to multiple copy ports
SSLO.REQ.0023	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.0024	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.0025	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.0026	Functional	The Proposed SSL Visibility Solution should have the capability to support scale-out of existing security solution.
SSLO.REQ.0027	Features	The Proposed SSL Visibility Solution should have the ability to import server-side certificates and private keys for decryption
SSLO.REQ.0028	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.0029	Features	The Proposed SSL Visibility Solution should support multiple active-inline devices simultaneously
SSLO.REQ.0030	Features	The Proposed SSL Intercept Appliance should have the Encryption support for TLS 1.1, TLS1.2, TLS1.3 SSLV3
SSLO.REQ.0031	Features	The Proposed SSL Visibility Appliance should have the ability to decrypt and re-encrypt traffic within the same appliance
SSLO.REQ.0032	Features	The Proposed SSL Visibility Solution should support Extended Validation (EV) certificates
SSLO.REQ.0033	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.0034	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.0035	Features	The Proposed SSL Visibility Solution should have the ability to configure encryption/decryption policy (incl. block/pass-through) based on Subject / Domain Name
SSLO.REQ.0036	Features	The Proposed SSL Visibility Solution should support OCSP stapling

S.No.	Parameter	Minimum Specifications
SSLO.REQ.0037	Features	The Proposed SSL Visibility Solution should allow TCPDUMP / Packet capture
SSLO.REQ.0038	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.0039	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.0040	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.0041	Features	The Proposed SSL Visibility solution should detect and evaluate connections from servers having invalid certificates.
SSLO.REQ.0042	Features	The Proposed SSL Visibility Solution should have the ability to maintain headers in regenerated TCP stream.
SSLO.REQ.0043	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.0044	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.0045	Features	The Proposed SSL Visibility Solution should support majority of cipher suites and even the draft versions
SSLO.REQ.0046	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.0047	Hardware	Should support device management using local console, CLI (SSH), GUI (HTTPS)
SSLO.REQ.0048	Solution	The Proposed SSL Visibility Solution should have CLI interface with all functionalities and configuration capabilities through CLI
SSLO.REQ.0049	Solution	The Proposed SSL Visibility Appliance should have Access Control Lists (ACL) on management interface
SSLO.REQ.0050	Solution	The Proposed SSL Visibility Appliance should support IPv6 and solution should be IPv6 certified to ensure all features of IPv6
SSLO.REQ.0051	Solution	Should support sending of logs to centralized Syslog Server.
SSLO.REQ.0052	Solution	System must have Web-based Graphical User Interface (GUI)
SSLO.REQ.0053	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.0054	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, external Radius/TACACS
SSLO.REQ.0055	Solution	Should supports mirroring packets (HTTPS/TCPS) to specified

S.No.	Parameter	Minimum Specifications
		network interfaces.
SSLO.REQ.0056	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.0057	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.0058	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.0059	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 " *.PEM", *.PFX",*.Cer and good to have Open SSL/Apache or "Netscape or *.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.0060	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.0061	Support	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

SYSTEM SOFTWARE'S

Operating System & Database software only will be procured separately by CRID and will be provided to the MSI based on the requirement as per project plan submitted by MSI. All other software & supporting tools are under scope of MSI.

Virtualization Software

S.No.	Minimum Specifications
VIRT.REQ.001	The solution should include bare metal hypervisor with functionality of HA and proactive HA, Minimal 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) with minimal disruption or downtime of working VMs for both windows and Linux base VMs, distributed switch/centralized network configuration, VM level encryption/VM disk 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 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/with 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 or 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 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 minimal downtime, zero data loss and high 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 scripts.

S.No.	Minimum Specifications
VIRT.REQ.0013	Virtualization software should have the ability to live migrate VM files/disks 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
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

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 solution from day 1, License proposed should have flexibility to decouple the HCI software from hardware, in order to run HCI software on any certified hardware or any other hardware make as well. 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 or PSU Data Centre or 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 & memory expansion without any compute & storage virtualization license implication in existing nodes.
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.
HCI.REQ.009	General	The Proposed solution should be able to support nodes of different generation CPUs in the same cluster, in case of scalability at a later stage.

Sl. No.	Component / Performance / Utility	Minimum Specification
C	**Management**	
HCI.REQ.0010	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.0011	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.0012	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.0013	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.0014	Management	The solution shall provide assistance in troubleshooting and operational management in the virtualized environment.
HCI.REQ.0015	Management	The solution should have the capabilities for configuration and change management workflows
D	**Reporting**	
HCI.REQ.0016	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.0017	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.0018	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.0019	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.0020	SW Feature	Must support Instant space optimized point- in-time Snapshots. Should support atleast 24 snapshots per day

Sl. No.	Component / Performance / Utility	Minimum Specification
HCI.REQ.0021	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.0022	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.0023	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.0024	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.0025	SW Feature	All servers in the HCI cluster must contribute Compute & Storage.
HCI.REQ.0026	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. The proposed solution must offer (native File Services, Object Services or integration with File Services & Object services) with the ability to scale-out. if additional license needs to be factored for replication, factor the same from day 1.
HCI.REQ.0027		Offered Solution must be supplied with safe & secure storage with Ransomware protection or any one of the following data protection mechanism: Inbuilt 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 & duration of the project. The usable storage as indicated in HCIS.REQ.0065 must not be utilized for enabling these features.
HCI.REQ.0028		The offered HCI solution must have the functionality to share the block/volume from their software-defined storage with the bare metal servers outside of the HCI solution over different protocol (ISCSI/FC,etc)
HCI.REQ.0029	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.0030	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.

Sl. No.	Component / Performance / Utility	Minimum Specification
HCI.REQ.0031	Virtualization	The solution should include bare metal hypervisor with functionality of HA, near Zero Downtime & Zero Data-loss. 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 or HCI encryption, Network and Storage I/O Control, VM based replication not more than 5 mins RPO, resource scheduling for storage and VMs.
HCI.REQ.0032	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.0033	Virtualization	The solution should provide capability to migrate existing physical/Virtual workloads to the proposed HCI solution with minimal disruption
HCI.REQ.0034	Virtualization	Virtualization software/solution should allow seamless migration across different CPUs across the hybrid cloud by persisting the hot migration with near 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
HCI.REQ.0035	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.
HCI.REQ.0036	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.0037	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. It should have capability of native backup and restoration of the virtualization management server
HCI.REQ.0038	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.0039	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**	

Sl. No.	Component / Performance / Utility	Minimum Specification
HCI.REQ.0040	Replication	The Proposed Solution should support synchronous and asynchronous, local and remote replication. 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
HCI.REQ.0041	Replication	The solution should provide orchestration layer to have automated disaster recovery. Required/Unlimited VMs licenses should be provided for covering all the available compute & storage.
HCI.REQ.0042	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.0043	**Disaster Recovery**	The solution should have capability to test DR failover to separate network with no impact to production workloads.
HCI.REQ.0044	**Disaster Recovery**	The solution should have feature to assist in failback process to Primary data centre. The Solution should have unified console natively from HCI to manage multiple clusters at DC & DR.
HCI.REQ.0045	**Disaster Recovery**	License not required on day 1, however, may require in future
I	**Security**	
HCI.REQ.0046	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.0047	Security	The proposed solution must offer Micro segmentation for VM-level security (at the vNIC) from the offered HCI console natively. It should be certified for common criteria, FIPS EAL/FIPS 140-2/FIPS/STQC or Equivalent Govt. certification and relevant copies of certificate should be provided by bidder/OEMs
J	**Cloud Management Platform**	
HCI.REQ.0048	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

Sl. No.	Component / Performance / Utility	Minimum Specification
HCI.REQ.0049	Cloud Management Platform	The proposed solution should support application lifecycle management with automated orchestration across major hypervisor and cloud.
HCI.REQ.0050	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.0051	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 like load balancing and Firewall API
HCI.REQ.0052	Cloud Management Platform	The solution should have Life Cycle Management Work flows: Provisioning
HCI.REQ.0053	Cloud Management Platform	The Solution should have the capabilities for customization of dashboards
HCI.REQ.0054	Cloud Management Platform	The solution should provide capability of generating reports for usage & performance
HCI.REQ.0055	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.0056	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
HCI.REQ.0057	Cloud Management Platform	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
HCI.REQ.0058	Cloud Management Platform	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/blueprint that manage cloud resources to achieve infrastructure as code (IaC). Should support bare metal server provisioning through automation tool or via lifecycle management software
K	**Nodes**	
HCI.REQ.0059	**Nodes**	Proposed cluster should have minimum 5 Nodes with single node failure.
HCI.REQ.0060	**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.0061	**Nodes**	RAM per Node: Minimum 1 TB DDR5 with ECC 4800 Mhz or higher

Sl. No.	Component / Performance / Utility	Minimum Specification
HCI.REQ.0062	**Nodes**	**Network Ports per Node** 4 Nos. 25/10 Gbps with SFP+ 1 No. IPMI (Management Port)
HCI.REQ.0063	**Nodes**	**Power Supply and fans per node** Redundant and hot swappable power supplies and fans
L	**Storage Space**	
HCI.REQ.0064	**Storage Space**	Proposed solution should be configured with min 250 TB usable Storage (All Flash NVMe) with RF2 and should tolerate 1 Node Failure, the proposed storage should have data savings features like compression, de duplication and erasure coding & should be able to provide resiliency with RF2 (Two Copies of Data) from day1. The proposed HCI solution should be able to run RF3 in the same cluster along with RF2 without any license implication to CRID. Should have redundant Boot drives
M	**Firmware Code and Patch Management**	
HCI.REQ.0065	**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.0066	**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.0067	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.0068	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.0069	Proactive Maintenance and Support	Original Equipment manufacturer should have online 24 x 7 support for any hardware or software related issue
HCI.REQ.0070	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.0071	**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

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/blueprint 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 own profiles/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 templates as 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 agents to 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.
CMOS.REQ.0018	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support

DOMAIN NAME SYSTEM SERVER (DNS)

S. No.	Parameter	Minimum Specifications
DSER.REQ.001	Motherboard	Minimum number of sockets available & minimum sockets populated from Day 1: **2**
DSER.REQ.002	Form Factor	1U or 2U
DSER.REQ.003	Total Core per server	Latest Generation Processors of OEMs (AMD/Intel) 32 Cores (min.2 proc with 16 core per processor)
DSER.REQ.004	Configured CPU	Processor Base Frequency (GHz) 3.0 GHz Or higher and should support memory speed@ 4800 MT/s or higher
DSER.REQ.005	Memory slots	24 or higher DIMM slots
DSER.REQ.006	Memory configured	Type DDR 5 SDRAM with ECC 4800 Mhz or higher supported PCIe Gen 5 RAM Size 128 GB
DSER.REQ.007	Capacity Drive	1. 2x 800 SSD or higher (in RAID 1)
DSER.REQ.008	RAID/HBA Controller	RAID controllers with minimum 12Gbps or higher speed with 4 GB or higher Cache Supporting RAID 0 & 1
DSER.REQ.009	I/O slots Bus Slot	At least 3 PCIe Gen5 Slots
DSER.REQ.0010	Ethernet ports	2 number 1/10G and 2 number 25G or Higher with 25 G QSFP28 from day 1
DSER.REQ.0011	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
DSER.REQ.0012	Power & temperature	Minimum Gold rated redundant Hot plug Power Supplies or better Should support hot plug redundant power supplies with minimum 80% efficiency

DSER.REQ.0013	Configuration & Management	**1. Management Features-1**
		• Remoter power on/ Shutdown of server
		• Remote Mangement of Server over LAN & WAN with SSL encryption through gigabit management port
		• Should have virtual Media support with all required licenses.
		  ○ Encrypted virtual media
		  ○ Server Health Logging
		  ○ Out of Band Management
		• 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

S. No.	Parameter	Minimum Specifications
		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
DSER.REQ.0014	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 **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
DSER.REQ.0015	IPv4/6 Ready	The Hardware should be IPv4 & IPv6 compliant & ready from day one
DSER.REQ.0016	Warranty & Post warranty Support	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support
DSER.REQ.0017	Fans	Redundant hot-plug system fans
DSER.REQ.0018	Operating Systems and Virtualization Software Support	OS: Microsoft Windows Server, Hyper-V, VMWare, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Cent OS

Note :

- 2 numbers of DNS Server should be installed with Red hat Enterprise Linux Server Standard subscription for 5 years and
- 2 numbers of DNS Server should be installed with Windows server Standard edition with 5 years subscription

Certification required: -

S.No.	Category of Standard	Description	Name of Certification.
INTELL.REQ.0001	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.0002	Energy Efficiency Standards	Energy Efficiency Standard	EnergyStar7.0 or Higher/Equivalent BEE Star rating
INTELL.REQ.0003	Environmental Standards	Environmental protection standard	EPEAT/Equivalent Indian Standard
INTELL.REQ.0004	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.

SECTION 6

GENERAL INSTRUCTIONS AND BID PREPARATION AND SUBMISSION

General Instructions

6.1.1 The Bidders are requested to examine the instructions, terms and conditions and specifications given in this tender document. Failure to furnish all required information in every respect will be at the Bidder's risk and may result in the rejection of bid.

6.1.2 The Bidder (s) shall be deemed to have satisfied itself fully before Bidding as to the correctness and sufficiency of its/their Bids for the Contract and price quoted in the Bid to cover all obligations under this Tender.

6.1.3 It will be imperative for each Bidder(s) to familiarize itself / themselves with the prevailing legal situations for the execution of Contract. HARTRON shall not entertain any request for clarification from the Bidder regarding such legal aspects of submission of the Bids.

6.1.4 It will be the responsibility of the Bidder that all factors have been investigated and considered while submitting the Bids and no claim whatsoever including those of financial adjustments to the Contract awarded under this tender will be entertained by HARTRON. Neither any time schedule nor financial adjustments arising thereof shall be permitted on account of failure by the Bidder to appraise themselves.

6.1.5 It must be clearly understood that the Terms and Conditions and Specifications are intended to be strictly enforced. No escalation of cost in the Tender by the Bidder will be permitted throughout the period of Contract or throughout the period of completion of Contract whichever is later on account of any reasons whatsoever.

6.1.6 The Bidder shall make all arrangements as part of the Contract to supply commission and train the beneficiaries at various locations at their own cost and transport.

6.1.7 The Bidder shall be fully and completely responsible to HARTRON and State Government for all the deliveries and deliverables.

6.2 Clarifications in the Tender

6.2.1 A prospective Bidder requiring any clarification in the Tender may notify HARTRON by E-mail to mdhartron-hry@gov.in with a copy to sandeepv.hartron-hry@gov.in, Hartron.tds@gmail.com; rajeshpandey.ditech@hry.gov.in

6.2.2 The responses to the clarifications if required will be notified in the websites by means of Corrigendum to the Tender Document.

6.3 Pre-Bid Conference – Amendments to the Tender.

6.3.1 In order to avoid clarification/confirmation after opening of bids, wherever specifically mentioned in NIT, Pre-bid conference shall be held so as to provide an opportunity to the participating bidders to interact with HARTRON with regard to various tender provisions/tender specifications, before the bids are submitted. In case, due to the points/doubts raised by the prospective bidders any specific term & condition (which is not a part of "Standard terms and conditions of tender") needs to be modified, then the same will be considered for modification.

6.3.2 A Pre-bid meeting will be held for addressing the clarifications.

6.3.3 After pre-bid conference, the specifications & other tender conditions will be frozen. No change in specification and tender conditions will be permissible after pre-bid meeting. All the bidders must ensure that their bid is complete in all respects and conforms to tender terms and conditions & the tender specifications in to failing which their bids are liable to be rejected without seeking any clarifications on any exception/deviation taken by the bidder in their bid.

6.3.4 Bidder should depute their authorized representative who should be competent to take on the spot decisions.

6.3.5 The clarifications to any of the terms and conditions and or technical specifications laid in the Tender document and amendments, if any, will be notified on the www.hartron.org.in and Haryana Government portal https://etenders.hry.nic.in. The Bidders are advised to check periodically for the amendments or corrigendum or information on these websites till the closing date of this Tender. Hartron will not make any individual communication and will in no way be responsible for any ignorance pleaded by the Bidders.

6.3.6 Any such supplement / corrigendum / amendment issued by Hartron before closing of the Tender shall be deemed to be incorporated by this reference into this RFP.

6.3.7 All such addendums / amendments / notices released in the form of corrigendum shall be binding on all Bidders.

6.3.8 HARTRON will not be responsible for any misinterpretation of the provisions of this RFP on account of the Bidders of their failure to update the Bid documents based on the addendums/ amendments/ corrigendum published via emails.

6.3.9 HARTRON at its discretion may or may not extend the due date and time for the submission of bids on account of amendments.

6.3.10 HARTRON is not responsible for any misinterpretation of the provisions of this tender document on account of the Bidders failure to update the Bid documents on changes announced through the website.

6.3.11 The bidder(s) can submit representation(s) if any, in connection with the processing of the tender directly only to the Competent Purchase Authority(CPA) i.e. to MD, HARTRON, Bays no. 73-76, Sector-2, Panchkula, upto specified date in the tender document. The same will be dealt either separately or in the pre-bid conference if scheduled for the tender.

6.3.12 In case any bidder makes any unsolicited communication in any manner, after the pre-bid conference or the bids have been opened (for tenders processed either on single bid or on two bid basis), the bid submitted by the particular bidder shall be summarily rejected, irrespective of the circumstances for such unsolicited communication.

Further, if the tender has to be closed because of such rejection, and the jobs has to be re-tendered, then the particular bidder shall not be allowed to bid in the re-tender.

The above provision will not prevent any bidder form making representation in connection with procession of tender directly and only to Competent Purchase Authority (CPA) as mentioned in the tender document. However, if such representation is found by CPA to be un-substantiate and / or frivolous and if the tender has to be closed because of the delays/disruptions caused by such representations and the job has to be re-tendered, then such bidder will not be allowed to participate in the re-invited tender.

In case, any bidder while making such representations to Competent Purchase Authority (CPA) also involve other officials of HARTRON and / or solicits/invokes external intervention other than as may be permitted under the law and if the tender has to be closed because of the delays/disruptions caused by such interventions and has to be re-tendered, then the particular bidder will not be allowed to participate in the re-invited tender.

6.4 Language of the Bid

6.4.1 The bid prepared by the Bidder as well as all correspondence and documents relating to the bid shall be in English only.

6.4.2 The supporting documents and printed literature furnished by the bidder may be in another language provided they are accompanied by an accurate translation in English duly familiar, in which case, for all purposes of the bid, the translation shall govern. Bids received without such translation copy are liable to be rejected.

6.5 Bid Currency

Prices shall be quoted in Indian Rupee (INR). All payments / deposits / fees in respect of this tender also shall be in Indian Rupee only

6.6 Consortium

Consortium is not allowed and the Bids submitted by consortium of companies/firms will be summarily rejected.

6.7 Bid Preparation and Submission

6.7.1 **Cost of Bidding**

The Bidders shall bear all costs associated with the preparation and submission of Bids. HARTRON will in no way be responsible or liable for these charges/costs incurred regardless of the conduct or outcome of the bidding process.

6.7.2 **Tender Document Cost**

The Tender Document is available online and can be downloaded from Hartron Website i.e. https://hartron.org.in or from Haryana Govt. e-procurement portal https://etenders.hry.nic.in.

6.7.3 **Earnest Money Deposit (EMD)**

6.7.3.1 EMD is to be made online directly as per the detail given under section-4, Eligibility Criteria.

6.7.3.2 The EMD of the Unsuccessful Bidders will be returned at the expense of the Bidders within a reasonable time consistent with the rules and regulations in this behalf. The EMD amount held by HARTRON till it is refunded to the Unsuccessful Bidders will not earn any interest thereof.

6.7.3.3 The EMD amount of the Successful Bidder(s) shall be returned once the PBG amount i.e 10% of total project order value received in full;

6.7.3.4 The EMD amount will be forfeited by HARTRON if the Bidder(s) withdraws the bid during the period of its validity specified in the tender or if the Successful Bidder fails to sign the contract or the Successful in bidder fails to honour the terms & condition of the Tender.

6.7.4 **Performance Bank Guarantee:-**

The successful bidder(s) will submit a Performance Bank Guarantee (PBG) at the rate of 10% of the total project order value in favor of Director (Administration), Citizen Resources Information Department, Room no-42, 9th floor, Haryana Civil Secretariat, Sector-1, Chandigarh-160001 within 15 days after the acceptance of the letter of intent and the said PBG shall be valid for 72 months from the date of Letter of Intent (LOI). If the contract is extended after the scope of work as per RFP, the PBG under rules at that time for the project value shall be applicable.

6.7.5 **PBG release schedule**

PBG =10% of TOTAL Project Order Value					
Year	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
PBG Amounts	16 % of PBG	16 % of PBG	20 % of PBG	24 % of PBG	24 % of PBG
PBG Release Schedule	24 months from LOI Date	36 months from LOI Date	48 months from LOI Date	60 months from LOI Date	72 months from LOI Date

6.7.6 **Tender Validity**

The e – tender submitted by the Bidders shall be valid for a minimum period of 240 days from the date of opening of the Commercial bid.

6.7.7 **Letter of Authorization**

A letter of Authorization from the Board of Directors / appropriate authority authorizing the Tender submitting authority or a Power of Attorney shall be submitted in the Technical bid, otherwise the Bids will be summarily rejected.

6.7.8 **Two Part Bidding**

The bids shall be submitted Online in two bid part as give below i.e Technical Bid and Commercial Bid as per the format given in the tender document and the respective online envelope available on the portal upto the due date & time. Bidders are required to examine all Instructions, Terms and Conditions and Technical specifications given in the Tender document. Failure to furnish information required by the Bid or submission of a Bid not substantially responsive in every respect will be at the Bidders risk and may result in rejection of Bids. Bidders shall strictly submit the Bid as specified in the Tender, failing which the bids will be non-responsive and will be rejected.

6.7.9 **Technical Bid (Stage 1)**

6.7.9.1 The Technical Bid format as given in the Tender shall be filled, signed and stamped on all pages. Errors if any shall be attested by the Bidders. The Technical Bid shall not contain any indications of the Price otherwise the Bid will be summarily rejected.

6.7.9.2 The bidders shall submit the details of make and model of the items offered against the tender requirement.

6.7.9.3 The technical bid should be submitted through e-bid as per the last date & time. The hard copy of technical bid containing all the duly filled & signed Technical bid as per the format given at 9.1 of the tender document and another annexure along with duly signed and stamped tender document downloaded from the website should also be submitted at Hartron Bhawan, Bays no. 73-76, Sector-2, Panchkula.

6.7.9.4 The Technical Bids shall be typed, signed and stamped in all pages by the familiarize

signatory of the Bidder. Any alternations, deletions or overwriting shall be attested with full signature of the familiarize signatory.

6.7.10 **Price Bid Form (Stage 2)**

6.7.10.1 The Price bid should be submitted through online mode as per price envelope given on the e-procurement portal against this tender. All the price items as asked in the tender shall also be filled in the Price Bid Format as given in the Tender and required to be uploaded on the e-procurement Portal. The Prices quoted shall be only in INDIAN RUPEES (INR) only. The tender is liable for rejection if price bid contains conditional offers.

6.7.10.2 All the Price items as asked in the Tender shall be filled in the Price Bid Format as given in the Tender at Format 2 COMMERCIAL BID and as pre bid clarification corrigendum

6.7.10.3 The price quoted by the Bidder shall include cost and expenses on all counts viz. cost of equipment, materials, tools/ techniques/ methodologies, manpower, supervision, administration, overheads, travel, lodging, boarding, in-station & outstation expenses, etc and any other cost involved in the supply and commissioning.

6.7.10.4 The Price Bid Form shall not contain any conditional offers or variation clauses, otherwise the Bids will be summarily rejected.

6.7.10.5 The Price Bid shall be typed and shall be signed by the authorized signatory in all pages. Any alterations, deletions or overwriting shall be attested with full signature of the familiarize signatory.

6.7.10.6 The cost quoted by the Bidder shall be kept firm during the period of contract in the Tender from the date of opening of the tender.. The Bidder shall comply with the Price variation for any additional purchase as per the clause mentioned in Section 4 : Right to vary quantity of the RFP

6.7.10.7 In case the selected bidder misses to include the cost of any hardware/software which is necessary to meet the requirements of this tender, the selected bidder shall be solely responsible for the lapse and would be required to provide the such hardware/software without any additional cost to the indenting department.

6.7.11 Discount: - Bidder are advised not to indicate any separate discount. Discount, if any should be merged with the quoted prices. Discount of any type, indicated separately, will not be taken into account for evaluation purpose. However, in the event of such an offer, without considering discount, is found to be lowest, HARTRON shall avail such discount at the time of award of contract.

6.7.12 Correction of error

6.7.12.1 Bidders are advised to exercise adequate care in quoting the prices. No excuse for corrections in the quoted figures will be entertained after the Commercial Bids are received by HARTRON.

6.7.12.2 In cases of discrepancy between the prices quoted in words and in figures, the value indicated in words shall be considered.

6.7.12.3 The amount stated in the Commercial Bid, adjusted in accordance with the above procedure shall be considered as binding on the Bidder for evaluation

6.7.13 Bid closing date and time

The e-Tenders shall be submitted not later than the date and time specified under relevant section of this RFP or Corrigendum if published. Hence the Bidders shall be cautious to submit the e-Tenders well in advance to avoid disappointments as system will not allow them to submit the bid once the due date & time is over.

6.7.14 Mode of Submission of Bids: -The Bids shall be submitted electronically on Haryana Govt. e-procurement portal strictly as specified in the Tender document. However, bidder will also submit a hard copy of technical bid to HARTRON upto due date & time of submission of offers. The Bids will not be received personally.

6.7.15 Modification and withdrawal of Bids: - The Bids once submitted cannot be modified or amended or withdrawn. No documents would be supplemented after submission of Bids unless specifically asked by Hartron.

6.7.16 Rejection of Bid: -

6.7.16.1 Bids submitted other than the electronic form on e-procurement portal of Haryana Government shall not be entertained.

6.7.16.2 Any condition put forth by the Bidders not conforming to the bid requirements, shall NOT be entertained and such bids shall be rejected.

6.7.17 Disqualification

HARTRON/Department may at its sole discretion and at any time during the evaluation of application, disqualify any Bidder, if the Bidder:

i. Made misleading or false representations in the forms, statements and attachments submitted in proof of the eligibility requirements.
ii. Submitted an application that is not accompanied by required documentation or is non-responsive.
iii. Failed to provide clarifications related thereto, when sought.
iv. Submitted more than one bid.
v. Was declared blacklisted by any Govt. or quasi-Govt. entity in India.

6.7.18 Conflict of Interest

Neither the successful Bidder nor any Personnel related to it shall engage, either directly or indirectly, during the period of contract, in any business or professional activities which would conflict with the activities assigned to them under or pursuant to this tender.

6.7.19 Confidentiality

The Bidder and their personnel shall not, either during the term or after expiration of this contract, disclose any proprietary or confidential information relating to the services, contract without the prior written consent of the Hartron.

6.7.20 Extension of Last date for Submission

HARTRON at its own discretion can extend the period for submission of bids by amending the Bid Documents / TENDER. In this case all rights and obligations of Hartron and Bidders shall stand extended. However, no request for extension of time from the Bidders shall be binding upon Hartron. The decision of Hartron in this behalf will be final, conclusive and binding on the Bidder.

6.7.21 Late Bids

Any bid received by Hartron after the deadline for submission of bids prescribed in the TENDER will be summarily rejected and returned unopened to the Bidder. No further correspondence on this subject will be entertained.

6.7.22 Duties, Taxes and Statutory levies

6.7.22.1 The Bidder shall bear all personnel taxes levied or imposed on account of payment received under this Contract.

6.7.22.2 The Bidder shall bear all corporate taxes, levied or imposed on the Bidder on account of payments received by it from Hartron/Department for the work done under this Contract.

6.7.22.3 Bidder shall bear all taxes and duties/GST etc. levied or imposed on the Bidder under the Contract including but not limited to Sales Tax, Customs duty, Excise duty, Octroi, Service Tax, VAT, Works Contracts Tax/GST and all Income Tax levied under Indian Income Tax Act – 1961 or any amendment thereof up to the date for submission of final price bid, i.e., on account of payments received by him for the work done under the Contract. It shall be the responsibility of the Bidder to submit to the concerned tax authorities the returns and all other connected documents required for this purpose. The Bidder shall also provide Hartron such information, as it may be required in regard to the Bidder's details of payment made by the Purchaser under the Contract for proper assessment of taxes and duties. The amount of tax withheld by Hartron/Department shall at all times be in accordance with Indian Tax Law and will furnish to the Bidder original certificates (Challan) for tax deduction at source and paid to the Tax Authorities.

6.7.22.4 If there are any changes (reduction, increase, introduction of new, deletion of exiting) in taxes / duties due to any revision by GOI or State Government whatsoever, after Award of Contract, the same shall be adjusted upwards/downwards in the contract prices and the bidder shall be paid as applicable on date of invoice.

6.7.22.5 The Bidder shall be solely responsible for the payment /fulfilment of its tax liabilities and obligations under the Income Tax Act and other such laws in force and Hartron/Department shall not bear responsibility for the same.

6.7.23 Deductions

All payments to the Bidder shall be subject to the deductions of tax at source under Income Tax Act, and other taxes and deductions as provided for under any law, rule or regulation. All costs, damages or expenses which Hartron may have paid or incurred, for which under the provisions of the Contract, the Bidder is liable; the same shall be

deducted from any dues to the Bidder. Hartron shall if so required by applicable laws in force, at the time of payment, deduct income tax payable by the Bidder at the rates in force, from the amount due to the Bidder and pay to the concerned tax authority directly.

6.7.24 Right to Accept/ Reject the Bid

HARTRON reserves the right to accept or reject any Bid and to annul the TENDER process and reject all such bids at any time prior to award of contract, without thereby incurring any liability to the affected Bidder(s) or any obligation to inform the affected Bidder(s) of the grounds for such decision.

SECTION 7

TENDER OPENING AND EVALUATION

Bid Evaluation Process

7.1 Initial Scrutiny

At the time of Technical Bid Opening, Initial Bid scrutiny will be conducted and incomplete details as given below will be treated as non-responsive and the Bids will be rejected summarily.

If Tenders are;

i. not submitted in two parts as specified in the Tender received without EMD amount and tender document fee;
ii. All responsive Bids will be considered for further evaluation;
iii. The decision of Hartron will be final in this regard;

7.2 Technical Bid Scrutiny

Initial Bid scrutiny will be conducted and incomplete details as given below will be treated as non-responsive. If Tenders are received: -

i. without the Letter of Authorization;
ii. found without Tender document fee, EMD;
iii. found with suppression of details with incomplete information;
iv. subjective, conditional offers submitted without support documents as per the Eligibility Criteria;
v. Evaluation Criteria non-compliance of any of the clauses stipulated in the Tender;
vi. Lesser validity period not found with OEM's compliance statement and the Technical Leaflets of the quoted models. The decision of Hartron will be final in this regard;

7.3 Clarifications by HARTRON

When deemed necessary, Hartron may seek any clarifications on any aspect from the Bidder. However, that would not entitle the Bidder to change or cause any change in the substance of the Bid or price quoted. During the course of Technical Bid evaluation, Hartron may seek additional information or historical documents for verification to facilitate decision making. In case the Bidder fails to comply with the requirements of Hartron as stated above, such Bids may at the discretion of Hartron, shall be rejected as technically non-responsive.

7.4 Suppression of facts and misleading information

7.4.1 During the Bid evaluation, if any suppression or misrepresentation of is brought to the notice of Hartron. Hartron shall have the right to reject the Bid and if after selection, Hartron would terminate the contract, as the case may be, will be without any compensation to the Bidder and the EMD / SD, as the case may be, shall be forfeited.

7.4.2 Bidders shall note that any figures in the proof documents submitted by the Bidders for proving their eligibility is found suppressed or erased, HARTRON shall have the right to seek the correct facts and figures or reject such Bids.

7.4.3 It is up to the Bidders to submit the full copies of the proof documents to meet out the criteria. Otherwise, HARTRON at its discretion may or may not consider such documents.

7.4.4 The Tender calls for full copies of documents to prove the Bidder's experience and Capacity to undertake the orders.

7.5 Technical Bid Evaluation

7.5.1 A Tender Scrutiny Committee will examine / scrutinize the e-Technical Bids against the Eligibility Criteria and Evaluation Criteria given in the Tender document. The evaluation will be conducted based on the support documents submitted by the Bidders. The documents which did not meet the eligibility criteria in the first stage of scrutiny will be rejected in that stage itself and further evaluation will not be carried out for such bidders. The eligible Bidders alone will be considered for further evaluation.

7.5.2 For those Bidders who have already worked or working with HARTRON, their previous performance in HARTRON would be the mandatory criteria for selection. If any unsatisfactory performances of those Bidders are found, their Bids will be straight away rejected. The Unsatisfactory performance is defined as: -

i. Non responsiveness after getting the work order
ii. Delay in supply, installation of the ordered products without any bonafide reason, etc
iii. Poor warranty support
iv. Not executing the contract as per the terms and conditions
v. Not furnishing the performance bank guarantee as per the requirement laid in the contract/work orders

7.6 Price Bid Evaluation: -

i. The Financial Bids of only those Bidders short listed from the Technical Bids by TEC will be opened in the presence of their representatives on a specified date and time to be intimated to the respective Bidders by Tender Process Section, and the same will be evaluated by a duly constituted Finance Evaluation Committee (FEC).
ii. If HARTRON in consultation with Departments considers necessary, revised Financial Bids could be called for from the technically short-listed Bidders, before opening the original financial bids for recommending the final empanelment.
iii. In the event of revised financial bids being called the revised bids should NOT be higher than the original bids except in case of change in Government levies and USD ($) – Exchange Rate Variations; otherwise the bid shall be rejected.
iv. The negotiations will be held as per the policy issued by the State Govt. vide G.O No. 2/2/2010-4-IB-II dated 18.06.2013, G.O No. 2/2/2010-4-IB-II dated 16.6.2014, G.O No. 2/2/2010-4-IB-II dated 09.02.2015,14/29/2023-6FA 26.05.2023 and amendment time to time will be applicable. These policy guidelines are available at http://dsndharyana.gov.in/en-us/Purchase/Rules-instruction-and-procedure/Instructions. The policy/procedure issued by State Govt. time to time will also be applicable.
v. Lowest Quoting Bidder will be selected.

7.7 No enquiry shall be made by the bidder(s) during the course of evaluation of the tender, after opening of bid, till final decision is conveyed to the successful bidder(s). However, the Committee/its authorized representative and officers of Indenting Department can make any enquiry/seek clarification from the bidders, which the bidders must furnish within the stipulated time else bid of such defaulting bidders will be rejected

7.8 Award of Contract

i. A letter of intent shall be issued by Hartron to the successful bidder.
i. The successful bidder shall accept this letter of intent within 10 days from the date of issue of the letter of intent.
ii. The successful bidder shall submit a performance bank guarantee within 15 days after the acceptance of the letter of intent.
iii. The successful bidder will sign the contract / agreement with Hartron/Purchaser within 7 days from the date of submission of PBG.
i. Subsequent to the signing of the contract, Hartron/Purchaser shall issue Award of Contract to the successful bidder.
ii. The purchaser reserves the right to award the complete project to L1 bidder. In case of any issue, the purchaser may award the whole project to L2/L3/ bidder on L1 rates as per the provisions of Government of Haryana (DS & D).
iii. The Successful Bidder shall not assign or make over the contract, the benefit or burden thereof to any other person or persons or body corporate for the execution of the contract or any part thereof without the prior written consent of HARTRON. HARTRON reserves its right to cancel the Award of Contract either in part or full, if these conditions are violated. If the Successful Bidder fails to execute the Contract within the stipulated time in the tender, the EMD of the Successful Bidder will be forfeited and their tender will be held as non-responsive.
iv. The expenses incidental to the execution of the Contract shall be borne by the Successful Bidder.
v. The conditions stipulated in the Contract shall be strictly adhered to and violation of

any of the conditions will entail termination of the contract without prejudice to the rights of HARTRON and HARTRON also have the right to recover any consequential losses from the Successful Bidder.

7.9 HARTRON reserves the right to:

I. Insist on quality / specification of materials to be supplied.
II. Modify, reduce or increase the quantity requirements to an extent of the tendered quantity.
III. Change the list of areas of supply locations from time to time based upon the requirement of the purchase.
IV. Inspect the bidders' factory before or after placement of orders and based on the inspection, modify the quantity ordered.
V. Withhold any amount for the deficiency in the service aspect of the ordered items supplied to the Purchaser.

Read and accepted

Signature on behalf of
M/s----------

SECTION 8

TERMS AND CONDITIONS OF THE CONTRACT

Terms and conditions of the contract

8.1 Acceptance of Tender and Withdrawals

The final acceptance of the tender is entirely vested with HARTRON who reserves the right to accept or reject any or all of the tenders in full or in parts without assigning any reason whatsoever. The Tender Accepting Authority may also reject all the tenders for reasons such as change in Scope, Specification, lack of anticipated financial resources, court orders, calamities or any other unforeseen circumstances. After acceptance of the Tender by HARTRON, the Successful Bidder shall have no right to withdraw their tender or claim higher price

8.2 Inspection of the items

i. The inspection may be carried out complete or on random basis for all the BOQ Items against the milestone; however, the physical verification like quantity, models, physical conditions etc. will be carried out for all the BOQ Items. The cost to facilitate the inspection of equipment shall be borne by the successful bidder.

ii. The Purchaser can authorize an inspection committee of experts to inspect the BOQ Items delivered on site. Based on the request of the bidder the inspection team can even visit the stores at manufacturer premises/ distributors' premises or at consignee site. In such case the cost of visit of the inspection team shall be borne by the bidder.

iii. The Purchaser reserves the right to accept/ reject the same or any part or portion of the BOQ items referring to report of the inspection committee with reference to the deviations against the specifications mentioned in the RFP. The bidder shall not be paid for supplies rejected as above and such supplies shall be removed/ replaced by the successful bidder immediately at his own expense with the equipment as the specifications of the RFP and subject to further inspection by the committee.

iv. Purchaser shall be under no liability whatsoever for rejected and the same will be at the successful bidders risk. Rejected supplies shall be removed by the contractor within 10 days after notice has been issued to him of such rejection (in case the supplies are delivered on site) and failing such removal of rejected goods will be at contractor's risk and Purchaser may charge rent from the contractor for the space occupied by such rejected goods and inconvenience caused thereof. Further, the overall timeline as per the delivery schedule mentioned in the RFP shall not get impacted and all the SLAs/ Penalties as per RFP shall remain in force.

8.3 Warranty

i. The Selected Bidder is required to provide a comprehensive warranty for the products for a period of 5 years from the date of Go live i.e after performing SDC after checking the functionality

ii. The warranty shall cover the system software, components and sub-components of the supplied infrastructure including patches and upgrades (free of cost) of the system software.

iii. In addition to warranty as mentioned in above clause, the Bidder shall, during the above said period replace parts, if any, and remove any manufacturing defect, if found, so as to make the device fully operative. Replacement of parts or the entire product is to be done free of cost.

8.4 Product Test

The successful bidder will be required to submit test report form OEM (or) from Govt. approved test & calibration labs like ERTL/ETDC etc. if HARTRON feels it necessary to get the specifications verified. As a confirmatory document for specifications of the products for each configuration. The cost of such test will have to borne by the successful bidder however, this will be applicable only on limited quantity i.e. one-unit test report of each configuration/ type. However, the corporation can place the orders on the contract in anticipation of the test report. In case of failure of test, the supplier will be responsible for any risk & cost. Accordingly, bidder should ensure that offered product is in conformation to the specification of NIT.

8.5 Licenses & Transportation

i. All the operating system/software licenses if applicable are to be registered in the name of the respective indenting department.
ii. The entire cost of transportation from the Manufacturing Plant or Port of Landing to the designated destination as specified by Hartron/indenting department shall be borne by the selected Bidder.
iii. The transit insurance for all the items being delivered at respective site as specified by Hartron/indenting department is the responsibility of the successful bidder. The successful bidder shall submit to the indenting department, documentary evidence issued by the insurance company, indicating such insurance has been taken.

8.6 Packing

The selected Bidder shall provide such packing as is required to prevent damage or deterioration of the goods during transit to their final destination as indicated in the Contract. The packing shall be sufficient to withstand, without limitations, rough handling during transit and exposure to extreme temperatures and precipitation during transit and open storage. The selected Bidder shall be responsible for any defect in packing and shall dispatch the material freight paid and duly insured at destination. Any equipment found to be damaged during the transit by the indenting department, the successful bidder shall replace the aid equipment at his cost within 15 days from the event reported by the indenting department/Hartron.

8.7 Additional Payment Clause:

i. All payment shall be made as per milestone mentioned section 4: srl no 4. Payment schedule of this RFP.
ii. Payment will be released on the basis of actually installed items.
iii. Payment shall be made after adjusting penalties (if any) as applicable.
iv. All payments shall be made subject to deduction of TDS (Tax deduction at Source) as per the current Income-Tax Act.
v. Failure to sign the contract and submit PBG in time mentioned above shall constitute sufficient grounds for forfeiture of the EMD. Subsequently failure to perform services as per contract shall constitute sufficient grounds for forfeiture of the PBG.
vi. The EMD & Performance Security of successful bidder Deposits without any interest accrued, shall be released only after the expiry of the warranty period of the systems successfully.
vii. The PBG shall be released immediately after expiry of its validity period provided there is no breach of contract on the part of the Vendor.
viii. No interest will be paid on the PBG & EMD.
ix. In the event of any correction of defects or replacement of defective equipment during the warranty period, "the warranty for the corrected/replaced equipment shall be extended to a further period of 1 year or till the scope of the contract whichever is greater". The PBG for a proportionate value (during said period) shall be extended 60 days over and above the extend warranty period.
x. The proceeds of the performance security shall be payable to the Purchaser as compensation for any loss resulting from the Supplier's failure to fulfill its obligations under the Contract.
xi. The Successful Bidder hereby agrees to get the refund of incentive, excise duty and proportionate sales tax from authorities concerned and pass it on to Purchaser(s) if the Government or any other appropriate agency reduces the Excise duty or Sales tax or give incentive of any type retrospectively after supplying the Ordered items failing which action will be taken to recover the balance amount from the Successful Bidder under the Revenue Recovery Act or any other relevant act.
xii. When the extension of time is required due to any delay on the part of HARTRON/end user, extension of delivery time for the period of such delay involved may be granted provided by MD, HARTRON the firm produces documentary evidence of the delay.
xiii. Penalty amount if any will be adjusted in the payment due to the Successful Bidder.
xiv. All taxes and other levies imposed by Governments in India will be paid at actual as applicable.
xv. The delivery of the ordered items is to be supplied within the delivery period mentioned at section Project Milestone & Deliverable unless otherwise specified in the work order. Some occasions may arise that the products as indented by the departments maybe required to be delivered within a

short period of 24 hours to the Purchaser/s. In such occasions, it may be very difficult to arrange shipment of the items from the vendor premises due to the routine formalities. To tackle such conditions, the successful bidder may maintain a reasonable quantity of items ex-stock.

8.8 Invoicing:

i. The purchaser shall make payments to MSI as per the schedule mentioned in section 4, payment schedule in this RFP. The purchaser shall make all efforts to make payments(50% of the invoice amount) to MSI within 30 (thirty) days once the purchaser provides acceptance for the invoice(s) and other required documents & deliverables as mentioned in this RFP and rest of the invoice amount within 90 days. If there is delay in payment (50% of the invoice amount) beyond 30 days MSI can claim 0.1% monthly interest on invoice amount from the purchaser.

ii. With every dispatch of goods or materials in the order, the successful bidder will prepare invoices in triplicate in the name of indenting department as mentioned in the work order.

iii. Invoice along with Delivery Challan in duplicate are to be sent by the successful bidder to the consignee. The duplicate of Delivery Challan to be returned by the respective indenting officers with the quantities or numbers received duly noted and signed thereon to the successful bidder.

iv. Second copy to HARTRON along with the duly signed Delivery Challan received by the successful bidder from the respective intending officers for further necessary action regarding payments, etc. The payment shall be released by HARTRON after the receipt of inspection/verification of the materials from the indenting department. The third copy to be sent by the successful bidder to Indenting department for record in its office.

8.9 Forfeiture of EMD and SD

A Forfeiture of Earnest Money: -

I. If the Bidder withdraws his bid before the expiry of validity or after the acceptance of the bid, the Earnest Money Deposited by the bidder will be forfeited.

II. If the Bidder fails to comply with any of the terms, conditions or requirement of order and the technical specifications of the tender document at time of award of contract, the Earnest Money deposited by the Bidder will be forfeited.

B forfeiture of Performance Security: -

a. The Corporation reserves the right of forfeiture of the performance guarantee in the event of the contractor's failure to fulfill any of the contractual obligations or in the event of termination of contract as per terms & conditions of contract.

b. In case the successful bidder fails to submit the performance guarantee of the requisite amount within the stipulated period or extended period, letter of Award automatically will stand withdrawn and EMD of the contractor shall be forfeited.

c. In case successful bidder fails to comply with the delivery period as specified in the work order/contract, including extensions (if approved by purchaser), the Performance security deposited by the vendor will be forfeited.

d. In case the vendor fails to provide services during the warranty period as per the satisfaction of HARTRON/ indenting department, the Performance security deposited by the vendor will be forfeited.

e. In case the vendor failed to supply the ordered items as per the specification mentioned in the Work order or ordered items are rejected during the inspection even after giving one or two extra chance for inspection, the Performance security deposited by the vendor will be forfeited.

f. Performance guarantee shall be returned after successful completion / testing / commissioning and handing over the project to the client up to the entire satisfaction of The Corporation / Client Performance guarantee shall be returned after successful completion / testing / commissioning and handing over the project to the client up to the entire satisfaction of The Corporation / Client**.**

8.10 Authenticity of submitted Documents/Information.

a. The documents forming the Contract are to be taken as mutually explanatory of one another. If an ambiguity or discrepancy is found in the documents, the Corporation shall issue any necessary instructions and the priority of the documents shall be in accordance with the order as listed in the Appendix.

b. If any discrepancy is noticed between the documents as uploaded at the time of submission of tender and hard copies as submitted physically by the bidder, the tender shall become invalid and cost of tender document and processing fee shall not be refunded.
c. If in case, any document, information & / or certificate submitted is found to be incorrect / false / fabricated, the Corporation at its discretion may disqualify / reject / terminate the bid/contract and also forfeit the EMD / All dues.
d. The bidders must submit an Affidavit as placed at **"Annexure-12"** along with the technical bid.

8.11 Consequences of Cancellation of Order:

a. Upon cancellation of order, by written notice with a notice period of 30 days, the successful bidder shall deliver or cause to be delivered all works carried out for and on account of the indenting department and all data and records required from or on account of the Indenting Department/Organization.
b. Cancellation of order shall not affect any continuing obligations of the successful bidder under the Contract Agreement, which, either expressly or by necessary implication, are to survive its expiry or termination such as confidentiality obligations of the successful bidder.
c. Upon cancellation of order for any reason whatsoever, the successful bidder shall return to the Indenting Department/Organization any and all confidential information and any other property of the Indenting Department/Organization.
d. HARTRON on behalf of and in consultation with Indenting Department/Organization may procure services similar to those undelivered, upon such terms and in such manner, as it deems appropriate, at the risk and responsibility of the successful bidder and the successful bidder shall be liable for any additional costs for such services.
e. The successful bidder shall continue the performance of the order to the extent not terminated.
f. Upon cancellation of order for whatsoever, HARTRON on behalf of and in consultation with Indenting Department/Organization shall have the right to perform the following penalties: -
    i. Forfeiture of earnest money
    ii. Imposition of liquidated damage.
    iii. Putting supplier on holiday/ Blacklisting of the bidder
        a) in case bidder backs out of the contract and fails to perform required activities after expiry of notice period
        b) in case bidder indulges in fraudulent and corrupt practices in competing for or in executing the Contract
    iv. Forfeiture of bank Guarantee (s)
    v. Risk Purchase on the expenses of vendor.

8.12 Termination of Contract

i. Termination for default

(ii) HARTRON may without prejudice to any other remedy for breach of contract, by written notice of default with a notice period of 30 days, sent to the Successful Bidder, terminate the contract in whole or part, (i) if the Successful Bidder fails to deliver any or all of the goods within the time period(s) specified in the Contract, or fails to supply the items as per the Delivery Schedule or within any extension thereof granted by HARTRON; or (ii) if the Successful Bidder fails to perform any of the obligation(s) under the contract; or (iii) if the Successful Bidder, in the judgment of HARTRON, has engaged in fraudulent and corrupt practices in competing for or in executing the Contract; or (iv) if the successful bidder backs out of the contract

b) In the event HARTRON terminates the Contract in whole or in part, HARTRON may procure & deliver, upon terms and in such manner as it deems appropriate, the goods and services similar to those and delivered and the Successful Bidder shall be liable to HARTRON for any additional costs for such similar goods. However, the Successful Bidder shall continue the performance of the contract to the extent not terminated.
c) Upon cancellation of contract for whatsoever, HARTRON shall have the right to perform the following penalties: -
    i. Forfeiture of earnest money
    ii. Imposition of liquidated damage.
    iii. Putting supplier on holiday/ Blacklisting of the bidder

a) in case bidder backs out of the contract and fails to perform required activities after expiry of notice period
b) in case bidder indulges in fraudulent and corrupt practices in competing for or in executing the Contract

iv. Forfeiture of bank Guarantee (s) and Security deposit

8.13 Termination for Insolvency

HARTRON may at any time terminate the Contract by giving written notice with a notice period of 14 days to the Successful Bidder, if the Successful Bidder becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the Successful Bidder, provided that such termination will not prejudice or affect any right of action or remedy that has accrued or will accrue thereafter to HARTRON.

8.14 Termination for Convenience

HARTRON may by written notice, with a notice period of 30 days sent to the Successful Bidder, may terminate the Contract, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for HARTRON's convenience, the extent to which performance of work under the Contract is terminated, and the date upon which such termination becomes effective. On termination, the Successful Bidder is not entitled to any compensation whatsoever.

8.15 Single point of contact

The Successful Bidder shall nominate and intimate HARTRON, an Account Manager for Single Point of Contact (SPOC), who shall be responsible for effective delivery of work complying with all the terms and conditions. The Successful Bidder shall ensure that the Account Manager fully familiarizes with the Tender Conditions, Scope of Work and deliverables.

8.16 Assigning of Tender whole or in part

The successful Bidder shall not assign or make over the contract, the benefit or burden thereof to any other person or persons or body corporate. The Bidder shall not under-let or sublet to any person(s) or body corporate for the execution of the contract or any part thereof without the prior written consent of HARTRON.

8.17 Liquidated Damages (LD)

If MSI fails to supply, install or maintain any or all of the Goods or fails to complete the Works or fails to provide the Services as per the Agreement, within the time period(s) specified in the RFP, the Authority without prejudice to its other rights and remedies under the Agreement, deduct from the Agreement value, as liquidated damage at the rate specified in the Contract Format for non-fulfilment of subject to the force Majeure conditions.

The Authority may without prejudice to its right to effect recovery by any other method, deduct the amount of liquidated damages from any payments due to MSI in its hands (which includes the Authority's right to claim such amount against MSI's Bank Guarantee) or which may become due to MSI at a prospective date.

The deduction shall not exceed 10% of the total contract value and upon reaching such limit, the Authority, in its sole discretion, may entail termination & blacklisting as per Section 8: Clause 8.12 Termination & Blacklisting of contract of this RFP.

Any such recovery or liquidated damages shall not in any way relieve MSI from any of its obligations to complete the Work or from any other obligations and liabilities under the Agreement.

8.18 Other Conditions

a) HARTRON reserves the right to reject any or all the tenders without assigning any reason, to relax or waive any of the conditions stipulated in the terms and conditions of tender as deemed necessary in the best interest of Project for good and sufficient reasons.

8.19 Indemnity

MSI is hereby agree to indemnify HARTRON and the indenting department/organisation**,** from and against all direct claims, losses, liabilities, obligations, damages, expenses and costs brought against or suffered by the other or any of its respective officers, employees or agents, resulting from, arising out of or relating to: -

(i) taxes/charges/cess/levies (and interest or penalties assessed thereon) against purchaser that are obligations of MSI pursuant to this Agreement;

(ii) any damages for bodily injury (including death) and damage to real property and tangible personal property caused by the MSI;

(iii) any claim or action by or on behalf of the MSI personnel based on his or her employment with the MSI, including claims arising under occupational health and safety, worker's compensation, provident fund or other applicable laws or regulations;

(iv) claims by government regulators or agencies for fines, penalties, sanctions or other remedies arising from or in connection with the MSI failure to comply with its regulatory/legal requirements and compliances;

(v) any claim on account of an alleged breach of confidentiality and security of data occurring as a result of acts of omissions or commission of the MSI employees or sub-contractors;

(vi) any claim occurring on account of misconduct, negligence or wrongful acts of omission and commission of employees of the MSI, and/or its subcontractors;

(vii) any claim occurring on account of misuse or negligent application, misuse of systems, failure to follow established procedure by the MSI and/or sub-contractor's employees

(viii) the extent that the MSI provided to purchaser under this Agreement infringes any third party's intellectual property rights;

(ix) In event of any theft, loss, damage, destruction, or any other act of vandalism or sabotage of the property of the purchaser in the possession of the MSI by virtue of this agreement, the MSI shall be liable to indemnify the first part to the extent of damage or loss so caused.

(x) MSI has all the requisite consents, licenses and permissions to (I) enter into this Agreement (ii) carry out the obligations set out in this Agreement and it shall keep all such consents, licenses and permissions renewed and valid at all times during the continuance of the Agreement.

8.20 FORCE MAJEURE:-

i. Neither party to this AGREEMENT shall be liable for any failure or delay on its part in performing any of its obligations under this AGREEMENT if such failure or delay shall be result of or arising out of Force Majeure conditions and, provided that the party claiming Force Majeure shall use its best efforts to avoid or remove such cause of non-performance and shall fulfill and continue performance hereunder with the utmost dispatch whenever and to the extent such cause or causes are removed.

ii. Parties shall use its best efforts to avoid or remove such cause of non-performance and shall fulfill and continue performances hereunder with the utmost dispatch whenever and to the extent such cause or causes are removed.

iii. Any extraordinary event, which cannot be controlled by the parties, shall for the purpose of this AGREEMENT, be considered as a Force Majeure event. Such events include

a. war (whether declared or undeclared), invasion, armed conflict or act of foreign enemy in each case involving or directly affecting the Project Land;
b. revolution, riot, insurrection or other civil commotion, act of terrorism or sabotage in each case within the Project Land or near vicinity;
c. nuclear explosion, radioactive or chemical contamination or ionizing radiation directly affecting the Project Land and/or the Assets, unless the source or cause of the explosion, contamination, radiation or hazardous thing is brought to or near the Project Land by the Developer or any Affiliate of the Developer or any Sub-

Contractor of the Developer or any of their respective employees, servants or agents;

d. strikes, lockdown, working to rule, go-slows and/or lockouts which are in each case widespread, nationwide or political and affects the Project Land;
e. any effect of the natural elements, including lighting, fire, earthquake, unprecedented rains, tidal wave, flood, storm, cyclone, typhoon or tornado, within the Project Land or near vicinity;
f. explosion (other than a nuclear explosion or an explosion resulting from an act of war) within the Project Land or near vicinity;
g. epidemic, pandemic or plague within the Project Land or near vicinity

It is clarified that non-availability of any plant, equipment, materials or financial resources for any reason whatsoever shall not be deemed to be an event of Force Majeure

iv. Force Majeure shall not include any events caused due to acts/omissions of MSI resulting in a breach/contravention of any of the terms of the Agreement and/or MSI's Bid. It shall also not include any default on the part of MSI due to its negligence or failure to implement the stipulated/proposed precautions, as were required to be taken under the Agreement.

8.21 Limitation Of Liability

Notwithstanding anything to the contrary in this Agreement/Contract, the liability of one Party towards the other Party for any damages or compensation of any nature whatsoever under this Agreement/Contract, shall not exceed Total Project Cost. The limitation hereunder shall not apply to any or all liabilities in respect of third parties. The Parties agree that the MSI/SI/Bidder's liability will be uncapped in case of any liabilities arising due to:

i. any amount payable as indemnity to the Authority due to its acts or omissions
ii. or fraud, gross negligence and willful misconduct;
iii. breach of any Applicable Laws or any Applicable Permits;
iv. any claims or loss on account of Intellectual Property rights violation by the MSI/SI/Bidder;
v. any personal bodily injury or death of any person caused by, arising out of or in connection with its performance of this Agreement/Contract; or
vi. any loss of or physical damage to property of the Authority/Department or any third party caused by, arising out of or in connection with the performance of this Agreement/Contract

8.22 Arbitration and Jurisdiction

a. If the parties are unable to resolve the Dispute in question within thirty (30) days of the commencement to negotiations in terms of Amicable Settlement Clause then the Dispute shall, unless the parties otherwise agree in writing, be referred for determination in accordance with the remaining provisions of this clause.
b. The dispute shall be referred to arbitration in accordance with the provisions of the (Indian) Arbitration and Conciliation Act, 1996.
c. The venue for arbitration shall be Chandigarh, and the language used in the arbitral proceedings shall be English.
d. The reference shall be referred to arbitration of an Arbitrator, to be nominated and mutually decided by all the parties concerned. The Award of the Arbitrator shall be binding upon parties to the dispute.
e. The decision of the Arbitrator appointed to deal with such matters shall be accepted by the parties as final and binding.
f. The parties shall continue to be performing their respective obligations under this Agreement, despite the continuance of the arbitration proceedings, except for the disputed part under arbitration.
g. The parties shall use their best endeavors to procure that the decision of the Arbitrators shall be given within a period of Six (6) months or soon thereafter as is possible after it has been demanded.
h. This is severable from theirs to this Agreement and shall remain in effect even if this Agreement is terminated for any reason.

i. The Courts in Chandigarh, India shall have exclusive jurisdiction in relation to this Agreement, including this clause.

8.23 Documents also to be included:

(a) Copy of ESI Registration or necessary Exemption Letter for ESI Registration shall be submitted (If required).

(b) Copy of EPF Registration or necessary Exemption Letter for ESI Registration shall be submitted (If required).

SECTION 9

FORMAT TO RESPOND TO TENDER

Format 1

PRE QUALIFICATION-CUM-TECHNICAL BID

(To be submitted on its Letterhead by the bidder)

To,

Managing Director
Haryana State Electronics Development Corporation Limited (HARTRON)
SCO 111-113 Sector 17 B, Chandigarh- 160017

Dear Sir,

Subject: e-Tender/Hartron/TDS/DC/2025-26/06

1) Having examined the Tender document, I/We [name of the bidder (s)], the undersigned, herewith submit our response to your Tender Notification dated _____for selection of vendor for the Selection of System Integrator for Supply, Design, Installation, Commissioning with O&M of IT components for Haryana State Data Centre _____ in full conformity with the said tender document no _____.
2) I/We have read the provisions of the Tender document and confirm that these are acceptable to us. Hence, we are hereby submitting our Bid.
3) I/We agree to abide by this Tender, consisting of this letter, financial bid and all attachments, for a period of 240 days from date of opening of commercial bid I/We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption, in force in India.
4) I/We understand that Hartron/Department is not bound to accept/annul any bid received in response to this Tender.
5) In case, I/We are engaged by HARTRON/Department as service provider contractor for supply of ordered items/goods/items of turnkey projects, I/We shall provide all assistance/cooperation required by Hartron/ Department appointed auditing agencies officials for performing their auditing and inspection functions. I/We understand that our non-cooperation for the same shall be grounds for termination of service/contract.
6) In case, I/We are engaged as a vendor, we agree to abide by all the terms & conditions of the Contract and Guidelines issued by Hartron/Department from time to time.
7) I/ We have submitted requisite fee and EMD as per procedure laid in the Tender. All other required documents (details given in summary table below) as per the stated Qualification Criteria
8) Our Entity's profile is as under:-

S#	Required Details	Remarks
1.	Legal Name of Entity	
2.	Type of Business	☐ Corporation ☐ Individual ☐ Sole Proprietorship ☐ Joint Venture ☐ Partnership ☐ Limited Liability Partnership ☐ Other
3.	Company Identification No. (CIN)	
4.	Business Address: City District State Zip code Telephone Nos.:	

S#	Required Details	Remarks
	Contact email:	
5.	Registered Address of the Company: Address: City District State Zip code Contact Person: Telephone Nos.: Contact email: Company Website URL	
6.	PAN No. of bidder TAN No. of bidder VAT or CST or GST of bidder	
7.	Has the firm transacted business under any other previous names? If yes, under which name business transacted	☐ Yes ☐ No
8.	Ownership of the Company/Firm: Whether Company owned or controlled by parent Company? If yes, complete the following: Legal name of the parent company Full address of parent company Street City District State Zip/Pin	☐ Yes ☐ No
9.	Relationship with the parent company	☐ Subsidiary ☐ Division
10.	Date of ownership	
11.	Shareholding pattern of Parent Company:	
	Percentage of shares held by the parent company	
	Other majority shareholders in the Indian Company	
	Details of Board of Directors	
12.	Name of Bid and Contract Signing Authority – I Name Designation Contact No. Email: Power Of Attorney or resolution of Board of Directors through which authorized as signatory Authority – II Name Designation Contact No. Email: Power Of Attorney or resolution of Board of Directors through which authorized as signatory	
13.	Memorandum of Association and Articles of Association of the company Bye Laws and certificates of registration (in case of registered firm)	
14.	Whether MOA of Bidding Company allows entering	

S#	Required Details	Remarks
	into the bid of respective services? If yes, indicate the relevant clause.	

9) Our Entity's Financial Details is given as under:-

S#	Required Details	Remarks
.	Authorized Capital of the Indian Company	
2.	Paid up Capital of the Company	
3.	Turnover of the Indian company for last three years	
4.	Net worth of the Indian company for last three years	
5.	Profit of the Indian company for last three years	
6.	Customer references	
7.	Past 1-3 year supply record	
8.	Quality certificates received, if any	
9.	Customer approval letters if any	
10.	Awards and recognition received , if any	
11.	After sales support mechanism	

10) Our entity's Legal Details

S#	Required Details	Remarks
1.	Whether in the past five years prior to the date of this application, has this entity or any principal of the entity has been deemed to be in default on any contract, or been forcefully terminated from any contract of any Organization? If yes, state the names of the entity, relationship to firm and the circumstances.	☐ Yes ☐ No.
2.	Whether an undertaking (Affidavit) submitted that the bidder has not been blacklisted/debarred by any central/state Government department/organization	☐ Yes ☐ No
3.	Whether an undertaking submitted to the effect that there has been no litigation with any Government department/organization on account of similar services	☐ Yes ☐ No
4.	Whether the entity has undergone legal proceedings in the past three years. If yes, Submit details	☐ Yes ☐ No

Technical part

I/We hereby tender for the _____ and provision of services during the 5 years warranty period, as per the specifications given in this Tender document within the time specified and in accordance with the specifications and instructions:

1. HSDC Site (CAPEX-BOQ)

Sl	BOQ ITEM	Offered Make/Model	QTY
1	Rack Server 128 Core (14 U)		7
2	HCI Solution for 5 Node		1
3	Core Switch HA		2
4	SAN Switch		2
5	TOR Switch		4
6	L3 Switch		4
7	Server Virtualization Software (Latest version)		1

	(for 14 sockets (64core per socket) in 7 server)		
8	Cloud Automation, Orchestration & Management (for 14 sockets (64core per socket) in 7 server)		1
9	SDN		1
10	Server Load Balancer		2
11	Distributed Denial-of-Service(DDOS)		1
12	SSL Decryptor & SSL Encryptor		2
13	Internal Firewall		2
14	External Firewall		2
15	Web application firewall (WAF)		2
16	Purpose Built Backup Appliance		1
17	Backup Software		1
18	Enterprise Monitoring Solution (EMS), Network Monitoring Solution (NMS)		1
19	DNS Server		4

2. OPEX BOQ

Sl	BOQ ITEM	QTY
1	Operation & Maintenance	1

Yours Sincerely,
Authorized Signatory (ies) [In full and initials]: _____
Name and Title of Signatory (ies): _____
Name of Bidding Company/Firm: _____
Address: _____ ***(Affix the Official Seal of the Bidding Company)***

Format 2
COMMERCIAL BID
(To be uploaded by the bidder in given Excel Sheet on NIC Portal only)

To,
Managing Director
Haryana State Electronics Development Corporation Limited (HARTRON)
SCO 111-113 Sector 17 B, Chandigarh 160017

Subject: e-Tender/Hartron/TDS/DC/2025-26/06

I/We hereby tender for the _____ and provision of services during the 5 years warranty period, as per the specifications given in this Tender document within the time specified and in accordance with the specifications and instructions. Mentioned below are the rates quoted in the prescribed format are FOR destination inclusive of all taxes: -

A. HSDC Site (CAPEX-BOQ)

Company Name :

S#	BOQ ITEM	QTY (A)	Make & Model	Basic Unit Price with one year warranty (₹) (B)	Additional four years warranty price in (₹) (C)	Applicable Taxes & Duties/GST on B+C= (D)	Total Price (₹) All inclusive E= AX(B+C+D)	Currency in case of import items	Import content in %
1	Rack Server 128 Core (14 U)	7							
2	HCI Solution for 5 Node	1							
3	Core Switch HA	2							
4	SAN Switch	2							
5	TOR Switch	4							
6	L3 Switch	4							
7	Server Virtualization Software (Latest version) (for 14 sockets (64core per socket) in 7 server)	1							
8	Cloud Automation, Orchestration & Management (for 14 sockets (64core per socket) in 7 server)	1							
9	SDN	1							
10	Server Load Balancer	2							
11	Distributed Denial-of-Service(DDOS)	1							
12	SSL Decryptor & SSL Encryptor	2							
13	Internal Firewall	2							

14	External Firewall	2							
15	Web application firewall (WAF)	2							
16	Purpose Built Backup Appliance	1							
17	Backup Software	1							
18	Enterprise Monitoring Solution(EMS),Network Monitoring Solution (NMS).	1							
19	DNS Server	4							
A	**Total**								

- For DNS Server :
    - 2 numbers of DNS Server should be installed with Red hat Enterprise Linux Server Standard subscription for 5 years and
    - 2 numbers of DNS Server should be installed with Windows server Standard edition with 5 years subscription

B. OPEX BOQ

Sl	BOQ ITEM	QTY (A)	Basic Unit Price (₹) (B)	Applicable Taxes & Duties/GST (C)	Unit Price (₹) All inclusive (D = B+C)	Total [E=A*D]
1	Operation & Maintenance for a period of 01 year	1				
B	**Total**					

- O&M of manpower support is initially for first year and is extendable on annual basis up to the period of 5 years
- The Capex & Opex ratio should not be greater than 70:30 of the total quoted value including all taxes & duties.
- Bidder has to disclose the man month rate for each role applicable for 1st year as per format below which in-accordance to overall cost quoted for OPEX cost for DC.

Sl	Role	Expertise Level	1st Year Man Month Rate
1	Project Manager	L4	
2	Network and Security Expert	L3	
		L2	
3	DC Cloud solution Expert including HCI	L3	
		L2	
4	DBA	L3	
		L2	
5	Storage and Backup Expert	L3	
		L2	
6	Server Expert/System Administrator	L3	
		L2	
		L1	

7	NOC Engineer	L1	
8	Helpdesk Engineer	L2	
		L1	
9	BMS Expert	L3	
		L2	
		L1	
		Total	

5. Bidder has to disclose the man month rate for each role applicable from 2rd year onwards as per format below in case the Purchaser intends to extend some resources beyond 1st year of OPEX period. These rates shall not increase more than 10% of 1st year or preceding year man month rate of that role. The discovery of these rates shall not be considered for financial evaluation i.e. declaring L1. However, the Purchaser reserves the right to compare the rates offered by L1 bidder with other bidders for the similar role and can negotiate the same before placing final Work Order.

Sl	**Role**	**Expertise Level**	**2nd Year Onwards Man Month Rate**
1	Project Manager	L4	
2	Network and Security Expert	L3	
		L2	
3	DC Cloud solution Expert including HCI	L3	
		L2	
4	DBA	L3	
		L2	
5	Storage and Backup Expert	L3	
		L2	
6	Server Expert/System Administrator	L3	
		L2	
		L1	
7	NOC Engineer	L1	
8	Helpdesk Engineer	L2	
		L1	
9	BMS Expert	L3	
		L2	
		L1	
		Total	

Note:

1. The L1 will be discovered on total bid value = A+B. The operation & Maintenance cost (Man Power cost) for 2nd year will not be included in the financial evaluation used to determine the L1 (lowest) bidder.
2. In the interest of competition, the Bidder may offer max up to two OEMs for any BOQ item of this RFP provided the offered product/ OEM fully complies with the eligibility & specifications as mentioned in the RFP. In case the product offered is not compliant due to any reason, the option Bidder shall not be allowed to exercise the option. Further, in such cases, the financial cost offered for that BOQ item for both the OEM options shall remain the same (financial bid). Furthermore, the Purchaser shall have the liberty to choose any of the offered OEM for a BOQ item (in case of multiple OEMs offered) considering the overall solution design, past experience, better support availability, better/ additional features if available, etc. without any extra cost to the purchaser.
4. The number of items may be increased / decreased at any time before signing of agreement/contract.

5. The CAMC of all active LAN components and UPSs will be as per State Govt's. approved CAMC Policy:

https://cdnbbsr.s3waas.gov.in/s35352696a9ca3397beb79f116f3a33991/uploads/2023/02/2023020883.pdf

The bid found in any other currency shall be summarily rejected.
No upward revision shall be allowed in the case of any fluctuation in the foreign currency

1. Period of Delivery: We do hereby undertake that in the event of acceptance of our bid, the supply of mentioned items will be completed within stipulated delivery period as motioned in RFP from the date of issues of Award of Contract/work order unless otherwise specified in the work order.
2. Terms of Delivery: The landed prices quoted are inclusive of current Excise Duty, Freight, Insurance, Sales Tax, etc.
3. **Right to vary quantity**
   i. At the time of award of contract, the quantity of goods, works or services originally specified in the bidding documents may be increased or decreased. It shall be without any change in the unit prices or other terms and conditions of the bid and the bidding documents
   ii. If the purchaser does not procure any subject matter of procurement or procures less than the quantity specified in the bidding documents due to change in circumstances limited to variation up to 25% of the total quantity (if the quantity is greater than equal to unit of measure), the Bidder shall not be entitled for any claim or compensation except otherwise provided in the bidding document. In case the quantity is less than 4 units, the Purchaser reserves the right to procure 1 unit of measure of the equipment specified.
   iii. Repeat orders for extra items or additional quantities may be placed limited to variation up to 25% of tender value (as indicated above) for next 2 years from the date of project Go Live on the rates and conditions given in the contract.
   iv. In case of delivery of any extra item or additional quantity, dollar or foreign currency hedging clause/ provisions would be applicable. In that case, the bidders would need to indicate the import content(s) and the currency (ies) used for calculating the value of import content(s) in their total quoted price, which (that is, the total quoted price) will be in Indian Rupees. The bidder to also indicate the Base Exchange rate for each such foreign currency used for converting the foreign exchange content into Indian Rupees at the time of bidding. Any increase or decrease in price by reason of the variation in the rate of exchange in terms of the contract will be borne by the bidder, if the prices are within or equal to 15% of variation. However, at the time of additional purchase, if there is a variation beyond 15% of the foreign currency/ dollar value, both parties shall bear 50% of the variation cost beyond 15%.
4. We agree to abide by our offer for a period of 240 days from the date of opening of commercial bid and that we shall remain bound by a communication of acceptance within that time.
5. We hereby certify that we have read and understood the terms and conditions applicable to the bidder and we do hereby undertake to supply as per these terms and conditions.
6. Validity of commercial bid: should be 240 days from the date of opening of commercial bid
7. A company and the person signing the bid/offer is the constituted attorney.

We do hereby undertake that until a formal Contract is prepared and executed, this bid, together with your written acceptance thereof and placement of letter of intent/ awarding the Contract shall constitute a binding Contract between us.

Yours Sincerely,
Authorized Signatory (ies)[In full and initials]: _____
Name and Title of Signatory (ies): _____
Name of Bidding Company/Firm: _____
Address: _____ *(Affix the Official Seal of the Bidding Company)*

ANNEXURE 1

Bidding Document Acknowledgement Form

(To be enclosed with technical bid)

To,
Managing Director
Haryana State Electronics Development Corporation Limited (HARTRON)
SCO 111-113 Sector 17 B, Chandigarh 160017

Subject: e-Tender/Hartron/TDS/DC/2025-26/06

I/We hereby acknowledge we have downloaded a complete set of Bidding Document enclosed to the "Invitation for Bid" pertaining to tender Notification dated _____ along with corrigendum, if any, for the selection of vendor for the supply of mentioned items _____

I/We have noted that the closing date for receipt of this tender document by Hartron is _____ at 2:30 PM.

I/We guarantee that the contents of the above said Bidding Documents will be kept confidential within our organization and text of the said documents shall remain the property of Hartron and that the said documents are to be used only for the purpose intended by Hartron. Duly signed and stamped copy of tender document is also enclosed.

Authorized Signatory (ies)[In full and initials]: _____

Name and Title of Signatory (ies): _____

Name of Bidding Company/Firm: _____

Address: _____ *(Affix the Official Seal of the Bidding Company)*

ANNEXURE 2
Undertaking for not blacklisted
(To be submitted on Letterhead by the bidder)

Date: _____

From (Name of bidder)
_____
_____

Subject: e-Tender/Hartron/TDS/DC/2025-26/06

The Managing Director,
Haryana State Electronics Development Corporation
SCO 111-113 Sector 17 B, Chandigarh 160017

I, _____son of Sh. _____ resident of _____do hereby solemnly affirm and declare as under: -

That we M/s _____ hereby confirm that we M/s _____ has not been blacklisted by any State Government/ Central Government/ Public Sector Undertakings/TSP/BFSI as on bid submission date and further confirm that our EMD/SD/Performance bank guarantee has not been forfeited by any State Government / Central Government / Public Sector Undertakings as on bid submission date due to our non-performance, non-compliance with the tender conditions etc.

That we M/s_____ hereby declare that all the particulars furnished by us in this Tender are true to the best of my/our knowledge and I/We understand and accept that if at any stage, the information furnished is found to be incorrect or false, I/We am/ are liable for disqualification from this tender and also are liable for any penal action that may arise due to the above.

That we M/s _____ certify that no refurbished components are used in the manufacturing and supply of Quoted Items and its related accessories / tendered items.

That in case of violation of any of the conditions above, We M/s _____ understand that We M/s _____are liable to be blacklisted by Hartron **for a period of three years** from participating any tender published by Haryana Government.

Yours Sincerely,
Authorized Signatory (ies) [In full and initials]: _____
Name and Title of Signatory (ies): _____
Name of Bidding Company/Firm: _____
Address: _____ ***(Affix the Official Seal of the Bidding Company)***

ANNEXURE 3
Statutory Undertaking
(To be enclosed with Technical bid)

Date: _____

Managing Director
Haryana State Electronics Development Corporation Limited (HARTRON)
SCO 111-113 Sector 17 B, Chandigarh 160017

Subject: e-Tender/Hartron/TDS/DC/2025-26/06

I/We **(Name of the Bidder)** having registered office at **(Address of the registered office)** and local office at (Address of the local office), hereby declare and confirm that-

1) The contents of the Tender have been carefully gone through and we undertake to fully comply with the terms and conditions specified in the tender document including addendum, if any thereof.

2) I/We are not engaged into litigation as of date with any Government Department/ PSU/ Autonomous body on account of similar services for indulging in corrupt or fraudulent activities. We also confirm that we are not determined non-performing by any of the entities specified above.

3) Neither the Bidder nor any of its Directors are the subject of criminal or civil proceedings that could be expected to adversely affect its business or its ability to Bid in the present tender.

4) We understand that the technical Bid, if found incomplete in any respect and/or if found with conditional compliance or not accompanied with the requisite Bid Security/ Earnest Money Deposit, shall be summarily rejected.

5) We understand that if at any time, any averments made or information furnished as part of this Bid is found incorrect, then its Bid and the contract if awarded on the basis of such Bid shall be cancelled.

6) We offer to execute the work in accordance with the Terms of Reference and Conditions of Contract of this Tender.

7) The information provided in the technical proposal (including the attachments) is true, accurate and complete to the best of my knowledge & belief.

Authorized Signatory (ies)[In full and initials]: _____
Name and Title of Signatory (ies): _____
Name of Bidding Company/Firm: _____
Address: _____ *(Affix the Official Seal of the Bidding Company)*

ANNEXURE 4
Technical Compliance
(To be enclosed with Technical bid)

Dated: _____

Managing Director
Haryana State Electronics Development Corporation Limited (HARTRON)
SCO 111-113 Sector 17 B, Chandigarh 160017

Subject: e-Tender/Hartron/TDS/DC/2025-26/06

I/We M/S---------- having registered office at (Address of the registered office) and local office at (Address of the local office), hereby declare and confirm that the specifications of the items offered match/exceed the ones quantified as minimum requirements in the Tender document.

I/ We, M/S---------- further undertake that following equipment to be supplied by us hereunder shall be brand new, free from all encumbrances, defects and faults in material, workmanship and manufacture shall be of the highest grade and quality and consistent with the established and generally accepted standards for materials of the type ordered shall be in full conformity with the specifications, drawings or samples, if any, and shall operate properly: -

Note: The Compliance should be submitted as per the following as under :

a. **The Compliance of Minimum Technical Specifications for each offered items/components mentioned in Section 5 of this RFP must be provided by bidder on OEM & Bidder letter head.**

b. **The Compliance of technical specifications of offered Products/ items (offered make & model) as per the format mentioned below;**

Sr. no.	Parameter	Minimum specification	Compliance Yes/No

Authorized Signatory (ies)[In full and initials]: _____
Name and Title of Signatory (ies): _____
Name of Bidding Company/Firm: _____
Address: _____ *(Affix the Official Seal of the Bidding Company)*

Annexure 5
Manufacturers'/Producers Authorization Form
(To be provided by OEMs of devices as mentioned in this tender document on their Letterhead)

Dated: _____

Managing Director
Haryana State Electronics Development Corporation Limited (HARTRON)
SCO 111-113 Sector 17 B, Chandigarh 160017

Subject: e-Tender/Hartron/TDS/DC/2025-26/06

Subject: <<Regarding Tender Ref No.:_____ Dated:_____>>

Sir,

This is to certify that We <Name of OEM> are the Original Equipment Manufacturer in respect of the products listed below. I/We confirm that

1. <Name of Bidder> is our National Distributor / Distributor / Company / System Integrator / Firm for offered products i.e. ……..
2. <Name of Bidder> have due authorization from us to provide product(s) listed below and related services of warranty, licensing and maintenance.
3. We as OEM or parent company or major promoter of the OEMs directly/ indirectly, shall not be from or belong to the countries sharing land borders with Indian Territory as per notification No:02/09/2020 – 4IB – II Dated 10-12- 2020 of the Department of Industries & Commerce Govt. of Haryana.
4. We warrant that,

a) All products supplied by us in this RFP shall be brand new, latest edition/model of applicable category, free from all defects and faults in material, workmanship and manufacture. They shall be of the highest grade and quality and shall be consistent with the established industry standards.

b) All hardware & software to be supplied under this tender have been provisioned with OEM comprehensive onsite warranty for 5 years from T5 timeline as per Project Milestone & Deliverable of this RFP.

c) The support including spares, update, upgrades, fixes, patches for the supplied products shall be available for even after 2 years (at least) from applicable 5 years warranty period as mentioned in point (b) above.

d) OEM agrees to support the product i.e. CAMC/AMC/ATS (Annual Technical Support) shall be applicable as per CAMC/AMC policy notified by CRID (formerly DITECH) Haryana vide circular no. 2/300/18122 dated 11.11.2022 and as updated from time to time.

e) Equipment/components of the infrastructure supplied under this RFP (hardware & or associated software item) shall not be declared "End of Sale" for next 18 months from bid submission date.

f) Supplied equipment/components under this RFP shall not be declared "End of Service/Support Life" till scope of this RFP + 2 years from bid submission date.

g) If any supplied product is de-supported by the us/OEM for any reason whatsoever we/OEM agrees to replace it with same or better substitute that is acceptable to CRID without any additional cost to the CRID and without impacting the performance of the solution in any manner whatsoever.

h) In case there is a shortfall in overall warranty period due to the time gap between warranty period ((b) above) and Go-Live date, we will ensure to support the Purchaser through the bidder for back-to-back warranty for the shortfall period. In case, the bidder is not

associated with the project at any stage, the back-to-back warranty shall be extended through our Authorized Service Provider/ alternate SI selected for this project by the Purchaser. This is to ensure that the overall warranty as per the scope and terms & conditions of the RFP is complied with.

~~i)~~ We will provide comprehensive warranty support as per the requirement of this tender for the total contract period as per RFP.

Sr. No.	RFP Item	Product Name	Make	Model
1				
2	…			

Thanking You,

Yours faithfully,

Authorized Signatory (ies)[In full and initials]: _____

Name and Title of Signatory (ies): _____

Name of Bidding Company/Firm: _____

Address: _____*(Affix the Official Seal of the Bidding Company)*

ANNEXURE 6

Undertaking for honoring warranty

(To be enclosed with Technical bid and to be submitted by the bidder on its letter head)

Dated:-

Managing Director
Haryana State Electronics Development Corporation Limited (HARTRON)
SCO 111-113 Sector 17 B, Chandigarh 160017

Sub: Undertaking for honoring warranty for the period indicated in the contract

Subject: e-Tender/Hartron/TDS/DC/2025-26/06

This bears reference to our quotation Ref. _____ Dated _____

We warrant that,

1) All products supplied by us in this RFP shall be brand new, latest edition/model of applicable category, free from all defects and faults in material, workmanship and manufacture. They shall be of the highest grade and quality and shall be consistent with the established industry standards.
2) We shall provide the documentary proof for warranty and proof of purchase at the time of deployment of infrastructure
3) Equipment/components of the infrastructure supplied under this RFP (hardware & or associated software item) shall not be declared "End of Sale" by the respective OEM for next 18 months from bid submission date.
4) If the infrastructure supplied by us is not-supported by the respective OEM during the period of contract for any reason, we will replace the product with a suitable same/higher hardware/software, meeting technical compliance as per RFP, for which support is provided by the OEM at no additional cost to Hartron/Indenting department and without impacting the performance or timelines of this project/agreement/contract.
5) If any hardware/software is not meeting technical compliance as per RFP for any reason, we will provide the hardware/software ensuring technical compliance as per RFP at no additional cost to Hartron/Indenting department and without impacting the performance or timelines of this project/agreement/contract.
6) We would provide on-site warranty support of the installed system(hardware & Software) for a period of 5 years from Go Live acceptance of the system (overall project) within the price quoted by us in the Commercial Bid.
7) In case, there is a shortfall in overall warranty period due to the time gap between installation date and Go-Live date, we will ensure back to-back OEM warranty for equipment for the shortfall period in order to comply with the scope and terms & conditions of the RFP, without any additional cost to the purchaser.

Authorized Signatory (ies)[In full and initials]: _____
Name and Title of Signatory (ies): _____
Name of Bidding Company/Firm: _____
Address: _____ *(Affix the Official Seal of the Bidding Company)*

Annexure 7

Checklist to be enclosed with Technical bid

Dated:-

Managing Director
Haryana State Electronics Development Corporation Limited (HARTRON)
SCO 111-113 Sector 17 B, Chandigarh 160017

Subject: e-Tender/Hartron/TDS/DC/2025-26/06

We M/s _____ has enclosed documentary evidence for fulfilling the Eligibility in the Technical Bid and other requirement laid in the tender document.

S#	Clause	Documents Required	Document Attached (Yes/No)	Bid. Pg. no.
	Processing fee for Tender should be submitted.	The Payment for Tender Document Fee ₹5,900/- (Rupees Five Thousand Nine Hundred Only) i.e. (₹5,000/- + 18% GST) and ₹1,180/- eService Fee i.e. (₹1,000+18% GST)can be made by eligible bidders through Online Mode at NIC Portal in favor of Haryana State Electronics Development Corporation Limited. Scanned copy of Online Payment Receipt should be uploaded with technical e-bid.		
	EMD fee	The Payment for EMD (refundable) of Rs.5,00,000/- (Rupees Five Lacs only) can be made by eligible bidders through Online Mode Available on NIC Procurement Portal). Scanned copy of Online Payment Receipt should be uploaded along with technical bid.		
		The Payment of Rs.45,00,000/- (Rupees Forty-Five Lacs only) also will be made by eligible bidders in the form of Bank Guarantee (BG) in favor of Director (Administration), Citizen Resources Information Department, Room no-42, 9th floor, Haryana Civil Secretariat, Sector-1, Chandigarh-160001 and will be submitted along with the technical bid in original.		
1.	The Bidder must be incorporated and registered in India under the Indian Companies Act 1956 or 2013, or a Limited Liability	Copy of Certificate of Incorporation / Registration under Companies Act 1956/2013 Articles of Association Partnership Deed for Partnership		

S#	Clause	Documents Required	Document Attached (Yes/No)	Bid. Pg. no.
	Partnership (LLP) registered under the LLP Act, 2008 or Indian Partnership Act 1932 and should have been in operation in India for a minimum of seven years as on Bid Submission Date.	Firms		
2.	The Bidder should have an average annual turnover of at least Rs 100 Cr from the IT System Integration/ Information Technology Infrastructure Projects Including implementation, operations & maintenance	Audited Balance sheet and Profit & Loss account statement or CA Certificate or Statutory Auditor Certificate of the Bidder for each of the last 3 Financial Years FY 2021-22, 2022-23, 2023-24, Considered balance sheet and loss & Profit statement of FY 2024-25 (if audited).		
3.	The bidder should have positive net worth (measured as paid up capital plus free reserves) in last 3 Financial Years FY 2021-22, 2022-23, 2023-24, Considered balance sheet and loss & Profit statement of FY 2024-25 (if audited).	i) CA Certificate / Statutory Auditor Certificate of the Bidder confirming the net-worth and profit after Tax for each of the last 3 financial years. ii) The net worth of the Bidder firm (manufacturer or principal of authorized representative) should not be negative and also should have not eroded by more than 30% (thirty percent) in the last three financial years.		
4.	The Bidder should possess all below certifications or latest which are valid as on bid submission date: 1. ISO 9001:2008 / ISO 9001:2015/ 2018 for Quality Management System 2. ISO or IEC 20000: 2011 for IT Service Management 3. ISO 27001:2013 for Information Security Managements	Copies of the valid certificates from authorized agencies.	iii)	iv)
5.	The Bidder should have: PAN card GST Registration Number	i) Copies of the valid certificates from authorized agencies ii) Income Tax registration / PAN number GST Registration Certificate	iii)	iv)

S#	Clause	Documents Required	Document Attached (Yes/No)	Bid. Pg. no.
6.	The Bidder should have experience in Supply, Design, Build, Installation, Commissioning with Operations and Maintenance **of IT components for Data Center** (Tier-IV/ Tier-III / Tier-II) for any Centre or State or UT Govt or PSU or National BFSI or National TSPs from Apr 2018 to till bid submission date (Only ICT Infra, manpower etc. excluding construction of building): a) **Three** (3) completed/ongoing orders each having minimum value of Rs 20 Cr (~40% of the estimated tender value) or more. OR b) **Two** (2) completed/ongoing orders each having minimum value of Rs 25 Cr (~50% of the estimated tender value) or more. OR c) **One** (1) completed/ongoing order of value Rs 40 Cr (~80% of the estimated tender value) or more. In last 7 financial years i.e. 2018-19, 2019-20, 2020-21, 2021-22, 2022-23, 2023-24, 2024-25 **IT components (as per BOQ of this RFP)** which includes Servers **and** network switching & routing **and** Security components(Firewall, DDoS, WAF, etc) **and** Virtualizations, HCI **and** Backup system, etc	Contract signed with client clearly highlighting the Scope of Work, Bill of Material and value of the Contract/order Completion Certificate issued & signed by the competent authority of the client entity on the entity's letterhead (For completed project) Bidder project experience of on-going projects with at least management (IT & Non IT) of minimum 5 racks in O&M phase shall be considered when 1) Go Live certificate signed by the authorized signatory of the client entity on the entity's letterhead for in order to ensure that the project is in Go Live phase or 2) Certificate signed by the authorized signatory of the client entity on the entity's letterhead for in order to ensure that the project-t is in O&M phase and is being run by the SI (initiated or completed or on going since Apr 2017 to till as on bid submission date) 3) In Case the desired tier certificate is not available/expired, the bidder to submit uptime Certificate of 99.74% or above issued & signed by the authorized signatory of the client entity on the entity's letterhead for consideration.	v)	vi)
7.	The Signatory signing the Bid on behalf of the Bidder should be duly authorized by the Board of Directors of the Bidding Company to sign the	i) A Certificate from the Company Secretary of the Bidder certifying that the Bid signatory is authorized by the Board of	ii)	iii)

S#	Clause	Documents Required	Document Attached (Yes/No)	Bid. Pg. no.
	Bid on their behalf.	Directors of the Company to do so, with acceptance of board resolution, resolution number and date		
8.	Bidder shall have office or local contact available in Tri-city (Chandigarh, Mohali and Panchkula)	i) Copies of rent agreement/proof of ownership of office or address detail of local contact in Tri-city (Chandigarh, Mohali and Panchkula) if available. OR ii) In case there is no existing office or local contact, an undertaking from the authorized signatory to establish the local contact or open the office within one month (30 days) from the date of award of contract in Tri-city (Chandigarh, Mohali and Panchkula)	iii)	iv)
9.	<u>OEM Criteria</u> 1.The OEM should be in the manufacturing of offered products or equivalent during any 3 out of 5 financial years (2020-21,2021-22,2022-23, 2023-24, 2024-25) 2. The OEM should have executed orders of quantity 300% of required tender quantity of the respective product with nearly similar type or configuration or size. The orders should be executed on behalf of any Central or State Govt or PSUs or National BFSI or National TSPs during the last 5 years as on bid submission date (2020-21,2021-22, 2022-23, 2023-24,2024-25) . 3. OEM of offered products must have their own Technical service & support Centre in India. 4. Authorization from OEM for confirming that the products quoted are not "end of life or end of sale products" shall be available for next 5 years from achieving Go-Live of the project.	1 Work orders or contract Agreement or supply order 2. Work Order or Contract Agreement or supply order 3. Documentary evidence for support center in India to be provided. 4 & 5. Documentary evidences such as Authorization letters MAF (Manufacturer's Authorization Form) from all OEMs whose products are being quoted by the Bidder need to be attached in the proposal as per format provided in RFP. 6 & 7. Self-Certification/ Declaration Certificate / affidavit duly signed by authorized signatory on company letter head	The OEM should have executed	

S#	Clause	Documents Required	Document Attached (Yes/No)	Bid. Pg. no.
	5. Undertake that the support including spares, update, upgrades, fixes, patches for the quoted products shall be available for next 5 years from achieving Go-Live of the project. 6. Undertaking from OEM to support directly, if needed, including delivery against defectives also within the scope of project (A certificate from OEM to provide support for the products with pre-qualification bid) 7. Undertaking for the proposed supplied equipment/product in the tender to discharge all responsibilities under warranty for the period indicated in the contract, in case the bidder fails to do the same for any reason.			
10.	Compliance from Bidder & OEM for detailed technical specifications of all the Products offered in this bid as per Bill of material (BOM)	The bidder must **enclose with a self-declaration the** item wise compliance for the technical specifications duly vetted by the respective OEMs specific to this tender **on respective OEM's letterhead**. The Model and Make/Version of the offered products should be clearly specified in the compliance document(Bill of material (BOM))		
11.	<u>Undertaking by Bidder & its OEMs</u> 1. Not be insolvent, bankrupt or being wound up, not have its affairs administered by a court or a judicial officer, not have its business activities suspended and must not be the subject of legal proceedings for any of the foregoing reasons; 2. Not blacklisted with any of the	Self-Certification/ Declaration Certificate / affidavit duly signed by authorized signatory on company letter head and as indicated in MAF (Manufacturer's Authorization Form)		

S#	Clause	Documents Required	Document Attached (Yes/No)	Bid. Pg. no.
	State/Central Government as on the date of submission of the bid. 3. No Dispute with Bidder or their OEM as on date of submission of bid related to supply/execution/implementation of any item placed by CRID(DITECH)/ HARTRON. 4. Undertaking from Bidder or Parent Company or major promoter of the OEMs directly/indirectly shall not be from or belong to the countries sharing land borders with Indian Territory. OR Bidder or its OEM from a country that shares a land border with India will be eligible to bid in this tender only if the bidder is registered with the Competent Authority. Bidder or its OEM has to undertake compliance as per Notification No:02/09/2020 – 4IB – II Dated 10-12-2020 of the Department of Industries & Commerce Govt. of Haryana. Any false declaration and non-compliance of this would be a ground for immediate termination of the contract and further legal action in accordance with the laws 5. Undertaking from			

S#	Clause	Documents Required	Document Attached (Yes/No)	Bid. Pg. no.
	Bidder & its OEM that they are registered entity in India & have direct presence in India for more than 5 years as on bid submission date 6. In case of additional purchase,If at any time during the execution of the contract the SI reduces the sale price or sells or offers to sell such scope of work as are covered under the contract, to any person or organization including the purchaser or any department of Central Government/State Government at a price lower than the price chargeable under the Contract, he/she shall forthwith notify such reduction or sale or offer of sale to the purchaser and the price payable under the contract for the supplied Bills of Quantity after the date of coming into force of such reduction or sale or offer of sale shall stand correspondingly reduced. An undertaking to this effect must be submitted along with tender.			
12.	ISO Certification	ISO 9001:2015/2018 or latest Certificate issued in the name of Bidder & OEM and ISO 14001 Certificate issued in the name of OEM for handling of hazardous items in the manufacturing process. **Note:- Applicable to OEMs involved in manufacturing of Hardware equipment only.**		

S#	Clause	Documents Required	Document Attached (Yes/No)	Bid. Pg. no.
13.	Product certification	As mentioned in the Technical Specification.		
14.	Certifications / Compliance	The Bidder should have all necessary certifications permissions, consents, NOCs, approvals as required under law for carrying out its business. The Bidder should have currently valid GST No. and PAN No.		
15.	No Dispute with Bidder or their OEM/Principal	At the time of submission of bids, there should be no dispute with the OEM/Bidder related to supply of any item placed by HARTRON. Bid of such OEM and their product/bidder will not be considered. (Annexure 13 & 14)		
16.	The concessions/Benefits are allowed to MSMEs as per Haryana State Public Procurement Policy for MSMEs-2016	The details of Haryana State Public Procurement Policy for MSMEs-2016 can be obtained from website of Directorate of Supplies & disposal Haryana (http://dsndharyana.gov.in/writereaddata/Document/1_93_1_msme_policy.pdf)		
17.	Technical Bid	Format 1		
18.	Commercial Bid	Format 2		
19.	Acknowledgement of bid document	Annexure 1		
20.	Self-Declaration on not being blacklisted	Annexure 2		
21.	Statutory undertaking	Annexure 3		
22.	Technical Compliance	Annexure 4		
23.	Certificate of Dealership/ Authorization	Annexure 5		
24.	Undertaking for honoring warranty	Annexure 6		
25.	Checklist	Annexure 7		
26.	After sales services	Annexure 8		
27.	Undertaking of rates	Annexure 9 (to be enclosed with Technical bid)		
28.	Format for Relaxations to Micro Small Enterprise registered in Haryana	Annexure 10		
29.	Format for Relaxations to Medium Enterprise registered in Haryana	Annexure 11		
30.	Authenticity of submitted documents/information	Annexure 12		
31.	Affidavit	Annexure-13		
32.	Compliance regarding restrictions under Rule 144	Annexure-14		

S#	Clause	Documents Required	Document Attached (Yes/No)	Bid. Pg. no.
	(xi) of the General Financial Rules (GFRs), 2017			
33.	Undertaking for Choice of payment option	Annexure-15		
34.	undertake that following equipment to be supplied by us is considered to be of different OEMs.	Annexure-16		
35.	Scope of existing MSI	Annexure 17		
36.	Tender Document	Signed and stamped copy of tender documents		

Authorized Signatory (ies)[In full and initials]: _____
Name and Title of Signatory (ies): _____
Name of Bidding Company/Firm: _____
Address: _____ *(Affix the Official Seal of the Bidding Company)*

ANNEXURE 8
(To be enclosed with Technical bid)

AFTER SALES SERVICE CERTIFICATE

Dated:-

Managing Director
Haryana State Electronics Development Corporation Limited (HARTRON)
SCO 111-113 Sector 17 B, Chandigarh. 160017

Subject: e-Tender/Hartron/TDS/DC/2025-26/06

Whereas, we M/s (Bidder Name) are established & reputable OEMs for sales & services of (Make of items) of [items name] having service offices at Tricity (Mohali, Chandigarh, Panchkula),Haryana/-. Details are as under:

S#	Address of Service Centre	Phone No	Number of Engineers
1.			
2.			
3.			
4.			
5.			
6.			

We do hereby confirm that:

Services including repair/replacement of defective parts will be done by us and fully backed by (name of the OEM). Replacement of defective Systems/parts will be done by equivalent or better systems/parts of the same make. We will attend all the complaints/service calls as per SLA. Down time will not exceed beyond SLA. In case, down time exceeds from SLA, then we will extend the warranty period of that item(s) double of the down time.

Authorized Signatory (ies)[In full and initials]: _____
Name and Title of Signatory (ies): _____
Name of Bidding Company/Firm: _____
Address: _____ *(Affix the Official Seal of the Bidding Company*

ANNEXURE 9
To be enclosed/uploaded with the commercial bid
UNDERTAKING OF RATES

Dated:-

Managing Director
Haryana State Electronics Development Corporation Limited (HARTRON)
SCO 111-113 Sector 17 B, Chandigarh 160017

Subject: e-Tender/Hartron/TDS/DC/2025-26/06

We M/s _____ do hereby confirm that:

The rates quoted against this offer are lowest possible and as on date we have not quoted less rates to any other customer than the rates quoted herein..

In case,

a. we quote less rates than this offer to any other customer within 1 month of the due date of this offer or before issuance of LOI (whichever is later) or
b. in case our Company/principal OEM/supplier officially reduce the price compared to the offered price before delivery as per delivery milestone schedule
c. then the benefit for the same will be passed to Purchaser of equal reduced amount or mutually agreed reduced rates.

We M/s _____ further undertake that any price benefit on account of providing higher version of "Offered items" than the required/specified in this offer shall not be claimed by us either from Hartron or from indenting Department.

Authorized Signatory (ies)[In full and initials]: _____
Name and Title of Signatory (ies): _____
Name of Bidding Company/Firm: _____
Address: _____ *(Affix the Official Seal of the Bidding Company)*

ANNEXURE 10

(To be submitted on its Letterhead by the bidder)

Format for Relaxations to Haryana based manufacturing Micro & Small Enterprises (MSEs)

Format of Affidavit

(Seeking benefits/concessions Past Performance/Experience & Purchase Preference by Haryana based manufacturing Micro & Small Enterprises (MSEs) in the State Public Procurement)

Subject: e-Tender/Hartron/TDS/DC/2025-26/06

I_____S/o_____aged_____residing at _____Proprietor / Partner / Director of M/s_____ do hereby solemnly affirm and declare that:-

1. My/our above noted enterprise M/s (name and Address)_____has been issued Manufacturing Entrepreneurs Memorandum in Haryana by the District Industries Centre_____ under acknowledgement No._____ of dated _____(Self Certified Copy of the same be attached as **Annexure 'A'** with this Affidavit) and has been issued for manufacture of the following items in **category Micro & small Enterprises** (please tick the either) as under:-
   i. _____
   ii. _____
   iii. _____
2. That the quoted items(s) in the tender_____is one (or more) of the item for which my/our above noted enterprise has been issued manufacturing Entrepreneurs Memorandum by the Industry Department Haryana as per details at the para 1 above.
3. That my/our above mentioned manufacturing Micro/Small Enterprises fulfils either or both of the below mentioned eligibility criteria:
   i. That my/our above mentioned enterprise has been issued quality certification of ISI mark/ISO/Ag. Mark /any other quality mark_____(Please tick either of the option) by_____(name of GOI/State Govt. Agency/institution authorized by GOI/State Govt.) on _____and the same is valid from_____ to _____ in respect of item/good (give name of item/good)_____mentioned in the tender (self certified copy of the relevant certificate is attached as Annexure-'A' with this affidavit)

   OR/AND

   ii. That my/our above mentioned enterprises has been registered with DGS&D, GOI/NSIC/Govt. Of India Departments/ State Govt. Department/Govt. Of India Public Sector Undertakings (PSUs) or State Govt. Public Sector Undertakings (PSUs) (**Please tick one of the option as above)** in respect of name of item/goods/works/services_____**(Name)** as mentioned in the tender for the corresponding period of time of this tender. A self certified copy of the same attached as **Annexure 'B'** with the affidavit.
4. That in case the work order of the quoted item is issued to me/us, it will not be outsourced or subcontracted to any other firm and the entire manufacturing of the order item shall be done in-house by our Enterprise base in Haryana (address mentioned as at Sr. No.1). Further, the billing will be done from Haryana.

Authorized Signatory (ies)[In full and initials]: _____
Name and Title of Signatory (ies): _____
Name of Bidding Company/Firm: _____
Address: _____ *(Affix the Official Seal of the Bidding Company)*

Annexure 11
(To be submitted on its Letterhead by the bidder)

Format for Relaxations to Haryana based manufacturing Medium Enterprise

Format of Affidavit

(for seeking the benefits/concessions by Haryana based manufacturing Medium enterprises in past Performance/Experience & Purchase Preference in the State Public Procurement)

Subject: e-Tender/Hartron/TDS/DC/2025-26/06

I_____S/o _____aged_____ residing at _____Proprietor/Partner/Director of M/s_____ do hereby solemnly affirm and declare that:-

1. My/our above noted enterprise M/s (name and complete address)_____has been issued Manufacturing Entrepreneurs Memorandum in Haryana by the District Industries Centre_____ under acknowledgement No._____ of dated _____(Self Certified Copy of the same be attached as **Annexure 'A'** with this Affidavit)and has been issued for manufacture of the following items in **category Medium Enterprise** as under:-
    i. _____
    ii. _____
    iii. _____
    iv. _____
2. That my/our above mentioned manufacturing Medium Enterprises meet all the remaining terms & conditions of the tender except Past Performance/Past Experience.
3. That my first work order under this benefit/concession was issued by State Government Department/ State Government Agency (name of Deptt./Agency)_____vide P.O No. _____of dated _____for the supply of _____(name of the item/good/work/services) was successfully complied by above mentioned Enterprises. A self certified copy of the same is attached as **Annexure 'B'** with this affidavit.
4. That in case the work Order of the quoted item is issued to me/us, it will not be outsourced or subcontracted to any other firm, however, the terms and conditions of the RFP in order to meet the Scope of Work shall be the responsibility of us/SI only.
5. That we agree to the condition that this benefit/concession to the Medium Enterprises is valid for one year from the date of getting the first supply order under State public Procurement .
6. That the billing will be done from Haryana

Authorized Signatory (ies)[In full and initials]: _____
Name and Title of Signatory (ies): _____
Name of Bidding Company/Firm: _____
Address: _____ *(Affix the Official Seal of the Bidding Company)*

ANNEXURE 12

(To be submitted on its Letterhead by the bidder)

Authenticity of submitted documents/information

AFFIDAVIT

(To be submitted by bidder on non-judicial stamp paper of Rs. 100/- (Rupees Hundred only to be duly attested by Notary Public)

Subject: e-Tender/Hartron/TDS/DC/2025-26/06

Affidavit of Mr..... S/o ..... R/o ..... I, the deponent above named do hereby solemnly affirm and declare as under:

1. That I am the Proprietor/Authorized signatory of M/s .....

   Having its Head Office/Regd. Office at .....

2. That the information/documents/Experience certificates submitted by M/s..... along with the tender for ..... *(Name of work*) ..... to the Corporation are genuine and true and nothing has been concealed.

3. I shall have no objection in case the Corporation verifies them from issuing authority (ies). I shall also have no objection in providing the original copy of the document(s), in case the Corporation demand so for verification.

4. I hereby confirm that in case, any document, information & / or certificate submitted by me found to be incorrect / false / fabricated, the Corporation at its discretion may disqualify / reject / terminate the bid/contract and also forfeit the EMD / All dues.

5. I shall have no objection in case HARTRON verifies any or all Bank Guarantee(s) under

   any of the clause(s) of Contract including those issued towards EMD and Performance Guarantee from the Zonal Branch /office issuing Bank and I/We shall have no right or claim on my submitted EMD before the Corporation receives said verification.

6. That the Bank Guarantee issued against the EMD issued by (name and address of

   the Bank) is genuine and if found at any stage to be incorrect / false / fabricated, the Corporation shall reject my bid, cancel pre-qualification and debar me from participating in any future tender for three years.

I, ..., the Proprietor / Authorized signatory of M/s..... do hereby confirm that the contents of the above.

Affidavit are true to my knowledge and nothing has been concealed there from..... and that no part of it is false.

Authorized Signatory (ies)[In full and initials]: _____
Name and Title of Signatory (ies): _____
Name of Bidding Company/Firm: _____
Address: _____ *(Affix the Official Seal of the Bidding Company)*

ANNEXURE-13

Affidavit

(On non-judicial stamp paper of Rs. 10/-)

Subject: e-Tender/Hartron/TDS/DC/2025-26/06

I, _____ S/o _____r/o _____ on behalf of the entity _____ do hereby solemnly affirm and declare as under: -

1 That I hereby confirm that my/our firm/company M/s…… have not been convicted of any criminal offence, by any of the courts to the best of our knowledge.

2 That I hereby confirm that my/our firm/company M/s…… have not been convicted, or reasonably suspected of committing or conniving at the commission of any criminal offence under any of the laws applicable in the country.

3 That I hereby confirm and declare that my/our firm/company M/s…… has not been black listed/ de-listed or put on holiday by any Institutional agencies/ Govt. Deptt in the last three years (FY 2022-23, 2023-24, 2024-25)

4 That I hereby confirm and declare that my/our firm/company M/s…… has paid all rents, royalties and all public demands such as income-tax, sales tax, GST and all other taxes and revenues payable to the Government of India or to the Government of any State or to any local authority and that at present there are no default in arrears of such rents, royalties, taxes and revenues due and outstanding and that no attachments or warrants have been served on us in respect of sales-tax, income-tax, GST, Govt. Revenues and other taxes.

5 To the best of our knowledge that in the past five years prior to the date of this application, I or any principal of the entity has not been deemed to be in default on any contract, or have not been forcefully terminated from any contract of any Organization.

6 To the best of our knowledge that I hereby confirm and declare that my/our firm/company M/s…… has not been blacklisted/debarred by any central/state Government department/organization.

7 That I hereby confirm and declare that my/our firm/company M/s…… that there has been no litigation with any Government department/organization on account of similar services to the best of our knowledge.

8 That I hereby confirm and declare that my/our firm/company M/s……has not undergone any legal proceedings of whatever kind in the past 03 years (FY 2022-23, 2023-24, 2024-25) to the best of our knowledge.

I hereby confirm that in case, any document, information & / or certificate submitted by me found to be incorrect / false / fabricated, the Corporation at its discretion may disqualify / reject / terminate the bid/contract and also forfeit the EMD / All dues. May take any appropriate legal action against me. Authorized Signatory (ies)[In full and initials]:

_____

Name and Title of Signatory (ies): _____

Name of Bidding Company/Firm: _____

Address: _____ *(Affix the Official Seal of the Bidding Company)*

Annexure 14
(To be provided on letterhead along with Technical bid)

Compliance regarding restrictions under Rule 144 (xi) of
the General Financial Rules (GFRs), 2017

Dated:-

Managing Director
Haryana State Electronics Development Corporation Limited (HARTRON)
SCO 111-113 Sector 17 B, Chandigarh 160017

Subject: e-Tender/Hartron/TDS/DC/2025-26/06

1. Any bidder from a country which shares a land border with India will be eligible to bid in this tender only if the bidder is registered with the competent authority.
2. "Bidder" (including the term 'tenderer', 'consultant', or 'service provide' in certain contexts) means any person or firm or company, including any member of a consortium or joint venture (that is an association of several persons, or firm or companies), every artificial juridical person not falling in any of the descriptions of bidders stated hereinbefore, including any agency branch or office controlled by such person, participating in a procurement process.
3. "Bidder from a country which shares a land border with India" for the purpose of this order means:-
   i. Any entity incorporated, established or registered in such a country; or
   ii. A subsidiary of an entity incorporated, established or registered in such a country; or
   iii. An entity substantially controlled through entities incorporated, established or registered in such a country; or
   iv. An entity whose beneficial owner is situated in such a county; or
   v. An Indian (or other) agent of such an entity; or
   vi. A natural person who is citizen of such a country; or
   vii. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above
4. The beneficial owner for the purpose of (3) above will be as under:
   a. In case of a company or Limited Liability Partnership, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.

      Explanation –

      i. "Controlling ownership interest" means ownership of or entitlement to more than twenty-five per cent. Of shares or capital or profits of the company;

      ii. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;

   b. In case of a partnership firm, the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership of entitlement to more than fifteen percent of capital or profits of the partnership;

   c. In case of an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals;

d. Where no natural person is identified under (1) or (2) or (3) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

e. In case of trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

5. An agent is a person employed to do any act for another, or to represent another in dealing with third person.

6. The successful bidder shall not be allowed to sub-contract works to any contractor from a country which shares a land border with India unless such contractor is registered with the Competent Authority.

   i. Model Certificate for Tenders: -

   "I have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India; I certify that we or our company/firm is not from such a country or, if from such a country, has been registered with the Competent Authority. I hereby certify that we or our company/firm fulfills all requirements in this regard and is eligible to be considered. (Evidence of valid registration by the Competent Authority shall be attached.)"

   ii. Tenders for Works involving possibility of sub-contracting:

   "I have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India and on sub-contracting to contractors from such countries; I certify that we or our company/firm is not from such a country or, if from such a country, has been registered with the Competent Authority and will not sub-contract any work to a contractor from such a countries unless such contractor is registered with the Competent Authority. I hereby certify that we or our company/firm fulfills all requirements in this regard and is eligible to be considered. (Evidence of valid registration by the Competent Authority shall be attached.)"

Authorized Signatory (ies)[In full and initials]: _____
Name and Title of Signatory (ies): _____
Name of Bidding Company/Firm: _____
Address: _____ *(Affix the Official Seal of the Bidding Company)*

ANNEXURE 15

UNDERTAKING FOR CHOICE OF PAYMENT OPTION

Dated:-

Managing Director
Haryana State Electronics Development Corporation Limited (HARTRON)
SCO 111-113 Sector 17 B, Chandigarh 160017

Subject: e-Tender/Hartron/TDS/DC/2025-26/06

We, M/s ----------, do hereby confirm that we have read and understood the payment terms options set out in this tender documents under **section "Payment Schedule".**

We hereby undertake that:

We have carefully considered the payment Schedule mentioned under clause "Payment Schedule" if order awarded to us:

We hereby declare that we fully understand and agree to the above undertaking.

Authorized Signatory (ies)[In full and initials]: _____
Name and Title of Signatory (ies): _____
Name of Bidding Company/Firm: _____
Address: _____ *(Affix the Official Seal of the Bidding Company)*

ANNEXURE 16
(To be enclosed with Technical bid)

Dated: _____

Managing Director
Haryana State Electronics Development Corporation Limited (HARTRON)
SCO 111-113 Sector 17 B, Chandigarh 160017

Subject: e-Tender/Hartron/TDS/DC/2025-26/06

I/We M/S---------- having registered office at (Address of the registered office) and local office at (Address of the local office), hereby declare and confirm that the specifications of the items offered match/exceed the ones quantified as minimum requirements in the Tender document..

I/ We, M/S---------- further undertake that following equipment to be supplied by us is considered to be of different OEMs.

#	Component	OEM Brand	Understanding of which OEM Brands not to be against respective components	Compliance Yes/No
1	Perimeter Firewall	B	C	
2	Internal Firewall	C	B,D	
3	Web Application Firewall (WAF)	D	B,C	

Authorized Signatory (ies)[In full and initials]: _____
Name and Title of Signatory (ies): _____
Name of Bidding Company/Firm: _____
Address: _____ *(Affix the Official Seal of the Company)*

ANNEXURE 17
(Scope of existing MSI)

GOALS OF COMMON IT INFRASTRUCTURE CONSOLIDATION

As part of the proposed scope of work, RailTel (MSP) has to perform consolidation of IT Infrastructure and its management at SDC. The overall goals for the effort are to:

- Align the common IT Infrastructure (SDC) of the state with the business needs and priorities.
- Move from hosting / co-location model to Cloud model i.e. Infrastructure As a Service (laaS), Platform As a service (PaaS) and Software As a Service (SaaS)
- Standardize IT services/resources and create operational efficiencies
- Ensure that the digital IT assets of the state are secure.
- The financials will be based on the services being managed under common IT Infrastructure.
- The e-Governance program is under IT Act 2000.

1.2 SCOPE OF COMMON IT INFRASTRUCTURE CONSOLIDATION

The following IT infrastructure services shall be consolidated at the state level:

- Single Helpdesk Service for the IT Infrastructure in place of separate helpdesk for SWAN and SDC. Calls will be received by the help desk and based on the issue the ticket/work will be assigned to the SDC or SWAN team. Currently, there is a single help desk for SWAN and SDC.
- Consolidation of IT infrastructure management tools: A separate agency is being engaged which will provide the tools and licenses for infrastructure management. However architecting the solution and getting it implemented through the agency and smooth implementation/transition shall be the responsibility of MSP i.e. RailTel in coordination with all stakeholders. Currently, each component such as HSWAN and HSDC is monitored separately. With consolidation monitoring the business level services are envisaged to be introduced. The monitoring and management tools shall be architected and configured in a way that end to end service delivery can be monitored. Views to the departments for their respective services and components shall be provided as a service. RailTel will act as a stakeholder and will be jointly responsible for making the blueprint for customization of upcoming and NMS/EMS.

- The focus is now to transition from ownership to pay as use model. As a first step, the infrastructure as part of co-hosting shall be brought under cloud management and leverage the Cloud infrastructure to provide self-provisioning Virtual machines (VMs). Subsequently effort shall be made to also bring in the co-located infrastructure under cloud management. A roadmap for the same needs to be proposed as part of Technical proposal.
- The server rooms for SDC and SWAN are separate. As part of consolidation these two server rooms shall be integrated and utilized as Server rooms for placing equipment related with SWAN and SDC. SDC and SWAN are co-located on the same floor in the same building. No civil work is required to integrate them. Managing reconfiguration of the existing infrastructure/ equipment is the responsibility of RailTel if the integration happens at the logical level.
- Consolidation of Internet Traffic for SWAN and SDC shall be achieved. This may require changes in the current routing of Internet traffic. Currently, SDC uses NKN and HFCL for Internet traffic. IN SWAN very limited Internet traffic flows. As part of consolidation the Internet traffic is required to follow the same incoming and outgoing path for SWAN and SDC. It is about integration of internet access over SDC and SWAN. No additional hardware is expected from RailTel. In case of any failure in links/ connectivity, RailTel will follow up with respective ISPs for resolving the issues.
- Separate physical and logical Access Management Systems for SWAN and SDC are used at present. A mechanism to manage an access control is required to be implemented. Presently, two separate access control mechanisms are in place for SDC and SWAN. RailTel will take responsibility to facilitate them as a single owner.
  Consolidation of management of VPN services**:** Currently, VPN is part of SWAN and provided to departments for accessing their servers in SDC. Once consolidated the VPN shall function as an integrated access for SWAN and SDC. Single policy implementation for VPN across the network is to be brought in. The departments shall be putting up single requests for VPN access to their servers and end to end access to be provided. Managing end to end VPN services will be the responsibility of MSP.

- Consolidation of Security management: Security is currently viewed as separate pieces for SWAN and SDC. Integrated security view is required to be brought in.

End to end security management shall be the focus as part of consolidation and it will be the responsibility of RailTel.

- Setting of the Common Portal for IT Infrastructure management. Monitoring of common IT Infrastructure managed by third party will be the responsibility of RailTel.
- The MSP shall propose any other consolidation areas for service improvement, and would provide any necessary technical assistance, if required.

1.3 MANAGED SERVICES

CIM.001	Shall provide Level 1 support to departments using Common IT Infrastructure services which shall include SWAN and SDC as a minimum. The primary goal of Level 1 support is to provide a single point of contact for Departments.
CIM.002	Shall ensure that the support engineers have excellent inter – personal skills, technical skills and business awareness to ensure that service reflects and encourages high standards. The help desk function can be classified as the primary team performing Incident Management.
CIM.003	Shall provide Level 1 support services through: • Setting up common Help Desk for Departments and defining the process. • Managing the Level 1 / Help desk • Staffing the Help desk with people with the right skill-sets • Providing reports on service levels
CIM.004	The Help Desk services shall • Be 24x7x365 days • Be provided through a Toll free/ Landline number. • Log all events or disruption of services with a ticket/docket number which will be informed to the caller / requester • The requests marked as closed shall be reopened by the requester within 24 hours of closing if the closure is not satisfactory. • Follow the guidelines as per the ITIL frame-work • Have a periodic feedback survey through a mail or recorded over voice on random sampled basis. • Provide Proactive and reactive monitoring and support. The Proactive

	monitoring will include L1 and L2 support which will be from the NOC (24x7) and L3 will be the re-active support and will be provided during the normal business hours and on call basis for 24x7 support.
CIM.005	Provide necessary channels for reporting issues to the help desk. The incident reporting channels shall be following: • Specific Email account • A help desk non-human mail id will be used to log issues with the help desk. This mail id will be published and will be manned 24/7 • Create a Help desk portal which will be available to submit requests. This will be based on the tool used by the incident management system • Implement a call logging system in line with the severity levels as per the SLAs. • The Help desk shall log user calls related to Common IT infrastructure and assign an incident / call ID number. Severity shall be assigned to each call as per the SLAs. • Track each incident / call to resolution. This will be the responsibility of RailTel to take all calls to resolution as per the SLA.
CIM.006	Shall provide an escalation matrix for the calls. The escalation matrix shall be available to all stakeholders. The escalation matrix will be part of SLA monitoring.
CIM.007	Shall Coordinate with respective vendors for closure of calls. The L1 team will engage with the vendors for any hardware level dependencies and will coordinate with the vendor to report or log calls with the vendor for vendor dependent support. Take appointment for part replacement and accompany the vendor representative to the SDC for hardware replacement as per the appointment The MSP shall maintain • Compliance to the SLA • Corrective action taken for the breaches. • RCA for high priority incidents including corrective actions taken. • Knowledge base on frequently asked questions to assist user departments in resolving basic issues themselves.

CIM.008	Shall provide System Monitoring and Administration for the Servers installed as part of IT infrastructure management services, co-hosting and Departmental servers. Under this service the MSP shall take care of the server`s operating system under the Windows & Linux environment.
CIM.009	The Monitoring and Administration services shall include the following as minimum: • Installation and configuration of servers as per the requirement • Performance monitoring of servers including but not limited to monitoring CPU, disk Service provider ace, memory utilization, I/O utilization, etc. • Hardening of the operating system • Patch management of the operating system as per defined procedure • Upgrades • Responding to alerts and / or tickets that are either auto-generated or user raised • Resolving the issue based on Incident and Problem Management procedure • Provide support, advice and guidance to corresponding stakeholder on server related issues • Analyse root cause of problems and minimize the adverse impact of these issues • RailTel will be responsible to manage the user names, roles and passwords for all the systems, including, but not limited to servers, applications, devices etc.
CIM.010	Ensuring the upkeep of existing systems that would be reused and also Incorporate necessary changes for new applications if any during the tenure of the contract.
CIM.011	Shall provide Database Administration service to Departments. The database team shall provide pro-active support of database systems across all platforms to ensure a stable and efficient data processing environment for the departments.
CIM.012	The Database Administration service shall include the following as minimum but not limited to :

	• Installation and configuration of Databases. • End-to-end management of database on an ongoing basis to ensure smooth functioning of the same; • Management of changes to database schema, disk Service Provide race, storage, user roles; • Conduct code and configuration reviews to provide tuning inputs to the State / User Department in order to improve the application performance or resolve bottlenecks if any; • Management of database upgrade or patch upgrade as and when required with. • Minimal downtime. • Maintain reliable database backups • Provide timely response to critical requests through 24/7 on-call support • Provide response to non-critical requests on working hours • Establish data security by reviewing current security levels every 6 months & modifying if necessary. • Maintain data security procedures • Engage in regular performance management of databases, application and files/tables
CIM.013	Shall install upgrades and perform preventative maintenance to all databases.
CIM.014	Shall provide Storage Support Services. It shall allow the departments to offload storage management tasks to MSP. This shall be aimed at helping the departments in improving data availability, productivity and security.
CIM.015	The storage support services shall ensure that the government retains full control of their storage environment with freeing up from time consuming storage administration.
CIM.016	A typical list of storage support services that shall be undertaken by MSP as a minimum are as follows: • Installation and support of the storage system • Configuration of storage and creation of Storage Units keeping in mind the performance requirement for the application.

	• Develop, improve and maintain the storage management policy, configuration and management of disk array, SAN fabric/switches, NAS, tape library, etc. • Management of storage Service Provider ace, volume RAID configuration, LUN, Zone, security, business continuity volume, NA, performance etc. • Handling/facilitating service requests for storage • Scheduled and ad hoc storage level back ups • Monitoring of backups and restart of failed backups.
CIM.017	Shall provide L1 level System Monitoring and Administration for the Web Server and /or Application server (Apache, IIS, JBOSS etc.).Under this service the MSP shall take care of the system under the Windows &/or Linux environment. Details of the databases, size and platforms are enclosed.
CIM.018	The Monitoring and Administration services shall include the following as minimum: ▪ Installation and configuration of Apache and/or application servers as per Departmental requirement ▪ Performance monitoring of Apache and /or application ▪ Implementation of security guidelines ▪ Hardening of Web server/ application server ▪ Patch management as per defined procedure ▪ Responding to alerts and /or tickets that are either auto-generated or user raised ▪ Resolving the issue based on Incident and Problem Management procedure ▪ Provide support, advice and guidance to Departments on web server/Application server related issues ▪ Analyze root cause of problems and minimize the adverse impact of these issues.
CIM.019	The MSP shall also provide backup and restore services The activities shall include: • Backup of operating system, database and application as per stipulated

	policies. • Monitoring and enhancement of the performance of scheduled backups, schedule regular testing of backups, schedule regular testing of backups and ensure adherence to related retention policies • Ensuring prompt execution of on-demand backups of volumes, files and database applications whenever required by user departments or in case of upgrades and configuration changes to the system. • Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes. • Media management including, but not limited to tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets. • Physical security of the media stored in cabinets. • On-going support for file and volume restoration requests at the SDC.
CIM.020	MSP shall pro-actively work to identify the possible risks in Common It Infra Management and work to mitigate the risks of the hosted, co-located and connectivity environment and have a contingency plan in place for the identified risks. Will maintain a risk register and keep it updated. Review the risks with the MSP / stakeholders to make them aware.
CIM.021	MSP shall define, implement and maintain standard operating procedures for maintenance of the infrastructure based on the policies of the state
CIM.022	MSP shall provide Domain name server (DNS) service. The DNS shall be for SWAN and Internet. In other words Split DNS. Currently, there is no split DNS configured in SWAN/SDC.

1.4 BASIC INFRASTRUCTURE SERVICES

Following services are provided by the Service Provider under the basic infrastructure services:

BIS.001	Ensure availability of the SDC infrastructures (both IT and non IT) including Power, Cooling CCTV, Access Control, Racks, Network Devices, Firewall, Storage and other peripheral equipment installed inside the SDC and the SWAN
BIS.002	Provide and maintain testing/staging infrastructure for testing the application

	before hosting on the racks and space management on racks inside SDC
BIS.003	Facilitate hosting of departmental application infrastructure at the SDC
BIS.004	Provide and maintain internet connectivity and ensure connectivity with SWAN and SDC
BIS.005	• SDC and NOC are secured areas. Access permission is given only to authorized personnel of RailTel. • The Access management will be the responsibility of RailTel towards the SDC and will be done as per the approved process decided by the stakeholders.
BIS. 006	Provide existing access card activation service for access to the SDC and SNMC. Access permissions will be maintained by the service provider in terms of rights additions, deletions and modifications. The access control list will be kept updated as per the ISO 27001 control requirements. The access approval process will have to be followed for enabling/disabling access. The process will be provided to RailTel.
BIS. 007	Provide locked server cabinets for storage, with IP-based CCTV surveillance and biometric access to all areas.
BIS. 008	Proactive and reactive maintenance, repair and replacement of defective components and replacement of defective components (physical and other peripheral IT infrastructure) installed at the Data Center will be the responsibility of RailTel. The cost for repair and replacement shall be borne by the Department/ CRID. However RailTel will need to inform the stakeholders about such changes/ requirements/ expiry of Annual Maintenance Contract with sufficient notice so that the procedural delays to fulfil such requirements are minimized as much as possible from the supplier/ vendor side.
BIS. 009	Asset management system will be maintained by the service provider with necessary labelling on the assets.
BIS. 010	• To maintain the critical services the service provider will keep standby equipment at strategic locations. • Any such requirements will need to be discussed and agreed with RailTel/ stakeholders

	• Before the start of the contract all necessary equipment will be ordered and arranged in accordance with the above agreements. • The asset management system will be maintained in line with the requirements of the standards such as ISO 27001. • The service provider will work with RailTel/ stakeholders to make the services in scope compliant to the standards such as ISO 27001 and will participate in the internal and external audits. • The assets as per the asset management system are audited at the physical and logical levels. There is a yearly exercise to track the physical IT and not IT assets to ensure that the asset management system is kept up to date. • Define a procedure for identifying the end of life of both IT and Non IT equipment. • License management will be a part of Asset management system and will be a responsibility of the service provider. All licenses procured will be in the name of Haryana State Government. • RailTel will participate in the transition activities (HOTO) while taking over and at the time of contract and handing over at the time of ending of the contract to the party who is going to be the next service provider and MSP/ Stakeholders in a seamless manner. Any gaps at the time of taking over of services from the present service provider will be identified, listed and agreed by all the parties (existing service Provider, incumbent service provider and MSP, Stakeholder).
BIS. 011	Monitoring & Management Services The activities will include the entire IT and Non IT assets and documentation. The scope of the services will cover IT, Non IT infrastructure management for the period of contract and will include Monitoring, Administration and Management of the entire SDC infrastructure. All passive and active devices will be covered. The entire stack of monitoring and management services will include the following: i. Help Desk Services ii. Server Monitoring, Administration & Management Services

	iii. Database Administration & Management Services iv. Storage Administration & Management Services v. Backup & Restore Services vi. Security Administration Services vii. Performance tuning
BIS. 012	Event log analysis generated in all the sub systems including but not limited to Servers, operating systems, database, applications, and security devices, Messaging etc. ensuring that the logs are backed up and regularly maintained.
BIS. 013	Any component (physical & IT installed at the time of SDC commissioning) that is reported to be faulty/ non-functional on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame agreed upon in Service Level Agreement (SLA). This will follow the ITIL framework. The service provider will maintain all the items in the configuration management database.
BIS.014	Proactive monitoring of the entire basic infrastructure installed at the SNMC, SDC and all location covered in HSWAN through building management software
BIS.015	RailTel will maintain records of the maintenance of the basic infrastructure and will maintain a logbook on –site that may be inspected by the State at any time. RailTel will need to have emergency repair teams from the existing staff managing the SDC, SWAN, NOC and all the network connected sites in the geography across HARYANA state.
BIS. 016	Temperature to be maintained 20°±2° at all times. Any violation in temperature shall be raised as a critical event in the incident management system. Relevant tickets shall be automatically logged.
BIS.017	Existing CCTV System availability is the responsibility of RailTel. Any sudden changes in temperature in SDC and SWAN areas shall be raised as critical events in the incident management system. Relevant tickets shall be automatically logged.
BIS.018	DVR system availability. Any violation in temperature shall be raised as a critical event in the incident management system. Relevant tickets shall be

	automatically logged.
BIS.019	CCTV recording -6 months from the time of recording. Any violation in temperature shall be raised as a critical event in the incident management system. Relevant tickets shall be automatically logged.
BIS.020	Event log analysis generated in all the sub systems including but not limited to servers, operating systems, databases, applications, and security devices, Messaging etc. ensuring that the logs are backed up and regularly maintained.

1.5 SECURITY ADMINISTRATION SERVICES

	The activities to be carried out under security administration shall include:
SAS.00	Addressing the ongoing needs of security management including, but not limited to, monitoring of various devices/ tools such as firewall, intrusion detection, Content filtering and blocking, virus protection, and vulnerability protection through implementation of proper patches and rules.
SAS.01	Root domain administration by creating the root and sub-domains and setting the root level security policies such as authentication mechanisms (single/multi factor), password policies such as password length, password complexity, password expiry, account lockout policy, certificate policies, IPSEC policies etc.
SAS.02	Maintaining an updated knowledge base of all the published security vulnerabilities and virus threats for related software and microcode etc.
SAS.03	Ensuring that patches/ workarounds for identified vulnerabilities are patched /blocked immediately.
SAS.04	Respond to security breaches or other security incidents and coordinate with respective OEM in case of a new threat is observed to ensure that workaround /patch is made available for the same
SAS.05	Provide a well-designed access management system, security of physical and digital assets, data and network security, backup and recovery etc. Maintenance and management of security devices, including but not limited to maintaining firewall services to restrict network protocols and traffic,

	detecting intrusions or unauthorized access networks, systems, services, applications or data, protecting email gateways, firewalls, servers, from viruses.
SAS.06	Ensuring that the security policy is maintained and updates to the same are made regularly as per ISO 27001 and BS 20000 guidelines.

1.6 NETWORK MONITORING SERVICES

NMS.00	RailTel will provide services for management of network environment to maintain performance at optimum levels on a 24×7 basis
NMS.01	RailTel will monitor and administer the network within the SDC up to the integration points with SWAN and Internet.
NMS.02	RailTel will create and modify VLAN, assignment of ports to appropriate application and segmentation of traffic.
NMS.03	RailTel will carry out break fix maintenance of the LAN cabling or maintenance work requiring civil work.

1.7 VENDOR MANAGEMENT SERVICES

VMS.00	RailTel will coordinate and follow-up with all the relevant vendors of the State User Department to ensure that the user problems and issues are resolved in accordance with the SLAs agreed upon with them.
VMS.01	RailTel will also ensure that unresolved issues are escalated to respective user departments in accordance with the escalation matrix.
VMS.03	RailTel will maintain a database of the various vendors with details like contact person, telephone nos., escalation matrix, response time and resolution time commitments etc.
VMS.04	RailTel will draw a consolidated quarterly SLA performance report across vendors for consideration of the user departments. Any issues being faced

	with the vendors must be discussed with the stakeholders.

1.8 INSTALLATION & CONFIGURATION OF APPLICATION INFRASTRUCTURE

ICAI.00	RailTel will provide installation and configuration support for the application infrastructure to be hosted by the respective user departments. This service shall be availed by departments based on their specific requirements. It shall not include application deployment, tuning or any other application related work. RailTel activities will include
ICAI.01	RailTel will undertake pre-installation planning at the State Data Centre including but not limited to Rack planning, structured cabling, SAN cabling, power points
ICAI.02	RailTel will be responsible for the commissioning of the storage, network & security components and related basic infrastructure at the SDC
ICAI.03	RailTel will manage the placement of equipment inside the SDC for optimal space utilization. The plan and layout design should be developed in a manner So as to optimally and efficiently use the resources and facilities being provisioned at the SDC.
ICAI.04	The plan and design documents thus developed shall be submitted to the user departments for approval and the acceptance would be obtained prior to Commencement of installation.

1.9 SOFTWARE LICENSE MANAGEMENT

SLM.00	Software License Management will be the responsibility of RailTel. RailTel will track software usage throughout the IT setup so as to effectively
SLM.01	Manage the risk of unauthorized usage or under licensing of software installed at the SDC. This may be carried out through the use of standard license management tools.
SLM.02	RailTel will do the lifecycle management of the licenses including raising of procurement request, after purchase allocation, de-allocation, license renewal, license pool management.

SLM.03	This will be applicable for the licenses used in the complete environment for the Haryana Government. All licenses will be procured in the name of Haryana state.

1.10 MIS REPORTS

	RailTel will submit the reports on a regular basis in a mutually decided format. The following is only an indicative list of MIS reports that may be submitted to the State. These reports will also be made available online.
MIS.00	**Daily dashboard reporting** • Summary of issues / complaints logged at the Help Desk • Summary of resolved, unresolved and escalated issues / complaints • Summary of resolved, unresolved and escalated issues/complaints to the vendors. • Log of backup and restoration undertaken.
MIS.01	**Weekly dashboard reporting** • Issues / Complaints Analysis report for virus calls, call trend, call history, etc. • Summary of systems rebooted. • Summary of issues / complaints lodged with the OEMs. Inventory of Service Provider are parts in SDC including • 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.
MIS.02	**Monthly dashboards reporting** • Component wise physical as well as IT infra-structure availability and resource utilization. • Consolidated SLA/ non-conformance report. • Summary of component wise Data Centre uptime. Summary of changes in the Data Centre. • Log of preventive / scheduled maintenance undertaken Log of break-fix maintenance undertaken

	• Business continuity risks and mitigation and contingency plans

1.11 ADVANCED DATA CENTER SERVICES

ADCS.00	Advanced Data Center Services shall mean, application related services which RailTel may provide to the user departments only upon mutual consent. The objective of application related services is to facilitate the user departments by providing them with "One Stop Shop" for all their requirements. This set of services shall include application migration, application enhancement, application maintenance, operational support and any other assistance regarding the application to be provided by RailTel to the user department. These services shall be mutually agreed upon amongst RailTel and the user department.
ADCS.01	Based on the above three types of the requirements from the departments, the scope of work for the Operations Phase has to be categorized under 2 three service categories as depicted in the figure below. Basic Infrastructure Services are mandatory services to be provided by the MSP to ensure seamless SDC operations. Apart from Basic Infrastructure Services, some departments would opt for hosting services while some departments even opt for advanced services for database / application management as per their specific requirements.
ADCS.02	Production Servers, Development and Test Servers.
ADCS.03	High Availability Architecture for Servers, Databases, Network devices.
ADCS.04	Backup Strategy will be provided, Backup tapes are stored in the same location where SDC is located.
ADCS.05	The respective departments will be responsible for the applications hosted in the Data Center. However, initial level diagnosis, hardware, software will be the responsibility of RailTel.

APPENDIX 1

REQUEST FOR CLARIFICATION

Bidders requiring specific points of clarification may communicate with the Hartron through email during the specified period using the following format.

Date: _____
To
Managing Director
Haryana State Electronics Development Corporation Limited (HARTRON)
SCO 111-113 Sector 17 B, Chandigarh 160017

Subject: e-Tender/Hartron/TDS/DC/2025-26/06

BIDDER'S REQUEST FOR CLARIFICATION			
<<Name of Bidder submitting query / request for clarification>>			
<<Full formal address of the Bidder>>			*Tel:*
			Fax:
			Email:
S. No	RFP Reference (Section No. / Page No.)	Content of RFP requiring clarification	Points of clarification required
1			
2			
3			
4			
5			
6			

Authorized Signatory (ies) [In full and initials]: _____
Name and Title of Signatory (ies): _____
Name of Bidding Company/Firm: _____
Address: _____ *(Affix the Official Seal of the Company)*

APPENDIX 2:

FORMAT FOR PERFORMANCE BANK GUARANTEE

Performance Bank Guarantee

Ref: _____ Date: _____

Bank Guarantee No.: _____

To
Director (Administration),
Citizen Resources Information Department,
Room no-42, 9th floor, Haryana Civil Secretariat, Sector-1, Chandigarh-160001

Dear Sir,

PERFORMANCE BANK GUARANTEE – for Selection of System Integrator for Supply, Design, Installation, Commissioning with O&M of IT components for Haryana State Data

WHEREAS

M/s. (name of Bidder), a company registered under the Companies Act, 1956, having its registered and corporate office at *(address of the Bidder)*, (hereinafter referred to as "our constituent", which expression, unless excluded or repugnant to the context or meaning thereof, includes its successors and assigns), agreed to enter into a Contract dated …….. (herein after, referred to as "Contract") with you for order of Supply, Commissioning and Maintenance of ----------, in the said Contract.

We are aware of the fact that as per the terms of the Contract, *M/s. (name of Bidder)* is required to furnish an unconditional and irrevocable Bank Guarantee (for orders valuing more than 3 lac.) in your favor for an amount of 10% of the Total Contract Value, and guarantee the due performance by our constituent as per the Contract and do hereby agree and undertake to pay any and all amount due and payable under this bank guarantee, as security against breach/ default of the said Contract by our Constituent.

In consideration of the fact that our constituent is our valued customer and the fact that he has entered into the said Contract with you, we, *(name and address of the bank)*, have agreed to issue this Performance Bank Guarantee.

Therefore, we *(name and address of the bank)* hereby unconditionally and irrevocably guarantee you as under:

In the event of our constituent committing any breach / default of the said Contract, and which has not been rectified by him, we hereby agree to pay you forthwith on demand such sum/s not exceeding the sum of ___% of the Total Contract Value i.e.,……..<in words> without any demur.

Notwithstanding anything to the contrary, as contained in the said Contract, we agree that your decision as to whether our constituent has made any such default(s) / breach(es), as aforesaid and the amount or amounts to which you are entitled by reasons thereof, subject to the terms and conditions of the said Contract, will be binding on us and we shall not be entitled to ask you to establish your claim or claims under this Performance Bank Guarantee, but will pay the same forthwith on your demand without any protest or demur.

This Performance Bank Guarantee shall be valid for _____ months, subject to the terms and conditions of the Contract. Any claim against the Bank Guarantee can however be made within ____ months from the date of submission of the same. We bind ourselves to pay the above said amount at any point of time commencing from the date of submission of Bank Guarantee, until ____ months.

We further agree that the termination of the said Agreement, for reasons solely attributable to our constituent, virtually empowers you to demand for the payment of the above said amount under this guarantee and we would honor the same without demur.

We hereby expressly waive all our rights:

i. Requiring to pursue legal remedies against the Department; and

ii. For notice of acceptance hereof any action taken or omitted in reliance hereon, of any defaults under the Contract and any resentment, demand, protest or any notice of any kind.

We the Guarantor, as primary obligor and not merely Surety or Guarantor of collection, do hereby irrevocably and unconditionally give our guarantee and undertake to pay any amount you may claim (by one or more claims) up to but not exceeding the amount mentioned aforesaid during the period from and including the date of issue of this guarantee through the period.

We specifically confirm that no proof of any amount due to you under the Contract is required to be provided to us in connection with any demand by you for payment under this guarantee other than your written demand.

Any notice by way of demand or otherwise hereunder may be sent by special courier, telex, fax, registered post or other electronic media to our address, as aforesaid and if sent by post, it shall be deemed to have been given to us after the expiry of 48 hours when the same has been posted.

If it is necessary to extend this guarantee on account of any reason whatsoever, we undertake to extend the period of this guarantee on the request of our constituent under intimation to you.

This Performance Bank Guarantee shall not be affected by any change in the constitution of our constituent nor shall it be affected by any change in our constitution or by any amalgamation or absorption thereof or therewith or reconstruction or winding up, but will ensure to the benefit of you and be available to and be enforceable by you during the period from and including the date of issue of this guarantee through the period.

Notwithstanding anything contained hereinabove, our liability under this Performance Guarantee is restricted to 10% of the Contract Value, and shall continue to exist, subject to the terms and conditions contained herein, unless a written claim is lodged on us on or before the aforesaid date of expiry of the claim period.

We hereby confirm that we have the power/s to issue this Guarantee in your favor under the Memorandum and Articles of Association / Constitution of our bank and the undersigned is / are the recipient of authority by express delegation of power/s and has / have full power/s to execute this guarantee under the Power of Attorney issued by the bank in your favor.

We further agree that the exercise of any of your rights against our constituent to enforce or forbear to enforce or any other indulgence or facility, extended to our constituent to carry out the contractual obligations as per the said Contract, would not release our liability under this guarantee and that your right against us shall remain in full force and effect, notwithstanding any arrangement that may be entered into between you and our constituent, during the entire currency of this guarantee.

Notwithstanding anything contained herein:

This Performance Bank Guarantee shall be valid for _____ months from the date of submission of Bank Guarantee.

We are liable to pay the guaranteed amount or part thereof under this Performance Bank Guarantee only and only if we receive a written claim or demand on or before ____ (__in words_____) months from the submission of Bank Guarantee.

Any payment made hereunder shall be free and clear of and without deduction for or on account of taxes, levies, imports, charges, duties, fees, deductions or withholding of any nature imposts.

This Performance Bank Guarantee must be returned to the bank upon its expiry. If the bank does not receive the Performance Bank Guarantee within the above-mentioned period, subject to the terms and conditions contained herein, it shall be deemed to be automatically cancelled.

This guarantee shall be governed by and construed in accordance with the Indian Laws and we hereby submit to the exclusive jurisdiction of courts of Justice in India for the purpose of any suit or action or other proceedings arising out of this guarantee or the subject matter hereof brought by you may not be enforced in or by such count.

Dated …….. this ……. day …….. 2023.

Yours faithfully,

For and on behalf of the …… Bank,
(Signature)
Designation
(Address of the Bank)

Note:

This guarantee will attract stamp duty as a security bond.

A duly certified copy of the requisite authority conferred on the official/s to execute the guarantee on behalf of the bank should be annexed to this guarantee for verification and retention thereof as documentary evidence in the matter.

APPENDIX 3:

FORMAT FOR EMD BANK GUARANTEE

Beneficiary:

To

Director (Administration),
Citizen Resources Information Department,
Room no-42, 9th floor, Haryana Civil Secretariat, Sector-1, Chandigarh-160001

(hereinafter referred to as Beneficiary / Government)

BANK GUARANTEE FOR: ----------

Date: ..... [Insert date of issue of BG] (To be insert by issuing bank) …….

BANK GUARANTEE No.: … [Insert guarantee number] … (To be insert by issuing bank) .....

BANK GUARANTEE Amount: ----------

e-Tender No.: - ----------

Applicant / Bidder:----------

Guarantor: …. [Insert name and address of the issuing Bank] ….(To be insert by issuing bank)...

Whereas Applicant / Bidder is willing to submit its bid against above referred e-Tender of the Beneficiary on behalf Director (Administration), Citizen Resources Information Department, Room no-42, 9th floor, Haryana Civil Secretariat, Sector-1, Chandigarh-160001 for the supply of Goods and / or Services and as per tender conditions, Applicant is required to submit a Bank Guarantee as EMD.

At the request of the Applicant, we as Guarantor, hereby irrevocably undertake to pay the Beneficiary any sum or sums not exceeding in total an amount of ---------- (--- in words---).

1. **If the Bidder withdraws or amends, impairs or derogates from the bid in any respect within the period of validity of this bid.**
2. **If the Bidder having been notified of the acceptance of his bid by the Purchaser during the period of its validity.**
3. **If the Bidder fails to furnish the Performance Security for the due performance of the contract.**
4. **Fails or refuses to execute the contract.**
5. **Fails to fulfil any other terms & conditions specified in the tender document.**

We undertake to pay the Beneficiary up to the above amount upon receipt of its first written demand, without the Beneficiary having to substantiate its demand, provided that in its demand

the Beneficiary will note that the amount claimed by it is due to it owing to the occurrence of any conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to and including --------- months after the period of bid validity up to ---------- (----------in words----------) and any demand in respect thereof should reach the Bank not later than the above date.

Dated .....
For.....
(Indicate the nameofthe Bank)
Signature.....
Nameofthe Officer.....
Designation ofthe officer .....
Code no .....
Nameofthe Bankand Branch.....

APPENDIX 4

Make India preference exemption Order

Haryana Government
Citizen Resources Information Department

हरियाणा सरकार
नागरिक संसाधन सूचना विभाग

Order
No. Admn/2/300/12946
Dated 06.06.2023

Pursuant to the recommendations of the Core Technical Committee constituted to finalize the RFP "Selection of System Integrator for Supply, Design, Build, Installation, Commissioning with Operations and Maintenance of a State Data Center along with Near Line BCP Disaster Recovery & Far Disaster Recovery site for 5 years", the committee in their RFP is seeking exemption from Public Procurement (Preference to Make in India) Clause for procurement items as per "Annexure A" of the order. This RFP and its clauses have been approved by following the due procedure of the Government.

The exemption referred to in the above-cited subject was requested by the Core Technical Committee constituted for procurement of ICT Hardware and Software for "Technology refresh" of HSDC through "Selection of System Integrator for Supply, Design, Build, Installation, Commissioning with Operations and Maintenance of a State Data Center along with Near Line BCP Disaster Recovery & Far Disaster Recovery site for 5 years" along with their justification for exemption which is mentioned hereunder as follows:

1. Following are the very critical and important design principals for any Data Centre and Disaster recovery centre for mission critical applications such as State Data Centres, Banking, Hospital Management, Defence, Law enforcement etc for Compute infrastructure, Storage infrastructure, Backup & replication and security between DC and DR and Connectivity purposes.

   i. Scalability
   ii. Security
   iii. Remote & Enterprise management
   iv. Performance
   v. Proactive Monitoring and Predictive Analytics

2. It is further to mention that success of such huge projects not only depend on the credentials of System Integrator, but on the quality, features, manageability and performance of infrastructure supplied for the project. Following points shall contribute to the success or failure of the project which are required to be considered:
   i. High-end compute like Servers are required for hosting Citizen centric critical application and services to the citizens. All such services would be rendered on 24x7 basis. So the equipment under this category shall be used for application testing, staging, and production and shall operate on 24x7x365 basis. As the same is being operated 24X7 the feature of remote enterprise management of the infrastructure is required which come with the firmware of the infrastructure.
   ii. Features like firmware management, security features, Protection from Cyber-attacks, management of infra in an elastic environment where the resources can be remotely increased or decreased based on requirement.

9th Floor, Haryana Civil Secretariat, Sector - 1, Chandigarh. 160001
Tel: PS (CRID): 0172-2740441, Email: psit@hry.gov.in, Director (Admn.): 0172-2748142,
Head SeMT & CITO: 0172-2703479, 0712-2708285, Email: cito.ditech-hry@nic.in
Website: www.haryanait.gov.in

iii. The infrastructure needs to be continuously updated/ upgraded based on the new releases considering the worldwide threat landscape and best practices. New OEMs lack this capacity & features and hence, are more vulnerable to new threats. Further, new OEMs lack must have features like maintaining repository for firmware with drivers and features to install or rollback compromised firmware with provisions even to restore to Factory settings.

iv. Out of the box features like support for managing multiple servers under a single console a one unit may not be available in new and emerging OEMs whether of Indian origin or not. Important features for SDC environment are listed as under which are very important in terms of energy efficient O&M of the infrastructure:
   a) Group Power Control
   b) Group Power Capping
   c) Group Firmware Update
   d) Group Configuration
   e) Group Virtual Media and Encrypted Virtual Media
   f) Group License Activation

v. Also, the enterprise solutions allow the complex environments like that of Data Centres with BCP Sites and Far DR facilities to have integrations not only at the application level but also at hardware level, which the new OEMs fail to achieve.

vi. Hardware equipment like Enterprise Class Storage have been provisioned for management of Storage at Data Centres (DC and Near BCP) initially with four controllers (active-active) upgradeable up-to eight controllers in future based on requirements with ransomware protection and disc encryption for scalability and cyber-resilience. Such features are not available in either New OEMs or MII OEMs.

vii. Performance in terms of processing, latency in information/data exchange within the DC ecosystem and response to any user accessing application/services rendered through HSDC shall be very crucial for success of electronic governance in State and all the equipment under this category i.e. compute and storage systems needs rigorous testing for their reliability, security, support (B2B from OEMs), performance etc. from their respective OEMs. Such systems are currently not available either with New OEMs or MII OEMs.

viii. Backup and restore technologies provide foundation of continuous data protection and also support automated failover & failback mechanisms once the primary data gets corrupted or damaged due to any reason. Maintaining backup policies as per the defined procedures of SDC need tried and tested equipment and hence, these features are not available to supported either by New OEMs or MII OEMs.

ix. For equipment like Web application firewall (WAF) the tried and tested features like Dynamic Application Security testing (DAST), vulnerabilities and its suggested controls are published at global level (like OWASP top 10) which if exploited, could result in loss of sensitive data, shutdown of the online service, destruction or corruption of data, etc. In view of the higher risk, the OEMs are required to be certified by global certifying Labs well accepted by Governments, Banks and PSUs which are not available either in New OEMs or MII OEMs

x. For equipment like Anti -APT, External and Internal Firewalls, IPS, HIPS, EPP, DDoS, NDR (Network Detection and Response), etc, the OEMs must have contributed for some minimum number of new vulnerabilities or attack patterns (zero-day /undisclosed

vulnerabilities) and created signatures to overcome vulnerabilities in the public domain for the betterment of the similar equipment community. These features would not only protect from the known threats but also from the upcoming threats.

xi. OEM in Research and Development Center develops latest signatures for enhancing the security based on their feeds of ongoing attacks from their deployed devices globally. Such features require maturity as an OEM which are not available either in New OEMs or MII OEMs.

xii. Advance Security technologies like Security orchestration, automation and response (SOAR) 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. Also, works on inbuilt threat indicator repository which can be used for active threat hunting using automated playbooks which are again not available in New OEMs or MII OEMs.

xiii. Security information and event management (SIEMs) devices have been provisioned in the Data Centre. The SIEM devices are capable of ingesting threat intelligence feeds and the quality of threat intelligence varies between vendors. These feeds, which are often acquired from self OEM, separate subscriptions, contain up-to-date information on threat activity observed all over the world, including, which hosts are being used to stage or launch attacks and what are the characteristics of such attacks. The greatest value in using these feeds is enabling the SIEM to identify attacks more accurately and to make more informed decisions, often automatically, about which attacks need to be stopped at the very time of detection. Factors to consider when evaluating threat intelligence should include how often the threat intelligence updates and how the threat intelligence vendor indicates its confidence in the malicious nature of each threat. Such features require maturity as an OEM which is not available either in New OEMs or MII OEMs

xiv. Element – Network Management System (EMS-NMS): The software should be compliant with latest encryption standards to ensure all the communication happening to and from the software is encrypted and secure in order to avoid any tampering of sensitive information in case of a data breach or data leak. The features require certifications on global standards for Incident management, Problem Management, Change Enablement, Service Configuration management, Service Catalogue Management, Release Management, Service Desk, Knowledge Management, IT Asset Management and Service Request Management for creating any workflow or process out-of-the box. Such features require maturity as an OEM which is not available either in New OEMs or MII OEMs

xv. SSL Orchestrator (SSLO) is a very important part for encrypting and decrypting network traffic coming in and out of Data Centre and is therefore, is very much required for the confidentiality and integrity of data in motion. Hence, any SSLO being deployed should be tried and tested and mature enough as an OEM which is mostly not available either in New OEMs.

xvi. Comprehensive DLP (Endpoint and Network), Fingerprinting technology for Data Leakage, out of the box policy templates (rich templates like for GDPR, Aadhaar, IT

Act 2008, etc. Such features again require maturity levels as an OEM which is not available either in New OEMs or MII OEMs

3. Also, the environments such as State Data Centre cannot be experimented with, as such stable, tested and well supported equipment are required for this highly complex and critical environment primarily dealing with citizen services, handling confidential & sensitive information of Citizen, Revenue and Finance related applications, etc. on 24X7 basis. Also, this equipment is required by the State in order to support the IT & e-Governance applications for a substantial period of time (5-7 years and even beyond).
4. On the above basis, the Principal Secretary to the Government of Haryana, Citizen Resources Information Department (CRID) grants exemption from Public Procurement (preference to Make in India - MII) for procurement of the items/services as mentioned in the RFP (List of items is enclosed at Annexure A) as per Clause 13 of the Haryana State Public Procurement - MII Order 2020 notified vide No: 02/08/2020-4IB-II, dated: 18-11-2020 by Department of Industries & Commerce Govt. of Haryana with a condition that exemption shall be granted for the above purpose only and shall be reviewed at any time after the completion of six (6) months.

(V. Umashankar)
Principal Secretary to Government Haryana
Citizen Resources Information Department (CRID)

Endst: No.:2/300/ 12947

Chandigarh dated, the 06.06.2023

A copy is forwarded to the following:

1. PS to ACS Industries and Commerce for kind information of ACS Industries and Commerce Department
2. Secretary to Special Secretary IT for information of Special Secretary IT.
3. Head SeMT and CITO, CRID.
4. Jt. CITO (SDC), CRID.

Director (Administration)
For Principal Secretary to Government Haryana,
Citizen Resources Information Department (CRID)

9th Floor, Haryana Civil Secretariat, Sector - 1, Chandigarh. 160001
Tel: PS (CRID): 0172-2740441, Email: psit@hry.gov.in, Director (Admn.): 0172-2748142,
Head SeMT & CITO: 0172-2703479, 0712-2708285, Email: cito.ditech-hry@nic.in
Website: www.haryanait.gov.in

Haryana Government
Citizen Resources Information Department

Azadi ka Amrit Mahotsav

हरियाणा सरकार
नागरिक संसाधन सूचना विभाग

Annexure - A

S.No.	BOQ Item
	Compute and Storage
1	Rack Server 64 Core & 32 Core CPU in Dual Socket
2	SAN Storage (All Flash NVME with 5 year warranty support)
3	SAN SWITCHES (48 Port) 4 Uplink (16/32) with cascade license
4	Object Storage
5	NAS Storage
6	Server Rack with PDU
7	High End Desktop for NOC & SOC setup
8	HCI Solution (in FTT2) with 2 mode failure
	Networking
9	TOR Switch (48 port)
10	Network Switches (L3)
11	Core Switch HA
12	Core Router
13	SDN
14	Global Server Load Balancer
15	Server Load Balancer
	Backup
16	Tape Library (LTO) with 50 Tapes, 2 cleaning tapes and tape labels
17	Purpose Built Backup Appliance with 3 PB raw capacity
18	Backup software license based on front end capacity for 500 TB for 5 year
	Cyber Security
19	Distributed Denial-of-Service(DDOS)
20	Web application firewall (WAF)(5 Year)
21	Advanced Persistent Threat (APT)
22	SSL Decryptor & SSL Encryptor
23	IPS
24	Internal Firewall HA NGTP (IPS,URL Filtering, Malware)
25	External Firewall HA NGTP (IPS,URL Filtering, Malware)
26	Security Information and Event Management (SIEM) with Video wall requirement
27	Security Orchestration Automation and Response (SOAR)
28	Network Detection & Response (NDR)
29	Data Loss Prevention (DLP)
30	Host Intrusion Prevention System (HIPS)/EDR/EPP/XDR(End Point Protection and Malware Detection& Removal and Prevention)
31	Application vulnerability security & audit tool
	System Software
32	Enterprise Monitoring Solution(EMS),Network Monitoring Solution (NMS), Application Performance Monitoring
33	Governance, Risk & Compliance (GRC) tool
34	Server Virtualization Software (Latest Version) with 5 year Support
35	Cloud Automation, Orchestration & Management

9th Floor, Haryana Civil Secretariat, Sector - 1, Chandigarh. 160001

Tel: PS (CRID): 0172-2740441, Email: psit@hry.gov.in, Director (Admn.): 0172-2748142,
Head SeMT & CITO: 0172-2703479, 0712-2708285, Email: cito.ditech-hry@nic.in
Website: www.haryanait.gov.in