Request for Proposal (RFP)

Procurement for upgradation of Servers, Storage & IT related Equipment through Central Public Sector Units (PSU's) –in a Single Bid System

For

New Haryana Secretariat, Sector-17, Chandigarh

Citizen Resources Information Department (CRID), Haryana

Regd. Office: SCO 109-110, Sector 17-B Chandigarh-160017 Phone 0172-2704922

Phones : - 0172-2703479

Email: - rosy.gandhi-hry@hry.gov.in, addl-cito.crid@hry.gov.in, munishchandan.crid@hry.gov.in,

Website: - https://etenders.hry.nic.in

Contents

INTRODUCTION

The Government of Haryana recognizes the important role of Information and Communication Technologies (ICT) in delivery of citizen services and governance processes in an efficient and transparent manner. Citizen Resources Information Department (CRID), erstwhile Department of Information and Technology (DITECH) of the State Government of Haryana was established to facilitate planning, designing, implementing and managing a wide range of IT initiatives at department/ organization levels.

With a wealth of IT and policy expertise, in-house development capabilities, Department enables implementation of government-wide information technology (IT) policies and programs, and use data, analysis and collaboration to deliver results and solutions that improve State Government IT service delivery with collaborative working relationships among Director (CRID IT), State Information Officer (SIO, NIC), Additional Chief Information Technology Officer (ACITO). Department also supports IT software development, personnel, solutions, support and expertise to address both the most common, and the most complex, State Government of Haryana's IT challenges. Operating at the intersection of policy and program execution, department's team helps to navigate the complexities of Information Technology (IT), including Cybersecurity, Domain Services and internet connectivity for the State Government of Haryana, Information Integrity, IT Accessibility and IT Infrastructure Modernization and data center optimization

The Department headed by the Commissioner & Secretary (CRID), develops and provides direction in the use of Internet-based technologies to make it easier for citizens and businesses to interact with the State Government, save taxpayer money, and streamline citizen participation.

To address the growing data requirements, Citizen Resources Information Department (CRID), on behalf of The Revenue Department, Government of Haryana, intends to procure comprehensive server and network infrastructure with Security software for a period of five years. The objective of this procurement is to establish a robust and highly available IT infrastructure to support mission-critical applications operating on the MS SQL Server database framework.

Purchaser: Citizen Resources Information Department (CRID), Haryana

Owner Department: Revenue & Disaster Management Department Haryana

SECTION 1

IMPORTANT INFORMATION

1. IMPORTANT INFORMATION

1.	Tender Inviting Authority Designation and Address	Citizen Resources Information Department (CRID), Haryana. Regd. Office:- SCO 109-110, Sector-17B, Chandigarh
2.	Name of the Work	Procurement for upgradation of Servers, Storage & IT related Equipment through central Public Sector Units (PSU's) –in a Single Bid System For New Haryana Secretariat, Sector-17, Chandigarh.
	Tender reference	e-Tender/CRID/Revenue ICT Infra/2025-26 And e-Tender ID: 2025_HRY_473189
	Place of Execution	New Haryana Secretariat, Sector-17, 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	**₹25.00 Crore + applicable taxes**
	Processing Fee for Tender	The Payment for Tender Document Fee **₹11,800/-** (Rupees Ten Thousand Eight Hundred Only) i.e. (₹10,000/- + 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 favour of Citizen Resources Information Department. Scanned copy of Online Payment Receipt should be uploaded with technical e-bid.
	Earnest Money Deposit (EMD)	The EMD will be ₹ 2,00,000/- (Rupees Fifty Lakh only), which shall be made by eligible bidders through Online Mode at NIC Portal in favour of Citizen Resources Information Department. Scanned copy of Online Payment Receipt should be uploaded with technical e-bid.
4.	Starting date of Tender	**19-09-2025 from 09:00 AM onwards**
5.	Last date and time for submission of e-Tender	**04-10-2025 at 05:00PM**
6.	Last Date for receipt of Queries for Pre-bid Conference	Date & Time: 26.09.2025, 3:30:00 PM Email Id: rosy.gandhi-hry@hry.gov.in, addl-cito.crid@hry.gov.in, munishchandan.crid@hry.gov.in
7.	Pre-bid Conference Date & Time (tentative)	Date & Time**: 27.09.2025, 11:30:00 AM** Preferably, in Haryana Nivas; however, confirmation on the same shall be communicated in 2 days in advance on the given link: https://haryanait.gov.in/#tenders (*under the Section "Tender & Notices"*)
8.	Last date for submission of hard copy of the technical bid to CRID.	**Within 3 Days from the date of opening of technical bids** (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 Additional Chief Information Technology Officer (ACITO), CRID, 4th Floor, SCO 109-110, Sec 17-B, Chandigarh, 160017
9.	Date and Time of Opening of Technical Bids	**07-10-2025, 04:00:00 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.**

SECTION 2

INSTRUCTION TO BIDDERS ON ELECTRONIC TENDERING SYSTEM

2. INSTRUCTIONS TO BIDDER ON ELECTRONIC TENDERING SYSTEM

1. Bidder should do Online Enrolment in this Portal using the option Click Here to Enrol available in the Home Page. Then the Digital Signature enrolment 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/MtnlTrustlin/SafeScrpt/TCS.

2. Bidder then logs into the portal giving user id / password chosen during enrolment.

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, purchase 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, as applicable to e-Tenders.

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

3. SCOPE OF WORK:

3.1 Citizen Resources Information Department (CRID), a State Govt. undertaking intends to procure comprehensive Compute, Storage, Network & Security infrastructure equipment for a period of 5 years. This procurement aims to establish a robust, highly available IT infrastructure to support their mission-critical applications framework with MS SQL Server database as per the minimum technical specifications and other terms and conditions.

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

3.3 All technical compliance documentation shall be cross-referenced with the OEM's official product datasheet and must include verifiable product links from the OEM's official website or documentation portal.

3.4 The successful bidder/ 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:

a. 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 the devices, equipment, accessories, software, licenses, tools, etc. shall also be provisioned according to the requirements of the solution.

b. Purchaser/Owner will not be responsible if the MSI has not provisioned for any components, subcomponents, assemblies, sub-assemblies as part of bill of material in the bid. The MSI will have to make provision(s) of any such required components, subcomponents, assemblies, sub-assemblies, etc. to meet the solution requirements at no additional cost and time implications to purchaser.

3.5 It is expected that MSI and OEM shall ensure that the equipment/components being supplied will be supported for minimum 5 years from date of bid submission. In the event that any equipment/ component is declared end-of-support or withdrawn from support by the OEM for any reason whatsoever, the MSI shall replace it with an equivalent or better substitute that is acceptable to purchaser without any additional cost to the purchaser and without impacting the performance of the solution in any manner whatsoever.

3.6 The 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 the purchaser shall not be bound or dependent on buying a particular hardware of virtualization solution.

3.7 Important technical components of the architecture must support scalability to provide continuous growth to meet the growing demand of the owner department without adversely affecting the response time and throughput of the system. Main technology components requiring scalability are storage, bandwidth, computing performance (IT Infrastructure).

3.8 The solution 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.

3.9 Upon award of purchase order / work order / contract, the selected vendor will carry out:

a. Minimal downtime during transition

b. Performance optimization and testing post-migration

3.10 Installation & Configuration of the Commissioned ICT Infrastructure: The MSI shall be responsible for the delivery, installation testing and commissioning of the servers, storage, network, security related equipment in the Data Centre.

a. The MSI shall carry out the planning and layout design for the placement of equipment in the provisioned space of 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.

b. 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.

c. The MSI shall carry out installation of equipment in accordance with plans and layout design as approved by the CRID.

3.11 Expectation and Consideration from MSI:

a. MSI shall engage early in active consultations with the Owner department 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 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. Validate / Assess the re-use of the existing infrastructure if any within Authority site.

3.12 MSI shall be responsible for supply of all the Products/equipment such as optical fiber cable, Network, Hardware, Software, Devices, etc. as indicated (but not limited to) in the tentative Bill of Materials included in the RFP and their appropriate quantity & capacity.

3.13 All offered equipment should support interoperability with major OEM brands for equipment like Routers, Switches etc.

3.14 All the features mentioned in the technical specifications should be available from day one.

3.15 Power & Console Cables, necessary drivers and software required to run the equipment must be supplied during installation and commissioning from day one without any additional cost.

3.16 Supply, Installation, and Commissioning of entire solution.

3.17 MSI has to provide Enterprise version for all Open-source software. No community version will be accepted.

3.18 MSI shall be responsible for up-gradation, enhancement, and provisioning additional supplies of network (including active / passive components), hardware, software, etc. as requisitioned by Owner/Purchaser.

3.19 MSI shall ensure that the end of support is not reached during the concurrency of the contract and 5 years thereafter.

3.20 MSI shall ensure compliance to all mandatory government regulations as amended from time to time.

3.21 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.

3.22 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.

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

3.24 Fibre Passive Components & UTP Cabling components (i.e. Cable, Patch Cords, Pig Tails,I/O etc) may be from any single OEM. Other Passive components must also be from the standard OEM meeting all the specifications as mentioned in the RFP and the MSI to quote single OEM for each category / type of Passive Equipment. All the components of different OEMs proposed in the bid should be compatible and interoperable.

3.25 The cost of all hardware items must include mandatory 5 years onsite comprehensive Original Equipment Manufacturer’s warranty.

3.26 25 years performance warranty certification is to be provided by supplier for cabling from OEM after complete installation.

3.27 The quoted products should not be end of sale / life for next 2 years and OEM support of the same should be available for next 5 years after end of life / sale.

3.28 The details of offered service support pack of the OEM is to be provided with the supplied components.

3.29 The Supplier is required to supply the latest updates, patches and upgrades for supplied server/computer OS updates, NGFW, WAF, SSC, Antivirus, database, storage free of cost during the warranty period.

3.30 The quoted rates should be inclusive of all installation works like but not limited to preparing of cable layout / diagram, cable tray, cable, punching, fixing of active & passive components, tagging of patch cords etc.

3.31 Proper tagging of all cables including uplinks with numbers is to be prepared by supplier & must be pasted on Rack Glass.

3.32 The Selected Bidder is required to provide a comprehensive warranty for the products for a period of 5 years from the date of acceptance letter/ Go live after completion of work.

3.33 The warranty shall cover the system software, components and sub-components of the supplied infrastructure including patches and upgrades (both functional and security for free of cost) of the system software.

3.34 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 without any additional cost.

3.35 All the operating system/software licenses if applicable are to be registered in the name of the owner department (Revenue & Disaster Management Department Haryana).

3.36 Supplier should also prepare a detailed professional project report which shall include and not limited to detailed labelled LAN diagram, list of all active & passive components, make & model/Part code with serial number, device numbering details, list of IP addresses including Switches, servers, firewalls other items IP Addresses and all configuration details, cabling diagram, connectivity diagram, patch panel details, tagging details of all cables including uplink with number, location details of Switches, Servers, Racks details, supplied OS Keys (if any) so that no ambiguity may arise. The report should be proper binding, name of project & site name & location address should be printed on cover, proper indexing and should be submitted in double copy i.e. each for Revenue & Disaster Management Department Haryana, Nodal Officer & CRID.

3.37 Key responsibility of supplier:

a. **Supply and installation of all hardware components:** Acquisition of appropriate Compute, Storage, Network, security and business continuity appliances based on organizational requirements for performance and capacity.

b. **Physical Installation:** Deployment of hardware in server rooms, including proper racking, cabling, power connections, and initial hardware testing to ensure all components are functioning correctly.

c. Supply of Security Software

d. **Configuration and Integration:** Installation of Windows Server operating systems and other softwares on servers / VM's, configuration of storage pools/volumes, setup of firewall security policies, and integration of all components into a cohesive network infrastructure with appropriate segmentation.

e. **Testing and commissioning:** Comprehensive testing of the entire infrastructure, including performance benchmarking, security assessments, failover testing, and validation that all systems meet the established technical requirements.

f. Must provide comprehensive technical support during the service period.

g. Documentation and knowledge transfer

h. Deploy, install and configure Database server(s)

i. Deploy, install and configure Web Services: IIS-based web applications

j. Knowledge Management / Training

k. Adaptive Maintenance. Any maintenance activity to be performed on off day / holidays.

l. Attending to and resolving system failures and snags.

m. Support and maintain the overall infrastructure

n. Configuration and backup of system data including documentation of all configurations, VLANS, Policies etc.

o. Maintains Secrecy of the systems i.e. not to share Network / LAN / Office details / other infrastructure details with any outside agency officially or unofficially.

p. Preventive Maintenance will be provided on quarterly basis which include cleaning & dusting of racks, switches, fans etc. even if no complaint is lodged. Signed reports by Nodal Officer must be submitted to CRID.

q. Support for warranty repairs / replacements will include equipment pickup, shipping, tracking and return etc.

r. Any other activity related to installation and commissioning as deemed fit by owner department.

3.38 Apart from the above MSI, need to ensure compliance of the project with Government of India IT security guidelines including provisions of:

a. The Information Technology Act, 2000 and amendments thereof and

b. 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.

3.39 Responsibilities: It is the responsibility of the supplier to keep the equipment in good working condition so as to ensure a minimum downtime as of the Haryana state data centre after carrying out all necessary repairs / maintenance of equipment, otherwise it shall be treated as a non-performance on the part of the Supplier for which suitable action may be taken against their firm. In case the supplier fails to rectify the problem within allotted time then penalty will be applicable as per penalty clause.

3.40 Owner at its discretion, may also engage independent auditors 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.

3.41 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.

3.42 MSI will be responsible to propose transition strategy for dismantling of existing hardware and setting up of new hardware with minimal impacting the services of owner. 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.

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

a. High Level Design, Logical and physical infrastructure design for all devices.

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, 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.

3.44 GST or other taxes at the time of billing will be applicable.

3.45 Payment shall be made after adjusting penalties (if any) as applicable.

3.46 All payments shall be made subject to deduction of TDS (Tax deduction at Source) as per the current Income-Tax Act.

3.47 Delivery terms: Delivery within 10 weeks from the date of issue of work order.

3.48 Installation & site handover schedule: Installation within 08 weeks of delivery of ordered material.

3.49 Payment terms: The payment for Phase(s) will be released site wise:

S#	Phase	Amount to Payment to be released	Document(s) to be submitted for release of payment	Remarks
Start	Letter of Acceptance (LOA)	The successful bidder(s) will submit total Performance Bank Guarantee (PBG) amounting to 10% of the tender value to be issued in favour of Special Secretary (IT) and Treasurer, CRID within 10 days from the date of issuance of Letter of Acceptance (LOA) with validity of 5 years and 8 months. If the contract is extended, the PBGs shall also be extended similarly by the successful bidder(s).		
	Phase-1: Payment on Delivery of active & passive items & Inspection Delivery Time: Within 12 weeks from the date of issue of work order.	80% of the CAPEX (as per Format 2) amount i.e. Network, Compute, Storage, Security devices etc. and approximate passive components	Invoice/s & delivery challans duly signed by the Nodal Officer(s) at the respective site and inspection reports per site duly signed by the Inspection Committee	This phase payment will be released after deduction of applicable SLA/ penalties (if any). Amount shall be derived based on the requirements of the components as available in the Contract/Agreement.
	Phase-2:	20% of the CAPEX (as per Format 2) amount	Final Acceptance Testing of	This phase payment will be released after

S#	Phase	Amount to Payment to be released	Document(s) to be submitted for release of payment	Remarks
	Payment on Installation and Go-Live Timeline: within 08 weeks of delivery of ordered material		1. Newly set system 2. Data migration 3. Unit Testing of department Application Invoice/s, installation reports, warranty certificates of all OEMs, HLD, LLD, Network Configuration document, Security Configuration document, Server Configuration, Go-live reports and other important document as required by the Owner/Purchaser.	deduction of applicable SLA/ penalties (if any).
	Phase 3 Warranty from year 2 to year 5	Payment for each year warranty as quoted against respective years in OPEX section of format 2 shall be released in 2 equal instalments at the end of each 6 monthly cycle starting from the next day of completion of previous year warranty. e.g. Payment for 2nd year warranty as quoted against "2nd year warranty for all items" in OPEX, shall be released in 2 equal instalments at the end of 6 monthly cycle starting from the next day of completion of Phase 4 i.e. completion of 1st year warranty	Invoice(s) along with , Incident Report / Service Call report and SLA compliance report verified by the respective Nodal Officer of the CRID.	This phase payment will be released after deduction of applicable SLA/ penalties (if any).

3.50 Overall UPTIME SLA

Penalty for Service and Equipment Failure (for the Data Centre ICT infrastructure components supplied and installed under this project) for the duration of 5 years from Go-Live shall be calculated on the basis of total Service failure and individual Equipment / Part.

S. No.	Measurement	Target uptime (Quarterly)	Penalty
1	Overall Uptime for Data Center	99.98%	No Penalty
		>=99.5% to <99.98%	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 up to 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. 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)
b. The downtime shall be the time from the point where 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 standby equipment is made available for carrying out intended operations (including installation, configuration, restoration, boot-up time, etc.)
c. 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.
d. MSI's SLA will not be affected by any downtime due to power related issues at HSDC.
e. The Penalty shall be calculated on quarterly basis as per the target specified.
f. 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.
g. If downtime of system or subsystem affects the operation of other systems, then MSI has to pay penalty for the affected systems also.

3.51 Penalty clauses:

a. Penalty for delay in delivery beyond the allotted time period (Phase-1) :

S#	Penalty	Duration of Delay (Weeks)					Penalty Amount on delivery per site (%)			
1	Penalty for delay in delivery beyond the allotted time period	Delay of first two weeks (14 days)					0.5% per week			
2		Delay for next three weeks (21 days)					0.75% per week			
3		Delay of next four weeks (28 days)					1% per week			
		Described as under:								
		Week-1	Week-2	Week-3	Week-4	Week-5	Week-6	Week-7	Week-8	Week-9
		0.50%	1.00%	1.75%	2.50%	3.25%	4.25%	5.25%	6.25%	7.25%
4		In case of further delay, thereafter, CRID could cancel the order or give the order to other vendor on same rates or re-tender it and suitable action as stipulated in this tender document could be taken against the company / firm.								
5		However, if, Purchasing Department opts to accept the items beyond the above-mentioned delay, 1% penalty per week would continue for any unjustified delay in delivery subject to maximum cap of 10% penalty.								
		The penalty will be calculated based on the CAPEX value of respective site.								

b. Delay in installation & commissioning – Phase 2:

S#	Penalty	Duration of Delay (Weeks)	Penalty Amount on total value (%) Per site
1	Penalty for delay in installation beyond the allotted time period	Delay of first two weeks (14 days)	0.5% per week
2		Delay for next three weeks (21 days)	0.75% per week
3		Delay of next four weeks (28 days)	1% per week
4		In case of further delay, thereafter, CRID could cancel the order or give the order to other vendor on same rates or re-tender and suitable action as stipulated in this tender document could be taken against the company / firm.	
5		However, if, Purchasing Department opts to accept the installation beyond the above-mentioned delay, 1% penalty per week would continue for any unjustified delay in installation subject to maximum cap of 10% penalty for site. The penalty will be calculated based on the total CAPEX value of the respective site	

c. Delay in achieving Collective Go- Live – Phase 3

S#	Penalty	Duration of Delay (Weeks)	Penalty Amount (%) – Collective
1	Penalty for delay in achieving Collective Go-Live	Delay of first two weeks (14 days)	0.5% per week
2		Delay for next three weeks (21 days)	0.75% per week
4		In case of further delay, thereafter, CRID could cancel the order or give the order to other vendor on same rates or re-tender and suitable action as stipulated in this tender document could be taken against the company / firm.	
5		However, if, Purchasing Department opts to accept the installation beyond above mentioned delay, 1.5% penalty per week would continue for any unjustified delay in installation subject to maximum cap of 10% penalty The penalty will be calculated based on the CAPEX value of the total project.	

3.52 Penalty during warranty period: The service calls will complete as per mentioned time durations otherwise penalty shall be levied @ ₹1,00,000/- per day for appliance(s) down. However, the total penalty under this clause shall be capped at 10% of the total contract value during the entire warranty period. Also, if the total penalty value is applicable beyond the Capped Value, the Department has right to terminate the contract and forfeit the Performance Bank Guarantees still submitted to the department and to Blacklist the bidder on the grounds of non-performance.

3.53 The vendor will depute a site-in-charge at the site for taking care of the delivered items and these will remain in the custody of the vendor only. Government will take ownership of the items after Go-live.

3.54 Lockable room will be provided at site and lock and key of the room will be in the custody of the site-in-charge deputed by the vendor.

3.55 Issuance of delivered items to the commissioning teams will be taken care of by the site- in-charge.

3.56 SS (IT) AND TREASURER, CRID reserves the right to terminate the contract any time, in case the Supplier does not provide quality service during warranty period and liable for suitable action can be taken against supplier company/firm.

3.57 EMD will be released upon receipt of PBG.

3.58 Arbitration: In the eventually of any dispute the arbitration will be done as per the Arbitration and conciliation Act 1996 G.O.I.

3.59 Physical Damage repair / replacement: Any damage to the equipment installed due to user negligence shall be replaced on paid basis as per approved rates.

SECTION 4

ELIGIBILITY CRITERIA

4. ELIGIBILITY CRITERIA

4.1. This RFP is open only to all Central Public Sector Undertaking within India, who are eligible to do business in India under relevant Indian laws as in force at the time of bidding. The PSUs shall have experience in installation and commission of data centers for other state departments or central departments.

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 Undertaking as placed at Annexure-13 & 14 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 CRID.

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 and Amendment Memo No. 2/3/2018-4IB-II dated 23.04.2018 and their sub sequent amendments. Manufacturing Micro and Small Enterprises (MSEs including Khadi and Village Industries/Units) who have filed Entrepreneur Memorandum or any other document as per the above-mentioned Notification and their amendments 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:

S#	Clause	Documents Required
1.	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 Citizen Resources Information Department. Scanned copy of Online Payment Receipt should be uploaded with technical e-bid.
2.	EMD should be submitted.	The EMD will be ₹ 2,00,000/- (Rupees Fifty Lakh only), which shall be made by eligible bidders through Online Mode at NIC Portal in favour of Citizen Resources Information Department. Scanned copy of Online Payment Receipt should be uploaded with technical e-bid.
3.	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.	A Certificate from CS certifying that the Bidder is authorized by Board of Directors / Managing Director / CEO.
4.	Manufacturer Authorization Format (MAF)	The bidder must submit a valid Manufacturer Authorization Format (MAF) issued on their letter head by the Original Equipment Manufacturer (OEM) in favour of the bidder as per the Annexure-5. The OEM must be registered in India under the Indian Companies Act, 1956. (copy of Registration certificate must be submitted) (For Network, Compute, Storage, Security and cable Components)
5.	The bidder must be registered Central Public Sector Undertaking in India under the Indian Companies Act, 1956 and should be in existence in India for at least the last 3 financial years, as on date of submission of bid.	The bidder shall provide the Certificate of Incorporation for Registered Companies.
6.	OEM Qualification Criteria The OEM should be in manufacturing of offered (or similar) products for at-least 3 out of last 5 financial years in addition to current year as on bid submission date for Active and cabling component.	Copies of Supply orders/ Invoices/ Completion Certificate from the concerned supplier/ client, conforming the total quantity/ value and destination where supplied, be considered proving at least 3 years out of 5 years in manufacturing in one each from any of the following Financial Years 2019-20, 2021-22, 2022-23, 2023-24, 2024-25 current FY/ till bid submission date. (For Network, Compute, Storage and Security Components)

S#	Clause	Documents Required
7.	The OEM should have supplied the similar equipment of 200% (Two times) of estimated tender quantity of respective items in last 3 financial years. The orders should be executed on behalf of States or Central Govt./ PSUs/ Central or State Universities/ Scheduled banks for Active components.	Certified letter from the concerned Client(s) confirming the total amount, date of engagement and successful completion of order within the time stipulated in work order. i.e. 2022-23, 2023-24, 2024-25 current FY/ till bid submission date. (For Network, Compute, Storage and Security Components) Any chain of POs and Completion Certificates which establish that the OEM Products were supplied during the project / engagement through System Integrator / Partner / Distributors to the customers mentioned in point 7 of this table shall be accepted.
8.	Bidder Qualification Criteria, they should be in the business of implementation and commissioning of data center for any 3 financial years out of last 5 financial years on behalf of States or Central Govt. / PSUs / Central or State Universities / Scheduled Banks.	Copies of work orders or contract proving at least 3 years, one each from any of the following Financial Years 2020-21, 2021-22, 2022-23, 2023-24, 2024-25, current FY/ till bid submission date.
9.	Registered Office.	There should be at least one registered office of the bidder in Tri- city/ Haryana/ NCR.
10.	The bidder should have executed orders of implementation and commissioning of data center in the last 3 financial years. The orders should be executed on behalf of States or Central Govt. / PSUs / Central or State Universities / Scheduled Banks.	Three completed orders each costing not less than the amount equal to 50% of the estimated cost. Or Two completed orders each costing not less than the amount equal to 80% of the estimated cost. Or One completed order costing not less than the amount equal to 100% of the estimated cost. For, 2022-23, 2023-24, 2024-25, current FY/ till bid submission date. (For Network, Compute, Storage and Security Components) (Work orders & completion reports for Data Center or other projects with equivalent quantity of active component where it includes installation and commission of active components along with UTP and fiber optic cable laying).
11.	The bidder should have positive net worth (measured as paid up capital plus free reserves) in any of two years out of 3 financial year i.e. 2021-22, 2022-23 & 2023-24	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.
12.	Should not have been black listed as on date of submission of Bid.	An Undertaking as per the Annexure-2 to be submitted by bidder on non-judicial stamp paper.
13.	Service Center	There should be at least one OEM owned or authorized service center in Tri- city/ Haryana/ NCR. (For Active Hardware components)

S#	Clause	Documents Required
14.	ISO Certification	ISO 9001:2015/2018 or latest Certificate issued in the name OEM and ISO 14001 Certificate issued in the name of OEM for handling of hazardous items in the manufacturing process. (For Network, Compute, Storage and Security Components)
15.	Product compliance	As mentioned in the Technical Specification. The Annexure- 4 shall be cross-referenced with the OEM's official product datasheet and must include verifiable product links from the OEM's official website or documentation portal.
17.	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 CRID. Bid of such OEM and their product/bidder will not be considered. (Annexure 13 & 14)
18.	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)

Note:- For MSME, Start up, the turnover, experience and other conditions will be applicable as per Haryana State Govt. Guidelines issued time to time.

Relaxations to Micro Small and medium Enterprise registered in Haryana: -

A. Concessions/benefits Micro-Small: -

S#	Area as part of qualifying requirements	Concession benefits allowed to MSEs.	Eligibility
1.	Tender Fee	Exemption on the payment of Tender Fee subject to fulfillment of conditions as per eligibility	Manufacturing Micro & Small Enterprises (MSEs) (including Khadi & village industries/ Units) who have filed SSI Certificate/EM Part-ll/Udyog Aadhaar Memorandum (UAM)/Udyam Registration in Haryana (applicable and valid on that date as per Govt. instructions) in respect of the quoted items, participate directly in tender and 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 the copy of SSI Certificate /EM Part-ll/ Udyog Aadhaar Memorandum (UAM)/ Udyam Registration in Haryana (Applicable and valid on thot date as per Govt. instructions) in respect of its category of Micro/ Small issued to the firm by the Industries Department Haryana as part of Technical Bid.
2.	Earnest Money Deposit (EMD)	Exemption on the payment of Earnest Money deposit (EMD) subject to fulfillment of condition a per eligibility.	
3.	Performance Security	90% concession on Performance Security as applicable to other Haryana based firms subject to fulfillment of condition as per eligibility	
4.	Turnover	a. Micro Enterprises: Concession of 80% on Turnover condition imposed as qualifying criteria. b. Small Enterprises: Turnover condition imposed as qualifying	

S#	Area as part of qualifying requirements	Concession benefits allowed to MSEs.	Eligibility
5.	Past Performance & Experience	Exempted in respect of Past Performance & Experience as part of qualifying Requirement of the tender subject to fulfillment of condition as per eligibility	Manufacturing Micro & Small Enterprises (MSEs) (including Khadi & village Industries/ Units) who have filled SSI Certificate /EM Part-ll/ Udyog Aadhaar Memorandum (UAM)/ Udyam Registration in Haryana (Applicable and valid on thot date as per Govt. instructions) in Haryana and Further: a) Those MSEs have Qualified Certification of ISI/ISO/AgMark/Quality Mark issued from competent authority in State or Central Govt. in respect of the item/ Goods mentioned in the tender. The firm will be required to submit the detailed information in respect of above through an affidavit as per the format enclosed as "Annexure 10" OR/AND b) Those who are registered with DGS&D/ NSIC /GOI Department/ State Govt. Department/GOI PSUs/State Govt. PSUs in respect of the item/goods mentioned in the tender. The firm will be required to submit the detailed information in respect of above through an Undertaking as per the format enclosed as Annexure-10.
6.	Purchase Preference	50% of the total tendered quantity provided quoting price within band of L-1+15% by bringing down their price to L-1and subject to condition that it agrees to fulfillment of other terms & conditions of the tender and further subject to fulfillment of conditions as per eligibility	

B. Concessions/benefits to Medium Enterprises: -

S#	Area as part of qualifying Requirements	Concessions/benefits allowed to medium Enterprises	Eligibility
i.	Past Performance & Experience	Exemption on Qualifying Requirement of Past Performance & Experience as part of Qualifying Requirements of the tender subject to the tender subject to fulfillments of conditions as per eligibility.	Manufacturing Medium Enterprises of the State that have filed SSI Certificate/ EM Part-ll/ Udyog Aadhaar Memorandum (UAM)/ Udyam Registration in Haryana (Applicable and valid on that date as per Govt. instructions for quoted items in Haryana, participate directly in tender and not through any intermediaries (their

S#	Area as part of qualifying Requirements	Concessions/benefits allowed to medium Enterprises	Eligibility
ii.	Purchase Preference	10% of the total tendered quality provided quoting price within band of L-1+15% by bringing down their price to L-1 and subject to condition that it agrees to fulfillment of other term & conditions of the tender and further subject to fulfillment of conditions as per eligibility.	dealers/agents/ Distributors), and will not subcontract to any other firm and to carry the entire manufacturing at their enterprise. This concession will be applicable only for one year to newly registered Medium Enterprises or Medium Enterprises of State who are not eligible in State Public Procurement due to eligibility criteria of part performance & Experience. The Firm will be required to submit the detailed information in respect of above through an affidavit as per the format enclosed as Annexure-11.

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

5. MINIMUM TECHNICAL SPECIFICATIONS OF THE PRODUCTS:

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

5.1. Server:

Servers Specifications	
Item	**Description of Requirement**
Chassis	2U Rack Mountable
CPU	Dual Intel Xeon/AMD Processor each with minimum 64 Cores each
Chipset	Intel® C741 Chipset/SOC Design
Memory	1024 GB RAM scalable upto 4.0 TB using DDR5 Registered DIMM (RDIMM) operating at 4800MT/s
Bus Slots	Server should support upto eight PCI-Express 5.0 x16 slots.
Storage	2x900GB SSD Drives for Operating System
HDD Bays	Upto 8SFF Drive Bays
Controller	Server should be supplied with Embedded / PCIe based x16 RAID controller with 4GB Flash backed write cache, supporting RAID 0, 1, 5, 6, 10, 50, 60. Must support mix-and-match SAS, SATA, and NVMe drives to the same controller. Controller must support 6G SATA, 12G SAS, 16G NVMe.
Networking features	4-Port 1Gb Ethernet Network Adapter , Dual Port 10/25Gb SFP+ Network Adaptor, Dual port 32Gbps Fibre Channel HBA with transreceivers
Interfaces	Serial - 1 (Optional) USB support with Up to 5 total: 1 front, 2 rear, 2 internal. 1GbE Dedicated management port
Power Supply	Should support hot plug redundant low halogen power supplies with minimum 94% efficiency
Fans	Redundant hot-plug system fans
Industry Standard Compliance	ACPI 6.3 Compliant PCIe 5.0 Compliant WOL Support Microsoft® Logo certifications PXE Support Energy Star SMBIOS 3.2 UEFI 2.7 Redfish API IPMI 2.0 Secure Digital 4.0 Advanced Encryption Standard (AES) Triple Data Encrytion Standard (3DES) SNMP v3 TLS 1.2 DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP)

Servers Specifications	
	Active Directory v1.0 ASHRAE A3/A4
System Security	UEFI Secure Boot and Secure Start support Tamper-free updates - components digitally signed and verified Immutable Silicon Root of Trust Ability to rollback firmware FIPS 140-2 validation Secure erase of NAND/User data Common Criteria certification TPM (Trusted Platform Module) 1.2 option Configurable for PCI DSS compliance TPM (Trusted Platform Module) 2.0 option Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser Bezel Locking Kit option Support for Commercial National Security Algorithms (CNSA) Chassis Intrusion detection option Secure Recovery - recover critical firmware to known good state on detection of compromised firmware
Operating Systems and Virtualization Software Support	Windows Server. Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware ESXi and Morpheous VM Essential Canonical Ubuntu Oracle Linux and Oracle VM, Citrix
Virtualisation Software	Bidder should offer the server with virtualisation software as per mentioned specifications for the total no of cores/sockets mentioned in CPU section for compute virtualisation with OEM support for 5 years.
Provisioning	1. Should support tool to provision server using RESTful API to discover and deploy servers at scale 2, Provision one to many servers using own scripts to discover and deploy with Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows PowerShell
Firmware security	1. For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable 2. Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware

Servers Specifications	
Embedded Remote Management and firmware security	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication 2. Server should have dedicated 1Gbps remote management port 3. Server should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware 4. Server should support agentless management using the out-of-band remote management port 5. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 6. Two factor Authentication 7. Local or Directory-based user accounts with Role based access control 8. Remote console sharing upto 6 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support.Should provide support for AES and 3DES on browser.Should provide remote firmware update functionality.Should provide support for Java free graphical remote console. 9. Should support managing multiple servers as one via Group Power Control Group Power Capping Group Firmware Update Group Configuration Group Virtual Media and Encrypted Virtual Media Group License Activation 10. Should support RESTful API integration 11. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support 12. Server should have security dashboard : displaying the status of important security features, the Overall Security Status for the system, and the current configuration for the Security State and Server Configuration Lock features. 13. One-button Secure Erase designed to decommission/repurpose servers 14. NVMe wear level display 15. Workload Performance Advisor - Provides server tuning recommendations to improve server performance

Servers Specifications	
Server Management	Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resources user is authorized to view.
	The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware • Appliance alerts
	The Systems Management software should provide Role-based access control
	Zero Touch Provisioning (ZTP) using SSDP with remote access
	Management software should support integration with popular virtualization platform management software like Vmware vCenter & vRealize Operations, and Microsoft System Center & Admin Center
	Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.
	Should provide an online portal that can be accesible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contrats and status. The Portal should also provide a personalised dashboard to monitor device heath, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud).
	Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.
	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
	The Server Management Software should be of the same brand as of the server supplier.
Cloud Enabled Monitoring and Management	1. Secure connection from customer sites to cloud service 2. Unified Identity & Access Management 3. Manages and controls servers regardless of physical location 4. Subscription-based entitlement 5. Efficient Device Onboarding 6. Firmware Update Awareness with Intelligent delta-only based updates 7. Set Group firmware Baseline and Compliance monitoring and notification 8. Group based firmware management that can be scheduled or on-demand 9. Remote Site management with low bandwidth/high latency

Servers Specifications	
	network connectivity 10. Role-based access and views for managed customer environments 11. GUI and Rest APIs for core features
Warranty	Server Warranty includes 5-Year Parts, 5-Year Labor, 5-Year Onsite support with next business day response.
OEM Brand Eligibility	The OEM brand should be in existance for last more the 20 years in India for better support services. The OEM should be present in Leaders Quardrant for servers in Latest Gartner report. The OEM should present in the top 3 brands in IDC report. The OEM should be ISO 9001, ISO 14001, ISO 20000, ISO 27001 Certified.

5.2. Storage:

Enterprise SAN Storage Specifications		
Sr. No	**Parameter**	**Technical Specifications**
1	Capacity & Scalability	Offered Storage array shall be supplied minimum with **500TB usable Capacity** using NVMe drives and shall be configured in Raid 6. Vendor shall not use more than 10D+2P while sizing the array. Offered Storage shall be able to protect against at-least 2 drives failure simultaneously within a given raid group.
2	Memory and CPU Processing Power	Offered Storage array should have at-least 512GB memory across both controllers. Offered storage controller shall be based upon at-least PCI 4.0 technology.
3	Host Ports and Back-end Ports	The offered Storage array shall have a minimum of 24 Front-end ports where vendor shall provide 4 dedicated ports each for connectivity of Fiber Channel, ISCSI, NVMe-of/TCP, NVMe-of/FC, NFS and IP based replication respectively. The offered fiber channel ports shall be running at 32Gbps and in future shall be upgradable to 64Gbps by replacing the SFP.
4	Operating System & Clustering Support	The storage array should support industry-leading Operating System platforms & clustering including Windows Server 2019 / 2022, VMware ESX 8.x hypervisor, HPE Morpheus VM essentials hypervisor. Red hat enterprise Linux and SUSE Enterprise Server (SLES) etc.
5	Data Availability and All Flash	1. The offered storage shall be a unified enterprise class storage array which can provide enterprise class resiliency & 100% data availability guaranteed architecture along with all NVMe controllers. 2. 100% data availability guaranty shall be clearly mentioned on vendor web site for the offered model. If vendors are not supporting the 100% data availability as per their web site then

Enterprise SAN Storage Specifications		
Sr. No	**Parameter**	**Technical Specifications**
		vendor shall quote additional Controller and 10% additional capacity as cold spare along with array for mitigating the failure situations.
6	No Single point of Failure	Offered Storage Array shall be configured in a No Single Point of failure configuration including Array Controller card,Boot drive, Cache memory, FAN, Power supply etc.
7	Disk Enclosures	1. Vendor shall ensure that all additional drive enclosures required within the given solution or achieving 2PB raw capacity shall be directly connected to offered controllers using dedicated 100Gbps NVMe-OF redundant links. 2. Vendor shall also ensure that each additional drive enclosure shall have dual node or dual controller where each node or controller shall have dedicated CPU and at least 64GB of memory.
8	Storage Encryption	1. Vendors shall offer only encrypted drives with appropriate encryption licenses. Vendor shall not offer any controller based or Software based encryption. 2. The offered Storage array shall support at-least external key managers from Utimaco ESKM and Thales Cipher Trust Manager. Vendor shall also offer internal Key manager engine for key management.
9	No. of Controllers	Storage array shall be offered with at least dual controllers where each controller shall have dual number of encrypted boot drives.
10	Architecture & Processing Power	1. Offered storage array shall be true Active-active so that every logical disk is striped across all offered drives and all drives shall be able to contribute the IOs to both controllers simultaneously. 2. Offered storage array shall have native virtualization support so that Raid can be carved out from a logical space instead of dedicating separate physical disks for each application.
11	Cloud Native data console Management	a. Common Dashboard for all managing multiple arrays through a single cloud native data console. b. Main Dashboard shall provide the information of Total number of Arrays, Volumes, hosts, Capacity and performance information of top Arrays and Volumes. c. Common role-based access control for managing multiple arrays through a single data console instead of creating users and assigning roles individually at each array. d. Common Audit management for all arrays e. Shall have capability for tagging the Storage volume to given host applications so that performance charts can be drawn for application instance for easy management and troubleshooting.

Enterprise SAN Storage Specifications		
Sr. No	**Parameter**	**Technical Specifications**
		f. Offered console shall advise about Placement of application on best fit system based on workload after application tagging. g. Shall be able to provide the context aware software updates on the storage array. h. Shall be able to offer storage management and configuration as a service instead of controlling, patching, and upgrading the management application by onsite team.
12	Cloud Enabled - Monitoring and Analytics	Cloud Enabled Monitoring and analytics engine shall have capability to provide following: a. Providing Firmware update path, previous version, readiness check before applying the update to production environment and severity level for required firmware update. b. Dashboard shall clearly highlight whether there is any issue with array and shall provide the detailed information about the issue. c. The dashboard shall provide consumption and capacity forecast trend for overall capacity planning. d. Providing granular near real time performance analysis, at-least at an interval of 5 minutes. It shall allow to create custom reports in csv and PDF format without the need for enabling extra logging, installing any appliances (physical or virtual), or installing any software. e. Providing overall headroom utilization of the array while combining and analyzing various parameters like IOPS, MB/sec, Block size, Latency etc. f. Headroom utilization shall clearly provide the breakup of headroom consumed by the Volumes or tagged application at storage array g. Providing the status of at-least top 5 volumes where latency is extremely high. It shall also provide shading functionality so that more severe hotspot can be easily identified.
13	Resource Planner	The offered Cloud native dashboard shall also provide the functionality for future workload planning on the offered storage using at least the following parameters: a. Window to provide the newer workload characteristics – Number of new volumes, type of application, Average Read and

Enterprise SAN Storage Specifications		
Sr. No	**Parameter**	**Technical Specifications**
		write IO size, Number of read and write IOPS, Capacity growth per week etc. b. The workload planner shall clearly advise whether the above additional workload characteristics can be serviced on the storage array offered. c. The Workload planner shall also provide the detailed report with workload inference.
14	Cloud Enabled - Anomaly Detection	Cloud enabled Advance Analytics engine shall have capability to provide following: a. Analytics engine shall have an overall resource contention analysis page where it shall be able to highlight the CPU and disk utilization contention and associated volumes which are causing the contention. b. Analytics engine shall have in-built anomaly detection for a given storage volume so that it can provide the variance insight of high LUN latency / response time. c. Analytics engine shall clearly mark all those anomaly detection points on the given LUN / Volume latency graph and shall be applicable for both read and write operations. d. Anomaly detection shall also be applicable for a given storage volume throughput so that drift of workload can be easily identified from the usual read and write pattern. e. Sustainability metrics reports including carbon utilization emissions and energy consumption.
15	Global Hot Spare	1. offered Storage Array shall support distributed Global hot Spare for offered Disk drives. 2. Global hot spare shall be configure as per industry practice.
16	Quality of service	1. Offered storage array shall support quality of service for critical applications so that appropriate and required response time can be defined for application logical units at storage. It shall be possible to define different service / response time for different application logical units. 2. Quality of service engine shall allow to define minimum and maximum cap for required IOPS / bandwidth for a given logical units of application running at storage array. 3. It shall be possible to change the quality of service Response time (In both milliseconds as well as Sub-milliseconds), IOPS, bandwidth specification at real time.

Enterprise SAN Storage Specifications		
Sr. No	**Parameter**	**Technical Specifications**
17	Capacity efficiency	1. Offered storage array shall support inline data efficiency engine (Supporting Thin Zero detect and re-claim, De-duplication and Compression) and shall be enabled by default. 2. Vendor shall have flexibility to enable / disable the data efficiency engine at the time of Volume creation. 3. Storage subsystem shall be supplied with Thin Provisioning, Thin Re-claim, Snapshot, remote replication, De-duplication, Compression, Performance Monitoring, and Quality of service on day 1 for the supplied capacity of the array.
18	Firmware Upgrade	Offered storage shall support online non-disruptive firmware upgrade for both Controller and disk drives.
19	Ransomware Detection	1. The offered storage shall have in-built inline data-adaptive ransomware detection engine for Block Volumes. 2. Ransomware detection engines shall be completely based upon dynamic calculation of trigger thresholds using in-built training periods and by analysing the write data path instead of using traditional approaches like measuring CPU utilization, change of data rate, data reduction efficiency ratios and data entropy. 3. It shall be possible to select a specific set of volumes or group of volumes to be enabled for Ransomware detection for block data. 4. It shall also be possible to adjust the balance between sensitivity of detection process and false positives events for effective detection process. Vendor shall provide required configurable parameters or handlers for same. 5. Ransomware detection engine shall be truly intelligent by creating an immediate creation of alert snapshots after noticing the suspicious event. 6. It shall also be possible to export the ransomware detection logs to a remote server, such as a SIEM or XDR and Call home support.
20	Snapshot / Point in time copy, No. of Volumes and Temper-proof protection (Ransomware Protection)	1. The storage array should have support for controller-based snapshots (At-least 1024 copies for a given volume). 2. The system must provide the capability to create immutable, read-only snapshots, that cannot be modified. 3. The system shall provide the capability to create compliant, read-only snapshots, which makes it impossible to modify or delete the snapshot and its base volume by the user, a system administrator, and the manufacturer. 4. The protection period of the above snapshots must be individually configurable between 1 minute and several years. Changing the system clock must not allow the tampering of protection.

Enterprise SAN Storage Specifications		
Sr. No	**Parameter**	**Technical Specifications**
21	Remote Replication	1. The storage array should support hardware based data replication at the array controller level across all models of the offered family. 2. Offered Storage array shall support both Synchronous and Asynchronous replication across 2 storage arrays natively without using any third party or software based solution. 3. Offered storage array shall have capability to create the application consistency group for replication operations. Shall have flexibility to have more than 256 volumes per consistency group. 6. Offered storage subsystem shall support incremental replication after resumption from Link Failure situation or during failback operations.
22	Active / Active Stretch Clustering	1. Offered Storage array shall have capability to provide true Active / Active Replication and Stretch clustering at metro distances for Zero RPO and RTO so that a given volume pair between primary and DR location can have concurrent access to both read and write operations simultaneously. 2. Active / Active replication shall be supported for all well-known OS like VMware, Redhat, Windows etc.
23	Multi-tenancy	Offered storage array shall be true multi-tenant and shall support at-least 128 Tenant per storage array. Every tenant shall be treated as a separate logical storage array with its own user control access.

5.3. SAN Switch:

SAN Switch Specifications	
Sr. No.	**Specifications**
Architecture/Scalability/Performance/Management/Availability:	
1	Minimum Dual SAN switches shall be configured where each SAN switch shall be configured with minimum of 24 Ports scalable.
2	Required scalability shall not be achieved by cascading the number of switches and shall be offered within the common chassis only
3	Should deliver 32 Gbit/Sec Non-blocking architecture with 1:1 performance for up to 24 ports in a energy-efficient fashion
4	Should protect existing device investments with auto-sensing 16, 32, and 64 Gbit/sec capabilities.
6	The switch should be rack mountable

SAN Switch Specifications	
Sr. No.	**Specifications**
7	Offered SAN Switch shall support less than 460 nanosecond for port to port latency with no contention.
8	Offered switch shall support at-least 2000 dynamically allocated frame buffers.
9	The switch shall provide Aggregate bandwidth of 1.536 Tb/sec.
10	Switch shall have support for web based management and should also support CLI.
11	The switch should have USB port for firmware download, support save, and configuration upload/download.
12	Offered SAN switches shall be highly efficient in power consumption. Bidder shall ensure that each offered SAN switch shall consume less than 110 Watt of power.
13	Switch shall support POST and online/offline diagnostics, including RAStrace logging, environmental monitoring, non-disruptive daemon restart, FCping and Pathinfo (FC traceroute), port mirroring (SPAN port).
14	Offered SAN switch shall support services such as Quality of Service (QoS) to help optimize application performance in consolidated, virtual environments. It should be possible to define high, medium and low priority QOS zones to expidite high-priority traffic
15	The switch shall be able to support ISL trunk up to 512 Gbit/sec between a pair of switches for optimal bandwidth utilization and load balancing.
16	SAN switch shall support to restrict data flow from less critical hosts at preset bandwidths.
17	It should be possible to isolate the high bandwidth data flows traffic to specific ISLs by using simple zoning
18	The Switch should be configured with the Zoning and shall support ISL Trunking features when cascading more than 2 numbers of SAN switches into a single fabric.
19	Offered SAN switches shall support to measure the top bandwidth-consuming traffic in real time for a specific port or a fabric which should detail the physical or virtual device.

5.4. Virtualization Software:

Virtualization Software Technical Specifications		
Sr. No	**Parameter**	**Technical Specifications**
1	Platform	The offered Hypervisor software shall be qualified for both Intel and AMD architecture and shall have capability to provide high availability.
2	Hypervisor Vendor	The offered hypervisor shall be either from Broadcom VMware, HPE, Microsoft or Nutanix.
3	Guest Operating System	The offered Hypervisor shall be supported with all leading Guest Operating Systems.
4	Availability Features	1. The offered Hypervisor shall support migration of a running virtual machine from one host to another within the same cluster with zero downtime.

Virtualization Software Technical Specifications		
Sr. No	**Parameter**	**Technical Specifications**
		2. The offered Hypervisor shall automatically restart virtual machines on another host in the same cluster in the event of an unexpected host failure within the cluster.
		3. The offered Hypervisor shall dynamically schedule the placement of virtual machines within a cluster based upon optimal workload distribution across the cluster.
		4. The offered Hypervisor shall support migration the virtual disk(s) of a running of virtual machine from one storage datastore to another with zero downtime.
5	Data Protection	1. The offered Hyper-visor Shall have in-built data backup solution which shall be able to protect VM and Hosts to Target Storage provider.
		2. Native backup engine shall be able to use at least CIFS, NFS, S3 from Storage providers as a backup target.
		3. In case vendor Hypervisor doesn't have in-built data backup solution then vendor shall provide additional backup software for the complete hardware and software configuration asked in the RFP.
		4. The offered integrated backup software shall be deeply integrated into the instances / VM provisioning window so that all newly created instances / VMs are protected and backed up automatically.
		5. The offered integrated backup software shall support critical features like Scheduling of backup, backup retention counts, on-demand backup etc.
		6. The offered Hypervisor shall support and integrate with storage - Object Buckets which can be used for Backup, Archives, Deployment and Virtual Images storage targets.
		7. It shall be possible to browse, upload, download, or delete files from Bucket and shall support all well-known object storage from AWS, Azure, Google, Dell-EMC ECS, Openstack Swifts buckets etc.
		8. The offered Hypervisor shall also allow creation of file share based NFS and CIFS protocols which can be used for Backup, Archives, Deployment and Virtual Images storage targets.
		9. It shall be possible to browse, upload, download, or delete files from File share and shall support all various file share protocols like CIFS, NFS, Local Storage and all well-known industry leading file storage arrays.
6	External Storage Integration	The offered Hypervisor shall support running virtual machines on external storage via iSCSI, NFS, and Fibre Channel
7	Automation Capabilities	1. The offered Hypervisor shall execute Bash or PowerShell scripts during virtual machine provisioning to automate system bootstrapping operations.

Virtualization Software Technical Specifications		
Sr. No	**Parameter**	**Technical Specifications**
		2. The offered Hypervisor shall also support the execution of Bash and PowerShell scripts on provisioned and discovered virtual machines like an operational workflow.
8	Identity Services	1. The offered Hypervisor shall have internal user management engine, integration with external directory-based providers – Active directory and LDAP, SAML based providers – Okta, Onelogin, Azure AD SAML etc.,
		2. It shall be possible for mapping of External integration provider users with offered hypervisor roles.
9	IP Address Management	The offered Hypervisor shall have Integration with external IPAM providers like Infoblox, phpIPAM, BlueCat, SolarWinds etc. to automate the reservation of an IP address for the virtual machine during the provisioning process.
10	DNS Integration	The offered Hypervisor shall have Integrate with external DNS providers like Infoblox, Microsoft DNS, BlueCat, SolarWinds etc. to automate the creation of DNS records for a virtual machine during the provisioning process.
11	Resource Allocation	The offered Hypervisor management engine shall have a concept of grouping of resources into a common identity, comprises of resources like Clouds, hosts, VMs, network, resource pools, data stores etc. so that required users can be assigned to it.
12	User Profile	The offered hypervisor management engine shall allow users to configure their photo, username, password, email, theme, 2FA, Linux and Windows VM login credentials from the console
13	Private Cloud Integration	The offered Hypervisor management engine shall support additional private cloud provider and hypervisor, preferably VMware, from the common interface without any additional coding.
14	Service Plans	1. The offered hypervisor Management engine shall allow administrator to create service plan or t-shirt size based on CPU, Memory and Storage and shall be available to users while creating / provisioning the instance / VMs
		2. Services plan shall also have the option to provide custom ranges and flexibility to provisioning users for providing predefined limit for number of additional volumes, customization of Volumes, number of cores etc.
15	Expansion / Shrink	The offered Hypervisor shall support both expansion and shrinking of VM cluster.
16	RBAC	Access to grouping of resources shall be controlled through appropriate roles while assigning to users. Roles shall provide access to resources using appropriate permissions. At-least, it shall be possible to configure following key permissions:
		a. Access to Native data protection configuration.
		b. Read or full access for creation of Service plans.
		c. Access to API to executes scripts on Instances / VM.

Virtualization Software Technical Specifications		
Sr. No	**Parameter**	**Technical Specifications**
		d. Access for allowing users to use Dynamic workload schedular for VM placement and pinning of VM to a specific host.
		e. Access for creating the automation scripts.
		f. Permission for resizing the instance.
		g. Access to instance / VM – Console, Adding or deleting an Instance / VM.
17	Virtual Machine Management	1. The offered Hypervisor shall support below features for Virtual Machine Management:
		a. Create / Delete / Restart / Start / Stop / Suspend and Discovery of Virtual machines.
		b. Snapshot operations – Create / Delete / revert of Virtual machines
		c. Tagging – Add / Delete / Edit tagging for Virtual Machines.
		d. Live Migration of VM, VM HA and Pin virtual machine to a specific host.
		e. Cloning of VM, Clone to VM Template.
		f. Virtual Hardware Management - Add and remove virtual hardware such as hard disks, network interfaces, CPU and memory from a managed virtual machine.
		2. The offered Hypervisor shall ensure that child snapshots of the restored snapshot are preserved instead of automatic deletion.
18	Pass through Support	1. The offered Hypervisor shall have passthrough support for PCI and NVMe devices.
		2. The offered Hypervisor shall support the passthrough support for GPU and USB devices.
19	Credential Store	The offered Hypervisor shall support both internal and external Credential store for securely pulling in the username and password, access and secret key along with key pair and SSH certificates.
20	Virtual Images	1. The offered hypervisor software shall provide the flexibility to bring / upload OS images.
		2. While uploading the OS image, it shall be possible to define the location and provide the flexibility to use internal space within the hypervisor cluster or using appropriate available S3 bucket or file share.
21	Licensing	1. Vendor shall ensure that offered Hypervisor is licensed per socket.
		2. In case vendor is not supporting the socket-based licensing then vendor can configure Core based licensing as well however vendor shall provide at-least 128 core license per configured physical server or actual provisioned cores per server, whichever is higher.

Virtualization Software Technical Specifications		
Sr. No	**Parameter**	**Technical Specifications**
22	Upgrade	1. It shall be further possible to upgrade the offered Hypervisor to full-fledge Cloud management platform so that all required functionality of Cloudops (Cloud operations for VM, and Container platforms), SecOps (Security and Control), Devops (Automate and Orchestrate) and Finops (Visualize and optimize) can be achieved with appropriate RBAC controls.
		2. After upgrading the Hypervisor to full-fledge cloud Management, it should become truly heterogenous and shall quickly integrate with below tools / Platforms / integrations:
		a. Hypervisors: VMware, Nutanix, HPE VME, Microsoft etc.
		b. Clouds: AWS, Azure, GCP, IBM, Oracle, Alibaba, Digital Ocean, Openstack etc.
		c. Identity: Active Directory, Okta, SAML, LDAP, Onelogin etc.
		d. Network: NSX, ACI, Infoblox, Bluecat, SolarWinds etc.
		e. Load Balancers: F5, A10, Citrix, ALB, Azure Load Balancer etc.
		f. Backup: Native Backup functionality, Veeam, Commvault, Zerto etc.
		g. ITSM: ServiceNow, Cherwell, BMC-Remedy etc.
		h. Container – AKS, EKS, GKE, Kubernetes, KVM cluster etc.
		i. Automation – Chef, Puppet, Ansible, Ansible tower, VMware Orchestrator etc.
23	Global Search	The offered Hypervisor shall provide global search to facilitate search of Instances, Users, cloud, group, hosts and networks.
24	Wiki	The offered Hypervisor shall allow creation of Wiki, which shall be RBAC-controlled, auditable Wiki that allows easy access to information, notes, configurations or any other data needed to be referenced or shared with others.
25	Dashboard	Consolidated dashboard for the offered Hypervisor shall highlight the overall environment status, System Status, Alarms, log history, Instance status, Instance status by configured clouds, cluster workloads etc.
26	Activity Report	1. The offered Hypervisor management engine shall provide activity report like provisioning tasks , Users related tasks etc.
		2. It shall be able to search the specific activity.
27	Image Conversion / Migration	The offered Hypervisor shall support conversion of VMware image to offered Hypervisor supported image format from the VM Migration perspective. Vendor shall provide this functionality either natively to offered Hypervisor management engine or shall factor additional software on Day 1 to achieve it.
28	Multi-Cluster Management	Vendor shall provision required management software for managing multiple clusters, at least 10 clusters, on day 1 for the offered configuration.

5.5. Backup Appliance and Software:

Purpose Built Backup Appliance	
Parameter	**Minimum Specification**
General Features	The offered purpose-built backup appliance should be sized appropriately for backup of front-end data of 600 TB (40% DB & 60% VM & File System) as per below mentioned backup policies: a. Daily incremental backup – retained for 4 weeks in the backup appliance. b. Weekly full backup for all data types – retained for 4 weeks in the backup appliance. c. Monthly full backup – retained for 12 months in the backup appliance. d. Yearly full backup - retained for 5 years in the backup appliance. The proposed purpose-built backup appliance must be sized for adequate capacity considering 2% daily data change rate for the contract period. Any additional backup storage capacity, software and any other component required as per sizing needs to be provided by the MSI and OEM at the time of bid. Bidder must provide the backup appliance sizing on OEM's letter head with seal & sign from the authorized signatory basis the backup retention policies.
	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.
	Must support Inline and Global data de-duplication technology (without excluding any file/part thereof) at block level using variable block length technology
	VTL Appliance must support High Availability of multiple components like Controller, CPU, FAN, backup storage, network and FC ports etc. without single point of failure for any component. The dual controllers must be active-passive so that the performance does not degrade even in case of controller failure.
Feature	PBBA VTL Appliance should be configured with RAID 6 or DDP or equivalent along with hot spare disks.
	The proposed appliance must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism. All file system data and Metadata must be verified continuously even if parts of the file system are never accessed for reads (Automated Data Scrubbing Process)
	The proposed appliance must provide a mechanism to restrict any date and time change of the system to protect against any accidental or intentional expiration of data through change in the Network Time internally or externally to the system

Purpose Built Backup Appliance	
Parameter	**Minimum Specification**
Feature	As PBBA VTL Appliance, solution 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.
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.
Feature	Software Licensing:
Feature	LAN/SAN Connection: Minimum 8 x 10/25 Gig SFP+ (fully populated) along with 8 x 32Gbps FC ports with all required accessories.
Feature	PBBA VTL appliance should have support for Encryption, Deduplication and Replication (Replication from appliances to appliances over TCP/IP network) from Day1.
Feature	PBBA should have manual/Automated Data Integrity check for backup data on device
Feature	The proposed appliance should be able to deliver a throughput of up to 75 TB/hr (at target side) Or more, considering with/without deduplication and compression ratio. Deduplication and compression must be ensured at source and target/backup appliance end.
Feature	Scheduling:
	a. Backup software used in PBBA should be able to retrieve data from tape to client server directly.
	b. logs & reports e.g. de-duplication report, Data growth analysis report, Compute utilization report during backup etc.
Feature	PBBA based backup solution should support following replication capabilities:
	a. Subsequent Replication should transfer only difference data from previous successful replication.
	b. Replication should provide the flexibility to transfer only dedup data.
	c. should provide compression of data while replication.
	d. Proposed appliance should support bi-directional, many-to-one, one-to-many, and one-to-one replication.
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.

Purpose Built Backup Appliance	
Parameter	**Minimum Specification**
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
Protection & retention	Proposed appliance should support retention lock/retention/ Immutability feature or any other to ensure that no data is deleted/overwritten accidently and support for point-intime copies of a LUN or volumes with minimal performance impact.
Updates and patch support	Software updates and patches: For the period of minimum 5 years and as per scope of this RFP.
Warranty& Post warranty Support	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support and 2 years post warranty support as per Haryana States' CAMC/AMC policy

5.6. Backup Software:

Backup Software	
S.No.	**Minimum Specifications**
1	The proposed Backup software must offer instance-based licenses with no restrictions on type of arrays (protecting heterogenous storage technologies), front end production capacity or backup to disk target capacity restrictions.
2	Backup software should have Capability to do trend analysis for capacity planning of backup environment, extensive alerting and reporting with pre-configured and customizable formats. Any specialized reporting modules needed must be quoted along with associated hardware to achieve this functionality. All necessary hardware resources required to run this module should be supplied.
3	Proposed solution should support 24x7 real-time monitoring, with at-a-glance and drill-down views of health, performance and workload of the virtual hosts.
4	Proposed solution should have security and compliance dashboard inbuilt with the product.
5	Proposed solution should support automated action for popular alarms (automated or semi-automated), with at-a-glance and drill-down views of health, performance and workload of the virtual hosts.
6	Software should be able to restore VMs to a cloud service provider like AWS, Azure or Google directly from the backup copy.
7	Software should be able to extend the backup repository to a public cloud service provider by moving older files to any S3 Compatible Object storage or Azure BLOB repositories.

8	Backup software should should have capability to archive data to Amazon Galcier or Microsoft Azure storage Arhive Tier or any S3 Storage. The Software must have capability to restore the data from archive tier, it should not be dependent on cloud vendor.
9	Backup software should support agentless backups of applications reisding in VMs like SQL, Exchange, Sharepoint, Oracle, etc. with non-staged granular recovery of all these applications. It should support crash consistent VM level backup for all other workloads. Backup software should support SAP HANA backup integrated with HANA Cockpit
10	The software must has the functionality to backup on-prem data directly into cloud repositories such as AWS S3 or Microsoft Blob.
11	Proposed backup software should be able to leverage Immutable Cloud based storage like S3-Immutable service to prevent backup copies of data from any corruption or ransomware attacks.
12	The proposed soloution should have on demand scans available for malaware attacks.
13	The backup Software must have inline detection & in guest detection via guest indexing against any malware attacks.
14	The proposed backup software should have four eyes apporval for any backup deletion.
15	Backup software should be a Hardware Agnostic software and it should support snapshot integration with hypervisors like VMware, Hyper-V, Nutanix AHV nad RHEV and support de-duplication on any storage target. It should be able to backup data to tapes (like LTO) or as well for long term retention on S3 storage.
16	The proposed backup software should provide Instant recoveries for any backup to Vmware or Hyper-V or Acropolis Virtual machine.
17	Backup software should support file level recovery from any backup of any VM or physical server. It should support a full system recovery in case of a system crash, either on a physical system or virtual machine or as a Cloud Instance(AWS, Azure or Google)
18	The Proposed backup Software should support Syslog and Service Now integration.
19	Backup software should support instant database recoveries of MS SQL and Oracle from the backup files.
20	Backup software should support Multi factor authentication for accessing Backup console and console auto log-off functionality.
21	Backup software must have a feature of data validation, whereby a workload (VM with OS and application) is powered-on in a sandbox environment and tested for its recoverability.
22	Recovery verification should automatically boot the server from backup and verify the recoverability of VM image, Guest OS and Application Consistency and then publish automated reports to be used in backup / recovery audits.
23	Backup software should provide Backup and Replication capabilities in one console only and also allow users to integrate with RBAC capabilities of the hypervisor, so that users can initiate backup and restore only those VMs to which they have access, without administrator intervention, thereby delivering self serve capabilities.

24	Proposed backup software should be able to Hardened the Linux Repository. This service will prevent backup copies of data from any corruption or ransomware attacks.
25	The software should support Group Managed Service Accounts which should have an option to users to allow change passwords after every 30 days and allows for complex password policy.
26	The proposed backup should have object storage backup.
27	Proposed backup software should have the ability to perform staged restores to enable admins to comply to regulations by selectively deleting files / records which should not be restored from the backup copies. This will help in complying to "right to be forgotten" regulations like GDPR, where user data is deleted from restored backup copies in an auditable manner.
28	The proposed Backup software must allow to configure the maximum acceptable I/O latency level for production data stores to ensure backup and replication activities do not impact storage Availability to production workloads.
29	Backup software should provide Recovery of Application Items, File, Folder and Complete VM recovery capabilities from the image level backup within 15Mins RTO.
30	The software should be Network-efficient, Secure backup data replication with variable-length encryption at the source, along with compression and encryption to ensure that backups are optimized for WAN transmission. This should be ensured with or without need of any other 3rd party WAN Accelerator requirements.
31	Bidder need to provide the 40VM license. Backup software should support for Virtual machine and volume backup.

5.7. SSE:

SN	Technical Specifications & Functional Requirement
1	The proposed SSE solution must be cloud native platform and the OEM should have services hosted in at least 2 Meity-empanelled cloud service provider's data centres in India.
2	The proposed SSE solution must have SWG, CASB Inline, Browser Isolation and ZTNA capabilities from day 1.
3	The Bidder must propose the above solution from a single OEM and the OEM must be a leader in SSE Gartner Magic Quadrant in the last 2 years consecutively.
4	The proposed solution should support integration with ADFS, Microsoft Azure AD and multiple other leading identity providers that support standard-based SAML 2.0 Identity Provider capability for user authentication.
5	The solution provider must be certified against internationally recognized government and commercial standards - frameworks such as ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC 2 and CSA - Star
6	The proposed solution must have the following ways to steer traffic to the cloud service - Agent based option - IPsec Tunnel

SN	Technical Specifications & Functional Requirement
	- Proxy PAC File
7	The solution must provide a dedicated data plane in the cloud where each user/application data transaction is processed through the cloud components which. are dedicated to <Name of the cutsomer>. Bidder to confirm the same by submitting a supporting document from the SSE vendor.
8	The solution provider must provide secure access to all RFP features from a single software agent.
9	All the mentioned SSE services in the RFP must be delivered from a single management and configuration console. The Management, Control, Data and Logging planes of the SSE service must be hosted in India for <Name of the cutsomer>.
10	The bidder must ensure the proposed SSE platform has a built-in 1 year log retention for all the SSE services mentioned in the RFP. If this is not the case, bidder to factor additional analytics tools and log storage as part of their solution to meet the requirement. The support and warranty period and SLA's for any additional tool must be the same as the SSE platform.
11	The SSE agent must have a password protection to prevent users from uninstalling the agent without the password.
12	The OEM support shall be 24x7x365 and allow support calls to be raised through web portal at any time schedule.
13	The solution must have Premium Support and include Customer Success Manager and Customer Success Engineer assistance.
14	The proposed solution must have an uptime of 99.999 per cent per month for all proposed services/security engines.
	Secure Web Gateway
1	The solution must support both a tunnel and proxy deployment modes to secure internet traffic. The solution must be able to provide SSL inspection/Decryption at scale for all the internet bound HTTPS traffic.
2	The solution must be able to secure access to all HTTP and HTTPS traffic on well known ports 443, 80 and customer ports such as TCP 8700, etc. The solution must support capability to apply controls to allow/restrict websites on custom ports.
3	The solution must have granular options to define the access policies. The options must include user based, group based, service based, application based, network based and device posture based policies.
4	The SWG must have granular category based web controls for controlling access to Adult, Hacking, Cryptocurrency, Malware, Phishing, Parked, Grayware websites. The SWG must have alteast 70 predefined categories for URL filtering.
5	The SWG must have a phishing prevention capability. It must have the feature to identify user's corporate credentials and prevent them from being submitted to those internet websites which are allowed in the organization as per the business requirement, but user's are not not authorised to be logged-in with corporate credentials. The admin must have flexibility to enable this capability for selective categories.
6	The SWG must have firewall capabilities to secure internet traffic on all TCP and UDP ports. It must allow admin to create alteast 500 firewall rules/policies and support policies based on application signature/ID's and user identities.

SN	Technical Specifications & Functional Requirement
7	The SWG must provide a dedicated Public IP address to <Name of the cutsomer> at each Cloud Compute location to redirect specific Government/Other Internet Websites via these Dedicated Egress IP's.
8	The SWG must have inline Advance Threat Protection (ATP) for the Internet and SaaS applications. The inline Malware prevention must prevent file based malware also from being downloaded. The solution must be able to prevent malware downloads on both HTTP and HTTPS websites. The sandbox must support multiple filetypes including PE, DMG, MS Office, PDF, Script, etc.
9	The SWG should prevent fileless malware such as javascript, powershell, shell scripts, ELF.
10	The SWG should be able to prevent unknown phishing websites that use phishing kits or stealthy techniques such as cloaking, website cloning.
11	The SWG should prevent phishing attacks using known Saas platforms such as Onedrive, Wix, Wordpress, Google Drive etc.
12	The SWG must have Advance DNS Security control to prevent DNS based attacks such as DNS tunneling, Domain Generation Algorithms, DNS based exfiltration, Command & Control.
13	The SWG must prevent advanced DNS techniques such as Strategically aged domains, Slow/Ultra Slow tunneling, Dictionary DGA etc.
14	The SWG DNS Security functionality should support enforcing sinkholing for malicious DNS requests to identify the actual source. It must also prevent DNS attacks on DoH (DNS over HTTPS), DoT (DNS over TLS). Additionally it must provide control to block or allow DoH/DoT.
15	The SWG must have advance Sandbox capbilitie to prevent zero-day attacks. The Sandbox must support multiple filetypes including but not limited to archives, executables, msoffice files, Script (BAT, JS, VBS, PS1, and HTA) files , JAR Files, Archive (RAR, 7-Zip, ZIP) files, pdfs and other web content like adobe flash, java applet, ELF, DMG and HTML.
16	The solution should have the capability to ingest IOC's from external sources.
17	The solution must have File Type control to prevent download of risky file types in the organization. The file type control must support alteast 200 filestypes.
18	The solution must have Isolation capabilities to allow risky website access with granular conrols like copy-paste restrictions, Screenshots controls, etc. This capability must be supported for all SWG users.
19	The SWG must have capability to block TOR and TOR Bridges, control unknown-tcp and unknown-udp based applications, protection from spyware, command & control, botnet, toolbar based threats. The solution should have a dedicated Ransomware protection.
	Cloud Access Security Broker
1	The solution must have detailed risk info of SaaS applications including capabilities, certifications and compliances and support a schedule based risk report.
2	The CASB must support 70,000+ cloud applications for a better visibility and control.
3	The CASB must support tenant restrictions on multiple applications including O365, Gmail, Github, Dropbox, etc. to restrict access to only authorized corporate tenant.

SN	Technical Specifications & Functional Requirement
4	The CASB must provide granular control for SaaS applications. The controls should include upload, download, allow, block, chat, streaming, share, delete, edit, etc. controls for different applications.
5	The CASB must support controls for AI applications such as ChatGPT with restrictions for uploading/posting sensitive data.
6	The CASB must support specific function based controls such as upload,download,sharing,editing. Examples - Dropbox upload, teams download/upload, github posting / copilot etc
7	The CASB must support dynamic application based control Office 365, Zoom, Webex, Teams, WhatsApp, etc. SaaS applications which are being accessed through thick clients of the respective SaaS application.

5.8. NextGeneration Firewall

Technical Specifications for NFGW		
S.No.	**Features**	**Details**
1	**Hardware Architecture**	The solution should provide firewall, AVC, IPS, Anti-Virus, Anti-Spyware, Anti Malware, File Blocking and DNS Security functionality in a single appliance from day one.
		Firewall must support zero-downtime inline policy changes without re-installation or full policy push. The hardware platform & Firewall with integrated SSL and IPsec.
2		The appliance should support atleast 8 *10G RJ45, 8 * 10G and 4 * 25G ports from day one loaded with SR modules
3		The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory and should support minimum of 32 GB of RAM
4		Proposed firewall should not consume more than 1RU of rack space
5	**Performance & Scalability**	Should support 10 Gbps of Thread prevention throughput (firewall, AVC, IPS Anti-Virus, Anti-Spyware, Anti Malware, File Blocking, DNS Security) real- world / production / Enterprise Testing performance / Or with app mix.
6		NGFW Firewall should support at least 20 M concurrent sessions on TCP or 2 M concurrent sessions on http
7		NGFW Firewall should support at least 2,000,000 connections per second on TCP or 200,000 connections per second on http
8		Firewall should support redundant power supply
9		Firewall should support multiple fans
10	**HA Capability**	High Availability Configurations shall support Active/ Passive or Active/Active-Clustering
11	**NGFW Feature**	
12		Firewall should support static nat, dynamic nat, dynamic pat
13		Firewall should support NAT functionality
14		Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6

Technical Specifications for NFGW		
15		Should support Multicast protocols like IGMP, PIM, etc
16		Solution should support PBR based on parameter likes source port, destination address, destination port, protocol, applications, or a combination of these objects. Also PBR / equivalent policy should rely on flexible metrics, such as round trip time, jitter, mean opinion score, and packet loss of the interfaces to identify the best routing path for its traffic
17		Should support capability to integrate with other security solutions to receive contextual information like security group tags/names
18		Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.
19		Should support more than 5000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency
20		Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.
21		Should support more than 21,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where multiple rules/event can be combined together for better efficacy
22		Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.
23		Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.
24		Should be capable of detecting and blocking IPv6 attacks.
25		Solution should be able to identify, decrypt, and evaluate both inbound & outbound Secure Sockets Layer & Secure Shell Protocol traffic on-box
26		Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control
27		The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor
28		Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist
29		Must able to do real-time inspection of both the DNS request and DNS response can stop DNS hijacking attacks in real time. Solution should perform Inline inspection to protect from DNS threats such as DNS Tunneling, DNS Sinkholing, DNS Hijacking, DGA,Domain Shadowing, DNS Injection attacks, Compromised DNS registrar

Technical Specifications for NFGW		
		analysis, DNS Spoofing, DNS Cache Poisoning and DNS Spoofing etc. All the DNS features can be provided natively or using 3rd party solution for at least 1 billion DNS request
30		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.
31		The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).
32		Should be able to identify attacks based on Geo- location and define policy to block on the basis of Geo-location
33		The 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.
34	**URL Filtering Features**	Should must support URL threat intelligence feeds to protect against threats
35		Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than million of URLs in more than 70 categories.
36		The NGFW to support English, Hindi and regional languages for URL and IP database to fulfill web security needs as per Indian cybersecurity needs.
37	**Other Capabilities**	Solution shall have capability to analyze and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN and FTP
38		Must have required subscription AVC, IPS, Anti-Virus, Anti-Spyware, Anti Malware, File Blocking and DNS Security from day1.
39		The management platform must be accessible via a web-based interface and ideally with no need for additional client software. The proposed firewall solution must support full-featured local policy creation, modification, and on any external centralized management system deployment directly from the firewall device without reliance
40		The management platform must be a dedicated OEM appliance or VM running on server
41	**Management , Reporting and Logging**	Solution must support policy audit trails and change history available locally on each firewall device.
42		The management platform must provide a highly customizable dashboard.
43		The management platform must provide centralized logging and reporting functionality
44		The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows

Technical Specifications for NFGW		
45		The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.
46		Should support troubleshooting techniques like Packet tracer and capture
47		Should support REST API for monitoring and config programmability
48		The management platform must provide multiple report output types or formats, such as PDF/ HTML/CSV.
49		The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e- mail, SYSLOG).
50		Firewall internal GUI management and management GUI platform should show unused policy and capabilities and turn them on with best practices, to understand gaps in configuration best practices, recommendations to close security gaps, detect hardware and software system issues.
51		Solution should be able to provide insights of hosts/user on basis of indication of compromise, any license required for this to be included from day one
52		The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports. The proposed Management platfrom solution must provide a mechanism to identify rules that are not being used or have not been hit by any traffic.
53		The management platform support running on- demand and scheduled reports
54		The management platform must risk reports like advanced malware, attacks and network
55		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.

5.9. Anti DDoS

Component / Performance / Utility	Minimum Specification
Generic	
	Appliance based Solution
	Inspection and prevention should be done in hardware.
	Solution must support VLAN's

	Solution must support at least 8 x 1GE Copper interfaces & 4 x 1GE SFP Interfaces from day one
	Solution must at least support 8 Gbps of total traffic
	Solution must have both copper & fiber interfaces.
	Operating system should be hardenend
	The device should support high availability
	Device management interface must be firewalled internally.
	System must be delivered as a single-box solution. This box must be rack-mountable in standard 19" rack.
	Performance should not be limited by any licensing system.
	In inline mode system must not modify MAC or IP addresses of passed frames
	Latency should be lower than 70 microseconds
	The solution shall support IPV6 protocol.
	The DDoS detection capability of the solution must not be impacted by asymmetric traffic routing.
	The system must detect the attack dynamically without the need of any static control/redirection (E.g. route maps or static routes)
	The system must support an updated threat feed that describes new malicious traffic (botnets,phishing, etc...).
	The system should be capable to mitigate and detect both inbound and outbound traffic.
	The DDoS detection solution shall have the learning mode to easily identify anomalies in the network communication.
Security	
	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
	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
	The system must limit number of simultaneous TCP connections on a per-client basis
	DNS Flood Mitigation using following mechanisms DNS Query-Response matching, DNS Query/MX/ALL/ZT/fragment/ per-Source Floods, DNS Query Source validation, DNS Unexpected Query, Unsolicited DNS Response Flood,DNS Response cache under flood, DNS Query TTL checks, DNS-specific ACLs, DNS Header anomaly prevention,
	Should support minimum 2 Million DNS Queries per second

	Local Address Anti-spoofing
	Adaptive Threshold Estimation and System Recommended Thresholds
	The system must enforce minimal request speed for HTTP and SSL/TLS
	The system must allow protection parameters to be changed while a protection is running. Such change must not cause traffic interruption
	Solution should support security at layers 3,4 and 7
	Solution should support for all 255 protocols at layer 3
	Solution should support all 64k TCP and UDP ports
	System must not use signatures, System must have methods of using behavioural and heuristic analysis
	System must detect and block HTTP Opcode Flood
	System must detect Excessive URL/source/second
	System must be able to detect and block SYN Flood attacks
	System must be able to detect and block Zombie Floods
	System must be able to detect and block ICMP Floods
	System must be able to detect and block Fragment Flood
	System must be able to detect and block HTTP GET Flood
	System must be able to detect and block Floods from Unwanted Geographical Areas
	Slow HTTP requests (from tools like Slowloris, RUDY, Slowread)
Deployment Options	
	Inline :- The DDoS appliance should support 'inline', meaning it is installed between the one or more protected systems and the rest of the network. In the simple network , data passes through the DDoS appliance as it travels to and from a protected system and the rest of an Ethernet local area network.
Protection Mechanism	
	DDoS Appliance should be completely Behavourial Based
	It should measures byte and packet counts, state transitions, fragments, checksum, flags, new connections, address pairs, and so on as Layer 3 to Layer 7 parameters to define Threshold
	DDOS should not work on fix thresholds .It should continuously learns traffic patterns for a large group of layer 3, 4, and 7 parameters in both directions.
	In case of threshold violation traffic should be drop
	It should be possible to write manual ACL's to block certain IP
	It should be possible to block Geographical Locations to prevent flooding attacks from a particular country
	Should provide inspection NTP Query and Response traffic
	Should support integration through RESTful API
High Availability & ByPass Protection	

	It should support Hardware Bypass for Copper Interfaces available on Unit.
Load Balancing to Increase Througput	
	DDoS appliance should support Load Balancing Mechanism to increase througput
	Load Balancing can be achieved by using a External Load Balancer which supports Load Balancing on bidirectional or unidirectional hashing algorithm
	Load Balancing can also be achieved using a External Layer2 Switch using LACP
Management	
	The system must support configuration via standard up to date web browsers. System user interface must be based on HTML without any third-party plugins such as ActiveX, Java or Flash
	The system must support the generation of PDF and e-mail reports
	System must support CLI access over RS-232 serial console port, SSH.
	Dedicated management port
	Management interfaces must be separated from traffic interfaces. System management must not be possible on traffic interfaces, management interfaces must not switch traffic
	Management interface must be firewalled (e.g. only allow SSH from IP x and HTTPS from IP y).
	System must have concept of users / groups / roles
	Management certificate must be possible to change
	Should support TLS 1.3 Management Logging

5.10. L3 Network Switch

LAN Switch (48-Port)		
S#	Parameter	Requirement / Specification
1	General Requirement	a) Should support non-blocking Layer 2 switching and Layer 3 routing.
		b) Should support the complete STACK of IPv4 and IPv6 services.
		c) Switch Should have the capability to function in line rate for all ports
2	Interface Requirement	a) Minimum 48 ports support 1/10/25 Gbps SFP/SFP+ ports for host connectivity and Minimum 6*40/100G QSFP 28 ports each supporting native 100Gig Ethernet. The switch should be populated with 24*10G fibre transceiver and 24*10G copper transceiver for downlink connectivity & 2*40/100G for uplink connectivity.
		b) Switch should have fixed management interface console / port for local management & out of band management.

LAN Switch (48-Port)		
3	Chassis & Power Supply	a) Switch should have redundant power supply & fan.
		b) **Switch should be deployed in HA (Active Active) from day one .**
		c) All components should be hot swappable.
		d) The switch shall be rack mountable and be supplied with proper rack mount kit to mount.
4	Performance	a) Modular OS with dedicated process for each routing protocol
		b) Switch should re-converge all dynamic routing protocol at the time of routing update changes i.e. Graceful restart for fast re-convergence of routing protocols (OSPF, BGP)
		c) Switch should support VRF instances with route leaking functionality
		d) The switch should support LPM routes
		e) The switch should have MAC Address table size of at least 64k
		f) The switch should support multicast routes
		g) Switch should support VLANs
		h) Switch should support ECMP paths
		i) Switch should support minimum 2 Tbps of switching capacity
5	Network Virtualization Features	a) Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN
		b) Switch should support VXLAN and EVPN IRB for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data center
6	Layer2 Features	a) Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S)
		b) Switch should support VLAN Trunking (802.1q)
		c) **Switch should support MAC addresses table size of 64K or Higher**
		d) Switch should support VLAN tagging (IEEE 802.1q)
		e) Switch should support IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy
		f) Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures
		g) Switch should support layer 2 extension over VXLAN across all Data Centre to enable VM mobility & availability
		h) The Switch should support DC Bridging i.e. IEEE 802.1Qbb Priority Flow Control (PFC), IEEE 802.1Qaz Enhanced Transmission Selection (ETS), Explicit Congestion Notification (ECN).
		i) Maximum number of port channel / link aggregation should be 48.
		j) Maximum no of ports in the port channel / link aggregation should be 16/32.
		k) The switch should support BGP EVPN Route Type 2/3 and Route Type 5 for the overlay control plane.

LAN Switch (48-Port)		
7	Layer3 Features	a) Switch should support static and dynamic routing
		b) Switch should support multi instance routing
		c) Switch should support multicast traffic reachable
		d) Switch should support multicast source discovery protocol (MSDP) **/ equivalent protocol.**
		e) Switch should support IGMP v2 and v3
8	Quality of Service	a) Switch system should support 802.1P classification and marking of packet using: CoS (Class of Service) and DSCP (Differentiated Services Code Point)
		b) Switch should support for different type of QoS features for real time traffic differential treatment using: Weighted Random Early Detection / Deficit Weighted Round Robin or equivalent
		c) Switch should support Rate Limiting - Policing and/or Shaping
		d) Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy
9	Security	a) Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy
		b) Switch should support for external database for AAA using:
		Ø TACACS+, RADIUS
		c) 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
		d) VXLAN and other tunnel encapsulation/decapsulation should be performed by switch.
		e) Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined.
		f) Switch should support DHCP Snooping.
		g) Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.
		h) Switch should support IP Source Guard/lockdown to prevent a malicious host from spoofing or taking over another host's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN.
		i) Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port.
		j) Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities.
		k) The Switch should support LLDP.
		l) Switch should support Spanning tree BPDU protection
10	Manageability	a) Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail
		b) Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures

LAN Switch (48-Port)		
		c) Switch should provide remote login for administration.
		d) Switch must have Switched Port Analyzer (SPAN) with minimum 4 active session and ERSPAN on physical, Port channel, VLAN interfaces
		e) Switch should support for management and monitoring status using different type of Industry standard NMS using:
		a. SNMP v1 and v2, SNMP v3 with Encryption
		f) Switch should provide different privilege for login in to the system for monitoring and management
		g) Should have Open APIs/REST APIs to manage the switch either through remote- procedure calls (JavaScript Object Notation [JSON] or XML) over HTTPS or should support puppet for management and automation purpose
		h) The Switch should support monitor events and take corrective action like a script when the monitored events occurs.
		i) Should support hardware telemetry.

5.11. Server Load Balancer

Sl.no	Technical Specifications
	Server Load Balancer
1	The proposed OEM should be Parent Technology OEM(Should NOT be Whitelabled or Co-branding or 3rd Party Technology or Open Source or Reseller Agreement).
2	The proposed appliance should be a dedicated appliance, it should not be part of any Firewall or UTM. There should not have any option to import 3rd party software on proposed appliance.
3	**Traffic Ports:** 2 x 10G SFP+ and 8 x 1G RJ45 (Break-Out should not be used) **L4 Throughput:** 5Gbps and scalable upto 20Gbps **Layer 7 requests per second:** 250,000 **RSA CPS (2K Key):** 7,000 **ECC CPS (EC-P256):** 4,000 with TLS1.3 Support **Concurrent Connections:** 20 Million * Data should be publically available
4	The solution must be able to decrypt SSL web traffic between clients and web servers

Sl.no	Technical Specifications
	Server Load Balancer
5	**The proposed appliance should support the below metrics:** – Minimum Misses, – Hash, – Persistent Hash, – Tunable Hash, – Weighted Hash, – Least Connections, – Least Connections Per Service, – Round-Robin, – Response Time, – Bandwidth, etc
6	**Following Load Balancing Topologies should be supported:** • Virtual Matrix Architecture • Client Network Address Translation (Proxy IP) • Mapping Ports • Direct Server Return • One Arm Topology Application • Direct Access Mode • Assigning Multiple IP Addresses • Immediate and Delayed Binding
7	The proposed Hardware must have Bandwidth Mangement feature from Day 1
8	Device must have Dynamic routing protocols like OSPF, RIP1, RIP2, BGP from Day 1
9	The proposed device should support standard VRRP (RFC - 2338) for High Availability purpose (No Propertary Protocol). Other mode like Switch HA Mode, Extended HA Mode and Service HA Mode should also be supported.
10	The solution should support IPv6 as well as IPv4 and have the ability to turn IPv4 traffic to IPv6 traffic on the backend
11	Should have ability to upgrade/downgrade device software Images.
12	The solution should support link aggregation for bonding links to prevent network interfaces from becoming a single point of failure
13	Should support HTTP/2 and HTTP/3
14	Supports SSL offload for the following protocols: – HTTPS – Generic SSL – SIP – SMTP (STARTTLS)* – IMAP (STARTTLS)* – POP3 (STARTTLS)* – LDAP (STARTTLS)* – FTPS*
15	Appliance should support Local Application Switching, Server load Balancing, HTTP, TCP Multiplexing, Compression, Caching, TCP Optimization, Filter-based Load Balancing, Content-based Load Balancing, Persistency, HTTP Content Modifications

Sl.no	Technical Specifications
	Server Load Balancer
16	The proposed device should support Content-Intelligent Cache Redirection: • URL-Based Cache Redirection, • HTTP Header-Based Cache Redirection, • Browser-Based Cache Redirection, • URL Hashing for Cache Redirection, • RTSP Streaming Cache Redirection
17	Supports the following health check types: • Link Health Checks, • TCP Health Checks, • UDP Health Checks, • ICMP Health Checks, • HTTP/S Health Checks, • TCP and UDP-based DNS Health Checks, • TFTP Health Check, • SNMP Health Check, • FTP Server Health Checks, • POP3 Server Health Checks, • SMTP Server Health Checks, • IMAP Server Health Checks, • NNTP Server Health Checks, • RADIUS Server Health Checks, • SSL HELLO Health Checks, • WAP Gateway Health Checks, • LDAP/LDAPS Health Checks, • Windows Terminal Server Health Checks, • ARP Health Checks, • DHCP Health Checks, • RTSP Health Checks, • SIP Health Checks, • Virtual Wire Health Checks, • DSSP Health Checks, • Script-Based Health Checks, • Cluster-based Health Checks,
18	The Solution should support native integration with Kubernetes Platforms and controller/connecter/plugin should operate within Kubernetes Cluster to automatically create service on Load Balancer. The controller/connecter/plugin should also support automatic creation, edition and deletion of service like VIP creation, Node/Real Sever Creation, Farms/Group Creation, SSL Binding etc.
19	The controller/connecter/plugin should support at least three components with different task as follows: a. A Controller which should discovers the service objects in the Kubernetes clusters. b. An Aggregator which should aggregates inputs from all the controllers and communicates the necessary configuration changes to Configurator. c. A Configurator which should prepare a load balancing configuration file and pushes it to the device.
20	The solution should support automatic renewal of SSL Certificate via integration with 3rd party Certification Authority such as Lets Encrypt
21	Should support for IPv4 and IPv6 traffic along with DNS functionality from day-1
22	Device should be accessed through the below: • Using the CLI, SSH, SCP • Using SNMP • REST API • Using the Web Based Management

Sl.no	Technical Specifications
	Server Load Balancer
23	**Solution should provide from day1:** Application Dashboard Per Application Analytics SLA Breakdown (Network, per server) SSL Statistics (handshake and cypher breakdown, rejected handshake) SSL CPS System Dashboard Network Dashboard **Option for future use:** L4 Events Per transaction type events (delay, user agent, response, headers) SSL Events (type of handshake, cypher, TLS version)
24	Bidder should propose Centralized Management & Reporting Solution from Day 1.
25	The proposed solution should be EAL2 certified. OEM should be ISO 9001, ISO 14001, ISO 45001, ISO 28000 certified.
26	Customer may ask for the demonstration of specific or all features if required.

5.12. Virtual Web Application Firewall

Sl. No.	Technical Specifications
	Virtual Web Application Firewall
1	The proposed OEM/Subsidiary should be Parent Technology OEM(Should NOT be White labled or Co-branding or 3rd Party Technology or Open Source or Reseller Agreement).
2	The proposed solution of WAF should be a dedicated solution, it should not be part of any Firewall or UTM. There should not have any option to import 3rd party software on proposed solution.
3	The vWAF shall be entirely Software based and shall support virtualization platforms like VMware ESXi, Hyper-V, KVM, OpenStack etc
4	The vWAF shall be able to run both IPv4 & IPv6 simultaneously (Dual Stack) from day one.
5	**The proposed appliance should support the below metrics:** — Minimum Misses, — Hash, — Persistent Hash, — Tunable Hash, — Weighted Hash, — Least Connections, — Least Connections Per Service, — Round-Robin, — Response Time, — Bandwidth, etc

Sl. No.	Technical Specifications
	Virtual Web Application Firewall
6	**Following Load Balancing Topologies should be supported:** • Virtual Matrix Architecture • Client Network Address Translation (Proxy IP) • Mapping Ports • Direct Server Return • One Arm Topology Application • Direct Access Mode • Assigning Multiple IP Addresses • Immediate and Delayed Binding
7	Shall have minimum 1Gbps throughput per instance.
8	Shall support one-arm and two-arm mode deployment mode.
9	Shall have minimum 8 Million concurrent connection per instance
10	Shall have minimum 300K L4 connections / second.
11	Shall have minimum 400K L7 Requests / second.
12	Shall support IPv4 to IPv6 address translation and vice-versa.
13	The solution must be able to protect both HTTP Web applications, SSL (HTTPS) web applications & Should support HTTP/2
14	Should supports the following modes of operation for cookie-based session persistence: Insert, Passive, Rewrite mode
15	Solution should support Role Base Access Control (RBAC) with Following User Accounts and Access Levels: User Operator Administrator Certificate Administrator
16	The proposed Solution should be PCI Compliant WAF. It must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification.
17	WAF should have the flexibility to be deployed in the following modes: Reverse proxy Out of Path (OOP)
18	Solution should dynamically understand the Changes on the Web/Application Server
19	The Proposed WAF Solution should support both a Positive Security Model Approach (A positive security model states what input and behavior is allowed and everything else that deviates from the positive security model is alerted and/or blocked) and a Negative Security Model (A negative security model explicitly defines known attack signatures) . The solution must support automatic updates to the signature database to ensure complete protection against the latest web application threats
20	The WAF should support the following escalation modes: a) Active, b) Bypass, c) Passive

Sl. No.	Technical Specifications
	Virtual Web Application Firewall
21	The solution must have a database of signatures that are designed to detect known problems and attacks on web applications
22	**Hiding Sensitive Content Parameters:** It should be able to Mask values of sensitive parameters (for example, passwords, credit card and social security details)
23	**Auto Policy Optimization**
	• Known Types of Attack Protection - Rapid Mode
	• Zero Day Attack Blocking - Extended Mode
	• Working in Learn Mode
	• Auto Discovery
24	**The proposed WAF should support the Activity Tracking, which should include the following:**
	Dynamic IP
	Anonymity
	Scraping
	Mimicking user behavior
	Clickjacking
25	**Device Fingerprint-based tracking**
	Should support Fingerprint technology which involves various tools and methodologies to gather IP agnostic information about the source. Should also involves running JavaScript on the client side. Once a JavaScript is processed, an AJAX request is generated from the client side to WAF with the fingerprint information.
26	Should support API Security, API Quota Management and GraphQL.
27	Should support Auto Policy Generation with: • Full Auto, • Auto Enabled, • Auto Refinements,
28	Should support Auto Discovery which should displays an application view that contains the server, tunnels, hosts, folders (URIs), files (pages), and parameters (Path and Query)
29	Solution should provide: Application Dashboard Per Application Analytics SLA Breakdown (Network, per server) SSL Statistics (handshake and cypher breakdown, rejected handshake) SSL CPS System Dashboard Network Dashboard L4 Events Per transaction type events (delay, user agent, response, headers) SSL Events (type of handshake, cypher, TLS version)
30	Shall be configured in High Availability Mode. In case of failure of one of the instance; the other available instance/s shall serve all the requests without any disruption or degradation in overall performance

Sl. No.	Technical Specifications
	Virtual Web Application Firewall
31	Shall support TCP and UDP applications.
32	Should support ECC in addition to other commonly used Ciphers from day1
33	Should support end – end SSL if required from day1
34	System supports performing load balancing across multiple sites, complete disaster recovery among sites and optimal service delivery , Single application failure etc
35	System supports global redirection based on DNS from day1
36	Supports the following health check types: • Link Health Checks, • TCP Health Checks, • UDP Health Checks, • ICMP Health Checks, • HTTP/S Health Checks, • TCP and UDP-based DNS Health Checks, • TFTP Health Check, • SNMP Health Check, • FTP Server Health Checks, • POP3 Server Health Checks, • SMTP Server Health Checks, • IMAP Server Health Checks, • NNTP Server Health Checks, • RADIUS Server Health Checks, • SSL HELLO Health Checks, • WAP Gateway Health Checks, • LDAP/LDAPS Health Checks, • Windows Terminal Server Health Checks, • ARP Health Checks, • DHCP Health Checks, • RTSP Health Checks, • SIP Health Checks, • Virtual Wire Health Checks, • DSSP Health Checks, • Script-Based Health Checks, • Cluster-based Health Checks,
37	Shall be able to support different cookie persistence methods
38	The proposed device should support standard VRRP (RFC - 2338) for High Availability purpose (No Propertary Protocol). Other mode like Switch HA Mode, Extended HA Mode and Service HA Mode should also be supported.
39	Shall support NTP for date & time synchronization from NTP Server.
40	Shall have static routing & dynamic routing (RIP, OSPF, BGP) capabilities.
41	The Solution should support native integration with Kubernetes Platforms and controller/connecter/plugin should operate within Kubernetes Cluster to automatically create service on Load Balancer. The controller/connecter/plugin should also support automatic creation, edition and deletion of service like VIP creation, Node/Real Sever Creation, Farms/Group Creation, SSL Binding etc.
42	The controller/connecter/plugin should support at least three components with different task as follows: a. A Controller which should discovers the service objects in the Kubernetes clusters. b. An Aggregator which should aggregates inputs from all the controllers and communicates the necessary configuration changes to Configurator. c. A Configurator which should prepare a load balancing configuration file and pushes it to the device.
43	The solution should support automatic renewal of SSL Certificate via integration with 3rd party Certification Authority such as Lets Encrypt
44	Shall be manageable (both GUI and CLI) using SSH, Web based management (HTTPS) etc.
45	Shall have feature to provide role based user's access for management.
46	Shall support authentication and authorization through Radius / TACACS+.

Sl. No.	Technical Specifications
	Virtual Web Application Firewall
47	Bidder should propose Centralized Management & Reporting Solution from Day 1.
48	The proposed solution should be EAL2 certified. OEM should be ISO 9001, ISO 14001, ISO 45001, ISO 28000 certified.

5.13. Server Security Solution

S.no	General requirements
1	The solution should offer Antivirus, Application Control, Change Control, HIPS, and Virtualised Security functionality for servers to ensure optimal security and compliance for critical servers on single agent.
2	The solution should be managed from a single centralized console.
3	The solution should have a small overhead footprint such that it minimizes impact on system resource
4	The proposed solution shall support the Windows & Linux Server platforms
5	The proposed solution should be able to manage both Endpoint & Server Secuirty solution from the same single management console.
	Anti-Virus & Anti Spyware For Servers
1	Solution must provide automated and centralized download and deployment of latest virus signature updates from the Internet to desktops and servers across the organization, across different Windows platforms. Updates should be incremental with update sizes of ~100KB on average
2	Solution must provide flexibility to install different components (Like – Management Agent, AV client, Anti-Spyware, HIPS,) separately for better use of network bandwidth
3	Should have the ability to detect and remove unwanted programs, toolbars, adware, spyware, dialers etc & Post detection the actions that the antiviral performs must be the following: Alert / Notify , Clean, Delete / Remove, Move / Quarantine, Prompt for Action
4	Should support file scan caching to avoid repetitive scanning of files which are unchanged since the previous scan
5	Proposed solution must automatically scan Floppy disks, Compact disks, USB devices and Network shares in real-time when accessed.
6	Proposed solution should provide multiple policies to lockdown the server like – change in registry, Internet Explorer file settings, Exe file execution etc to block unknown zero day attacks and reduce dependency on frequent signatures
7	Should allow the On Demand Scanner to recognize the last scanned file and resume scanning from that file if an “On demand Scan” is interrupted
8	Should have the ability to control the amount of CPU resources dedicated to a scan process
9	The proposed solution should be capable of detecting and preventing buffer overflow vulnerability, irrespective of the exploit that is using the buffer overflow vulnerability. The solution should support buffer overflow detection and prevention on the following minimum applications: Windows OS Services,

	Media Player, Internet Explorer, SQL Server, Word, Excel, Power Point, Auto Update, Explorer, Instant Messenger, Outlook, Outlook Express etc
10	Proposed solution should be capable of blocking TCP/IP ports on the System and also creating exceptions for specified applications to use these blocked ports.
11	Proposed solution should be capable of blocking read, write, execute, delete & change permissions on specified file(s)/folder(s)/Network Share(s).
12	Discover and Report the IP Address of the end-point system (infection source) that sent malicious code to the server and optionally, block further communications from the infection source end-point system for a configurable time period or indefinitely
13	The proposed solution should provide Self protection from modifying or disabling AntiVirus Client
14	Proposed solution should allow to configure different policies for different set of Processes
15	The Antivirus should allow for automated rollback of virus definition, if required
16	Should be able to lock down all anti-virus configurations at the servers.
17	Proposed solution should be capable of detecting and blocking communication from hosts that are spreading viruses/worms.
18	Should support unique real time update based on over the web cloud technology to provide real time signatures for dynamic and latest threats to reduce the dependency on Daily Signature updates
19	The proposed solution should have the option to block the intruder hosts for a specific number of seconds.
20	Sould have enhanced tamper protection that guards against unauthorized access and attacks, protecting users from viruses that attempt to disable security measures
	Antimalware
1	The proposed solution updates should be incremental with the option of full updates when the client is not updated for a long period
2	The proposed solution should protect the registry of the proposed solution
3	Solution should offer different client/server communication settings be imposed based on different groups
4	The proposed solution should scan system memory for installed rootkits, hidden processes, and other behavior that suggests malicious code is attempting to hide itself.
5	It should support Signature as well as behavioral based detection along with the automatic rollback features when the system is compramised with ransomeware attack.
6	Proposed solution should support rollback feature in case machines gets compramised
7	The system should periodically scan log files for anomalous activity andnotify the system administrator if they have detected suspicious pattern on thehosts.
8	The proposed solution's agent should be light weight and should be able to work on the system with the 3Gb RAM & 2GHz processer or higher.
	Application Control For Servers

1	The solution should provide the dynamic management of execution capability of applications on a server system, prevent unauthorized registry manipulation and in memory protection of application
2	It should prevent execution of all unauthorized software, scripts, and dynamic-link libraries (DLLs) and further defends against memory exploits
3	The solution should provide for a real time capability to prevent execution of any authorized application to execute on the server system
4	The solution should allow an administrator to authorize a well defined update mechanism to alter the state of gold image as being enforced currently to a new gold image.
5	The solution should allow an administrator to remote view the constituents of a system image and hence compare the image with a well defined gold image.
6	The solution should allow for well defined update mechanism to allow changes to the state of server system and then enforce the new state of the system
7	The solution should not require updates to be rolled to client system in order to approve new applications to be executed.
8	The solution should allow/ban individual application based on different characteristics such as name, checksum etc.
9	It should restrict administrators with physical or remote access to the machine to override protection
10	The solution should augment blacklisting, real-time reputation awareness, and behavioral approaches, helping IT to consistently enable the known good, block the known bad, and properly handle the new and unknown.
11	The solution should prevent the tampering of application on the disk and in the memory.
12	The solution should have a small overhead footprint which includes:
	• Easy setup and low initial and ongoing operational overhead
	• No file system scanning that could impact system performance
	• Designed to work in disconnected and in “offline“ mode if necessary
13	The solution should be able to create inventory of a target system and hence report on installed software and applications on client machines.
14	The solution should not be dependent on any external verification of allowed/banned application. It should be able to take its input on the basis of local state of server system as verified by the system administrator
15	The solution apart from allowing only authorised applications to run, should block any changes from being done to authorized applications, like DLL's, System files, registry etc., thus providing application treat protection
	File Intigrity Monitoring For Servers
1	The solution should support Real-time Change Tracking Audit log. It should Include File, User, Program name and contents that have changed. FIM should support detect and block mode.
2	The solution should support Change Prevention as part of the core solution
3	The solution in the event of unauthorized file change, should reports WHAT changed, WHO made the change, HOW they made it and precisely WHEN they did the changes
4	The solution should offer intelligent filters which are pre-configured to track the relevant objects on the system, for each standard Operating System covering systems files including Windows, Solaris, and Linux. It should also

	include application filters for Apache, Tomcat, Websphere and JBOSS, IIS, Weblogic, Websphere , etc., and should be customizable.
5	The solution should monitor application and operating system files in real time
6	The solution should provide email and SNMP alerts
7	The solution should integrate with change management, data center automation, and configuration management database (CMDB) solutions from HP, BMC, IBM, and others
8	The solution should be capable of tracking changes to databases in two manners (1) changes to the database structures themselves (tables, indexes etc.) (2) changes to the data itself, in real time
	HIPS for Servers
1	It should support Signature as well as behavioral based detection
2	It should support policies creation based on – User defined, Adaptive mode and Learn mode
3	It should support desktop firewall capabilities to directly block unwanted traffic
4	HIPS solution should provide facility to create different policy for different network connectivity like – LAN, DHCP.
5	It should support firewall policy to enable cloud based network reputation lookup. For e.g. if a client is communicating with an IP address with a bad reputation or bad URL, the firewall should stop the communication without having to create a rule.
6	HIPS Solution should provide blocking of unwanted applications trying to run
7	HIPS solution should provide facility to create User defined signatures
8	HIPS solution should provide protection from known attacks like – SQL injection, Cross Site scripting, Buffer Overflow without having signature updates
9	HIPS solution should provide vulnerability shielding to the application not having patches installed
	Virtualization security
1	The Proposed Solution should offloads scanning, configuration, and .DAT update operations from individual guest images to an offload scan server within the premises
2	The solution should build and maintain a global cache of scanned files to ensure that once a file is scanned and confirmed to be clean, subsequent VMs accessing the file won't have to wait for a scan.
3	Should allows separate policies for on-access and on-demand scanning to enable fine-tuned security execution
4	Should provide Connector for VMware vSphere provides a complete view into virtual data centers and populates key properties such as servers, hypervisors, and VMs through the same management console.
5	The Solution should provide administrators gain visibility into the security status of all VMs and can monitor hypervisor-to-VM relationships in near real time.
6	The Proposed Solution should work agentless on VMware workloads
7	Solution should extend visibility and control across Amazon Web Services (AWS) and Microsoft Azure public clouds and physical servers.

	Server Security
1	Server security solution should be capable of integration with cloud IaaS platforms such as; AWS, GCP, Azure. Private cloud platform such as, VmWare virtual platform, Hyper-V etc.
2	Proposed solution should support shahow IS feature. E.g. Post integration with server management platforms it should automatically discover all the tenents configured on concern management platform.
3	Solution should display potential threats and unsafe settings so that appropriate actions can be taken.
4	It should be capable of defining compliance policies for security assessment and view all high and low compliance events in the dedicated dashboard.
5	It should display security group information of virtual instances across cloud accounts.
6	It should show how many instances are associated with any firewall (security group) or network security.
7	It should also manage these firewalls (security groups) by adding, editing, or deleting rules, and detaching firewall (security group) from an instance.
8	It should support multiplatform environment
	Management
1	Proposed solution should provide single agent and console to manage all components – Threat Prevention for Windows and Linux platforms Desktop Firewall Application & Chnage Control Virtualized environment which includes both on premises and on public cloud
2	The centralized management console must be web-based
3	The centralized management console should be capable of deploying remotely the managed products (such as Endpoint Security).
4	The tool should support hierarchical grouping of machines and policy deployment. The grouping could be based on IP Address of a subnet of machines or a particular site
5	The Centralized management tool should be capable of deploying Pattern Files, Scan Engines, emergency releases of pattern files, patches, hot fixes and new product versions for all managed products
6	The centralized management tool should be able to deploy signature files for different products at scheduled times.
7	The management platform allows for separate deployment of components to systems. This allows for flexibility of deployment.
8	Centralized management console should provide dashboard with multiple information & these information should also be fetched from database based on different queries
9	Console should support tagging of information in the database to provide flexible reporting
10	The centralized management should provide Asset Management functionality and provide complete details of managed endpoints such as, Hostname, IP address, OS type, Freee memory etc.
11	Administrator should be able to configure the update process as automatic or manual, controlled deployment
12	Update process should conserve WAN Bandwidth by having a distributed framework for signatures and policy updates

13	The centralized management console should provide management reports for different managed components like – Top N reports, Trend reports, Outbreak reports, Compliance reports,
14	The centralized management console should support a way to build custom queries on the database to create custom reports
15	Central management console should provide automatic generation and delivery of reports to the respective administrators
16	Central management console should provide actionable reports
17	The proposed solution should integrate with Active Directory and other LDAP based directory services.
18	Central management console should support granular role based access control
20	The Centralized Management Console should deliver security threat information including current threats and the DAT and engine files necessary to protect against them
21	Reports should be in CSV, HTML and Microsoft Excel Format
22	Explain if your central management is based on an Open framework that unifies security management for systems, applications, networks, data, and compliance solutions
23	Extensible platform integrates with and leverages your existing IT infrastructure
24	Must provide native 64 bit performance for report generation from the database
25	Must provide real time software deployment and updates to large organization networks made up of multiple subnets and vlans
26	Must natively provide management snapshots for all managed settings, preferences and files and quicker disaster recovery and management restoration
27	Solution must offer locally and globally sourced threat intelligence, which enriches protection through file and URL reputation
28	Solution must have AI Capability and must not completely depend on internet based threat feeds and have its own heruristic and machine learning capability .
29	Must report on the management server if the managed AV machine is under a VDI mode
30	Must provide side by side policy settings and management comparison
31	Must include the ability to Identify unknown assets on your network and bring them under control with rogue system detection
32	Proposed solution should have separate console to manage workload on different servers. It should not be limited to server placement (e.g. On-prem or cloud only)

5.14. Integrated Smart Rack

S. No	Description of Requirements
1	**Scope of Work**

S. No	Description of Requirements
1.1	This specification covers Intelligent Integrated Smart Rack Infrastructure, standalone system design, testing at manufacturer's works, supply, delivery at site, unloading, handling, proper storage at site, erection, testing and commissioning at site of complete infrastructure for the proposed Smart Rack solution
1.2	The critical components of the smart rack solution can be maintained easily in the events of failure. All the components of the infrastructure should be such that it can be easily dismantled and relocated to different location.
2	**Requirements**
2.1	The Integrated Smart Rack Solution with inbuilt hot and cold aisle containment of 1 rack should cater IT load up to 7 kW.
2.2	Integrated Smart Rack Solution essentially should include environmental controls, Rack mounted air conditioning, smoke detection & fire suppression, Water leak detection and humidity sensors and security devices. Environmental monitoring shall be done from IP based software.
2.3	The Integrated smart rack solution must be CE Certified.
2.4	The critical components like Cooling unit, Rack, UPS , rack PDU & Monitoring unit should be from same & single OEM for better integration & service support.
3	**The Intelligent integrated Infrastructure shall have following components: -**
3.1	**Rack based closed loop Air-Conditioning**
3.1.1	The smart rack should be equipped with rack mounted cooling unit to provide closed loop cooling system which should be able to cool the equipment's uniformly right from 1st U to 42nd U of Rack
3.1.2	Rack Mounted Air-Cooling unit should be of 7kW/2TR capacity, (01 no. of 7kW rack-based cooling unit). The air from will be from bottom to top. The unit will have following configuration: Rack based Air Cooling with indoor - out door design, SHR >0.9, 100% Duty cycle, scroll compressor, 9U rack mountable, electronically commutated (EC) fan, High Pressure & Low-Pressure protection, Washable filter with 80% efficiency down to 20-micron, Hydrophilic evaporator coil, ON/OFF switch at indoor unit for emergency purpose, R407C/R410A Refrigerant.
3.1.3	The unit should support indoor to outdoor copper piping distance up to 30 mtrs including vertical piping distance up to 30 mtrs.
3.2	**Power Distribution**
3.2.1	0U, Vertical Rack PDU , 32A, 230V, 7.3kW with 20 no. IEC C13 & 04 no. IEC C19, 3m power cord with 1P+E (IP44), Black Powder Coat.
3.3	Electrical Distribution System

S. No	Description of Requirements
3.3.1	Rack mountable Power Output Device with essential breakers to be provisioned. All input supply cables from POD unit to equipment's are connected with industrial socket (male - female) with suitable rating
3.4	**Environmental Controls**
3.4.1	Intelligent Smart Rack (01 Nos.) should include basic environmental controls: Smoke Detector Water Leak Detection system Temperature/ Humidity Sensor Door Sensor Alarm beacon
3.5	**Rack & accessories**
3.5.1	Rack is 42 U 19" mounting type with 2100 (Height) x 800 (Width) x 1200 (Depth) with safe load carrying capacity of 1400 Kg on enclosure frame and 1000 Kg on 19" mounting angles
3.5.2	Front Glass door for complete 42U height visibility and rear plane/split door with stiffener for strength
3.5.3	Cable entry provision from top & bottom both side of rack
3.5.4	Cut outs with rubber/brush grommet on top and bottom cover of rack for cable entry
3.5.5	Vertical Cable manager on both LHS & RHS on rear side
3.5.6	Thermally insulated cold aisle chamber
3.5.7	Blanking panels to prevent air mixing
3.5.8	Status based LED light to be provided on each rack
3.5.9	70% Blanking panels to be supplied with the Smart rack
3.6	**U Space**
3.6.1	Intelligent Smart rack should have Min 24U(total) space available for IT equipment's and network equipment
3.7	**Monitoring**
3.7.1	Detailed Monitoring & Diagnostics 1U rack mountable monitoring unit with redundant power supplies & capable of single window monitoring of all the environmental parameters along with Air conditioning through a single window dashboard over ethernet & Capable for sending Email Alerts
3.7.2	Monitoring unit should integrate & monitor environmental parameters like temperature, humidity, door access, smoke etc. with cooling unit in a single dashboard along with other environmental parameters like temperature, humidity, smoke etc.

S. No	Description of Requirements
3.7.3	The monitoring unit should support basic protocols like Telnet, SSH, FTP, SFTP, HTTP, HTTPS, NTP, DHCP, DNS Server, smtp, TCP/IP4. It should support network interface of 10/100M self-adaptable Ethernet ports.
3.7.4	Air conditioning should be integrated with the monitoring unit to monitor all critical parameters (Cooling unit: Unit status, supply & return air temperature, humidity in a single dashboard.
3.8	**Safety & Security**
3.8.1	Rodent Repellent system Rack to be covered with rodent repellent system
3.8.2	Access Control System The system deployed will be rack based access control system based on Biometric Technology. The front & rear rack doors will be provided with electromagnetic locks and will operate on fail-safe principle through Biometric access control system.
3.8.3	01 no. IP Based Camera for live monitoring.
3.8.4	Fire Detection & NOVEC 1230/FK-5-1-12 Fire Suppression system Rack to be covered with Fire alarm & gas-based suppression system. The system should have fire suppression unit mounted internally / externally on the rack. The fire suppression agent should be NOVEC 1230 / FK 5-1-12 clean agent gas based as per NFPA 2001 guidelines
3.9	**UPS System (02 no. x 10 kVA)**
3.9.1	UPS should be of True On-line, Double conversion and IGBT minimum 10 kVA capacity in N +N topology, 1 Phase input & 1 phase output, rack mountable (≤ 2U) with unity power factor and efficiency up to 95 % & eco mode efficiency up to 99%.
3.9.2	Input Parameters: Input Voltage Range: 176-288VAC at full load; 100-176VAC at linear derating; 100VAC at half load Input Power factor: 0.99, at full load; ≥0.98, at half load Input frequency range (Hz): 40-70 Hz Current THD at full linear load (THDi%): <5
3.9.3	Output parameters: Nominal output voltage (V): 220/230/240 (1-phase) Rated power factor(kW/kVA): Unity.

S. No	Description of Requirements
	Voltage harmonic distortion (%): <2% for Linear loads & <5% for Non-linear loads Overload capacity: At 25°C: 105% ~ 125%, 5min; 125% ~ 150%, 1min; 150%, 200ms Crest factor: 3:1 Frequency synchronization range: Rated frequency±3Hz. Configurable range: ±0.5Hz ~ ±5Hz Dynamic response recovery time: 60ms
3.9.4	Transfer time Mains←→Battery: 0ms Inverter←→Bypass: Synchronous transfer: ≤0ms Asynchronous transfer (default): ≤20ms
3.9.5	UPS should be RoHS certified, Energy star & BIS certified with IP20 Protection level. Noise level should be < 55dB
3.9.6	Operating temperature for the UPS: 0°C ~ 50°C; Relative humidity: 5%RH ~ 95%RH, non-condensing
3.9.7	Conformity & Standard Compliance: General and safety requirements - IEC/EN 62040-1, EMC - IEC/EN 62040-2; Surge protection for UPS: IEC/EN-61000-4-5, ANSI C62.41, 6kV/2Ohms
3.9.8	UPS system should support battery backup 15 min @ rated load per UPS. Batteries to be placed in separate battery racks.
4	**OEM Credential**
4.1	The critical components of Integrated Smart Rack solution like Cooling unit, UPS , Rack, Rack PDU, Monitoring unit should be from same & single OEM for better integration & service support.
4.2	The Integrated smart rack solution must be CE Certified.
4.3	Smart Rack OEM or Manufacturer should be ISO 9001: 2000, ISO 14001, ISO/IEC 27001:2013 and ISO 45001 certified.
4.4	Smart rack OEM should have its own manufacturing facility in India for offered or similar capacity range of Rack & Precision air conditioning units for high availability of the proposed solution. Supporting document/undertaking regarding the same to be submitted along with the bid.
4.5	The Smart rack OEM should have at least 10 years of experience in executing similar works (Similar works means – "SITC of Integrated Smart Rack Infrastructure of minimum 01 rack configuration") in Central/State/PSU Organizations. Completion Certificate, as a proof of experience, signed by the concerned authorities to be submitted along with the bid.

S. No	Description of Requirements
4.6	OEM or Manufacturer of the offered goods/ equipment's should be a company registered under the companies act since last 10 years. Valid company registration certificate should be submitted.

NOTES:

1. The cost of all hardware items should include mandatory 5 years onsite comprehensive Original Equipment Manufacturer's warranty.
2. The quoted products should not be end of sale / life for next 2 years and OEM support of the same should be available for next 5 years after end of life / sale.
3. All the required licences in the solution should be in the name of the Owner department i.e. Revenue and Disaster Management département, Haryana.
4. The details of offered service support pack should be provided with complete active component compliance from OEM.
5. The Successful bidder is required to supply the latest updates, patches and upgrades, OS updates free of cost during the warranty period.
6. The quoted rates should be inclusive of preparing of cable layout, cable, punching, fixing of active & passive components, tagging of patch cords etc.
7. In case of any additional item, as per site requirement, like Switch, Jack Panel, Rack etc. is required the same be provided / installed by supplier after written confirmation by purchaser/ Owner département. The copy of the same is required to be forward to CRID.
8. Proper tagging of all cables including uplink with number is prepared by supplier & the copy of the same is submitted to the nodal officer.
9. The list of IP addresses including Computer Name, IP Address, Workgroup / Domain is to be prepared by the supplier & provide to the nodal officer for future reference. The copy of the same is forward with installation report to CRID.
10. Power Source: Power source will be provided at the data center.
11. Any Indian product is allowed which meets all the specifications subject to "Standardization Testing and Quality Certification (STQC) certification for trusted supply chain compliance", wherever applicable.

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

6. 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. CRID 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 CRID. 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 CRID 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 CRID by E-mail to rahul.narwal@nic.in, sit@hry.nic.in with a copy to addl-cito.crid@hry.gov.in, munishchandan.crid@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.

Note: - Queries must be strictly submitted only in the prescribed format (.XLS/ .XLSX) as per Appendix 1. Queries not submitted in the prescribed format shall not be considered/ responded at all by the purchaser.

6.3 Pre-Bid Conference – Amendments to the Tender (may or may not be required)

6.3.1 In order to avoid clarification/confirmation after opening of bids, wherever specifically mentioned in NIT, Pre-bid conference may be held so as to provide an opportunity to the participating bidders to interact with CRID 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 If required, 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 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 https://haryanait.gov.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. CRID 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 CRID 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 CRID 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 CRID 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 CRID 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 SS (IT) AND TREASURER, CRID, Sector-17/B, Chandigarh-160017, 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 CRID 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. CRID 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 CRID Website i.e. https://haryanait.gov.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.

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 CRID 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) can be converted as the Security Deposit (SD) for successful execution of the orders during contract period and will be returned only after the successful fulfilment of the Contract.

6.7.3.4 The EMD amount will be forfeited by CRID 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 Tender Validity

The e – tender submitted by the Bidders shall be valid for a minimum period of 180 days from the date of opening of the Commercial e-bids.

6.7.5 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.

6.7.6 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.

6.7.7 **Technical Bid (Stage 1)**

6.7.7.1 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.

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

6.7.7.3 The technical bid should be submitted through e-bid (uploaded) as per the last date & time and all pages to be duly filled & signed & stamped as per the formats given in the tender document and annexures. Bidder to ensure that the uploaded content should be clear and readable. The Purchaser can ask for clarification or better scan of any document at any time during office hours which the bidder agrees to provide within 2 hrs.

6.7.7.4 6.7.7.4 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.

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

6.7.8.1 The Price bid should be submitted through e-bids as per the online 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.

6.7.8.2 All the Price items as asked in the Tender shall be filled in the Price Bid Format as given in the Tender at “Format2: Commercial Bid”.

6.7.8.3 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.

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

6.7.8.5 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 authorized signatory.

6.7.8.6 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 keep the Price firm during the period of Contract including during the period of extension of time if any. Escalation of cost will not be permitted during the said periods or during any period while providing services whether extended or not for reasons other than increase of duties / taxes payable to the Governments in India within the stipulated delivery period. The Bidders shall particularly take note of this factor before submitting the Bids.

6.7.8.7 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 CRID.

6.7.8.8 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, CRID shall avail such discount at the time of award of contract.

6.7.9 Correction of error

6.7.9.1 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 CRID.

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

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

6.7.10 **Bid closing date and time**

The e-Tenders shall be submitted not later than the date and time specified as under or Corrigendum if published. Last date and time to submit the bid upto 2.30 PM. 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.

6.7.11 **Mode of Submission of Bids: -** The Bids shall be submitted electronically on Haryana Govt. e-procurement portal strictly as specified in the Tender document. The hard copy to technical bid will be submitted at O/o ACITO, CRID, 4th Floor, SCO 109-110, Sec 17-B, Chandigarh, 160017.

6.7.12 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 CRID.

6.7.13 **Rejection of Bid: -**

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

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

6.7.14 Disqualification

CRID/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 ineligible/ blacklisted by any Govt. or quasi-Govt. entity in India.

6.7.15 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.

6.7.16 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 CRID.

6.7.17 Extension of Last date for Submission

CRID 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 CRID and Bidders shall stand

extended. However, no request for extension of time from the Bidders shall be binding upon CRID. The decision of CRID in this regard will be final, conclusive and binding on the Bidder.

6.7.18 Late Bids

Any bid received by CRID 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.

6.7.19 Duties, Taxes and Statutory levies

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

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

6.7.19.3 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 CRID 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 CRID/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.

6.7.19.4 If there is any reduction in taxes / duties due to any reason whatsoever, after Award of Contract, the same shall be passed on to CRID.

6.7.19.5 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 CRID shall not bear responsibility for the same.

6.7.20 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 CRID 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. CRID 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.

6.7.21 Right to Accept/ Reject the Bid

CRID 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.

6.7.22 Limitation of Liability:

Notwithstanding anything to the contrary in this Agreement, the cumulative liability of the successful bidder towards Purchaser for any damages or compensation of any nature whatsoever under this Agreement, shall be limited to the amount of payment receive or receivable by the Bidder for the applicable milestone or the project as applicable.

SECTION 7

TENDER OPENING AND EVALUATION

7. 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 CRID 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 CRID will be final in this regard;

7.3. Clarifications by CRID

When deemed necessary, CRID 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, CRID may seek additional information or historical documents for verification to facilitate decision making. In case the Bidder fails to comply with the requirements of CRID as stated above, such Bids may at the discretion of CRID, 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 CRID. CRID shall have the right to reject the Bid and if after selection, CRID 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, CRID 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, CRID 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 CRID or HARTRON, their previous performance in CRID or 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 purchase 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/purchase 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. The negotiations will be held up to L3 bidders if the difference between L1 quoted rates and those quoted by L2 & L3 is within 5% of the L1 quoted rates 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 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.

iii. 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 CRID 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. The award for contract will be issued to the successful bidder(s) as per State Govt. Policy applicable at that time of finalization of Contract.

ii. Total quantity will be apportioned among the L1 apportioned among the L1 Bidder and other Bidder who have agreed to match L1 rate, as per the option of purchaser. However, in case the end user does not indicate any choice, SS (IT) AND TREASURER, CRID reserves the right to distribute the quantity among the successful vendor.

iii. Purchase preference can be given to the eligible vendors as per the Govt. guidelines prevailing from time to time.

7.9. Letter of Acceptance (LOA)

After acceptance of the Tender by CRID, a Letter of Acceptance (LOA) will be issued to the Successful Bidder(s) by CRID. Under this contract, CRID has the right to issue LOA to more than one bidder.

7.10. Security Deposit (SD)

The EMD of the successful bidder (s) shall be converted into a Security deposit and shall be retained till the submission of required PBG. The EMD will be refunded to the Successful Bidder only after successful completion of the contract period as mentioned above. The Security Deposit held by CRID till it is refunded to the Successful Bidder will not earn any interest thereof.

The Security Deposit will be forfeited if the Successful Bidder withdraws the Bid during the period of Bid validity specified in the Tender or if the Bidder fails to sign the contract.

7.11. Execution of Contract

7.11.1. The Successful Bidder shall execute a Contract in the non-judicial Stamp Paper of the required amount bought in Haryana/Chandigarh only in the name of the Bidder within 20 days from the date of Letter of Acceptance issued by CRID with such changes/modifications as may be indicated by CRID at the time of execution on receipt of confirmation from CRID.

7.11.2. 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 CRID. CRID reserves its right to cancel the purchase order 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/SD of the Successful Bidder will be forfeited and their tender will be held as non-responsive.

7.11.3. The expenses incidental to the execution of the Contract shall be borne by the Successful Bidder.

7.11.4. 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 CRID and CRID also have the right to recover any consequential losses from the Successful Bidder.

7.12. CRID 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 customers.

SECTION 8

TERMS AND CONDITIONS OF THE CONTRACT

8. Terms and conditions of the contract

8.1. Acceptance of Tender and Withdrawals

The final acceptance of the tender is entirely vested with CRID 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 CRID, 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 on random basis, the Networking items being a standard product; however, the physical verification like quantity, models, physical conditions etc. will be done for all the vendors against respective order.

ii. The Special Secretary (IT) and Treasurer, CRID can authorize any of the experts or any of its officer or person shall have the power to inspect the stores at manufacturer premises/ distributors premises or at consignee site and to reject the same or any part or portion after the written approval of the Special Secretary (IT) and Treasurer, CRID, if he or they be not satisfied that the same is equal or according to the specifications submitted by the contractor. The contractor shall not be paid for supplies rejected as above and such supplies shall be removed by the successful bidder immediately at his own expense. Any harm whatsoever incidental to a full and proper examination and test of such supplies. CRID shall be under no liability whatsoever for rejected and the same will be at the contractor's risk. Rejected supplies shall be removed by the contractor within 10 days after notice has been issued to him of such rejection and failing such removal of rejected goods will be at contractor's risk and CRID may charge rent from the contractor for the space occupied by such rejected goods. Super inspection of stores already inspected may be carried out at the discretion of Special Secretary (IT) and Treasurer, CRID, by such officer as may be familiarize by him.

iii. The Successful bidder shall provide without any extra charge all materials, tools, labor and assistance of every kind which the aforesaid officer may consider necessary for any test or examination which he may require to be made on the successful bidder's premises and shall pay all cost attendant thereon. In the case of stores inspected at Manufacturer's premises, all facilities including testing appliance, tools etc. for carrying out the tests shall be provided by the manufactures other than special tests, or in dependent tests. Failing these facilities at the own premises for making the tests the successful bidder shall bear the cost of carrying out test elsewhere, the bidder shall provide and deliver the item also free of charge at such place as the aforesaid officer may direct such materials as he may require for tests. If for the purpose of determining the quality of stores the aforesaid Officer find it necessary to have the stores tested at the test house or laboratory, all expenses incidental to the test shall be borne by the contractor. On the failure of the contractor to pay the expenses within 10 days of the receipt of intimation in this behalf from the Inspecting Officer, the Special Secretary (IT) and Treasurer, CRID shall have the right to deduct the amount from the security deposited by the successful bidder, and if the amount so deducted is not deposited within 10 days, the Special Secretary (IT) and Treasurer, CRID may treat the default as a breach of agreement and proceed as per agreement without further notice. Further the aforesaid officer shall have the right to put all articles or materials to such tests as he may

think proper for the purpose of ascertaining whether the same are in accordance with the specifications or sealed sample mentioned in the tender and to cut out or off and/or destroy a portion not exceeding 2% from each delivery for such purpose and the quantity so cut out or off and/or destroyed as aforesaid shall be replaced by successful bidder free of charge.

iv. CRID reserves the right to waive of the inspection on case to case basis for standard products, green channel products/urgent requirements/ products for which test reports from ERTL/ETDS etc. are made available by the successful bidder. CRID reserves the right to conduct the inspection of limited quantity on random sample basis.

8.3. Refund of EMD

The EMD amount paid by the Successful Bidder(s) will be kept as Security Deposit for the duration of the contract. If the Successful Bidder submits Security Deposit for the stipulated value in full by way of Bank Guarantee, the EMD will be refunded. The EMD amount of the Unsuccessful Bidder will be refunded after familiarizes and issue of Firm Purchase Order to the Successful Bidder.

8.4. Warranty

i. 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.

ii. 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.

8.5. **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 CRID 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 CRID 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.

8.6. Licenses & Transportation

i. All the operating system/software licenses if applicable are to be registered in the name of the purchaser.

ii. The entire cost of transportation from the Manufacturing Plant or Port of Landing to the designated destination as specified by CRID shall be borne by the selected Bidder.

iii. The transit insurance for all the items being delivered at respective site is the responsibility of the successful bidder.

8.7. **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 purchaser, the successful bidder shall replace the aid equipment at his cost within 10 days from the event reported by the CRID.

8.8. Additional Payment Clause:

i. No payment shall be made in advance for any supplies made under this order.

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 for a minimum period of 12 months or till the scope of work, whichever is more. The PBG for a proportionate value 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/Owner 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 CRID/end user, extension of delivery time for the period of such delay involved may be granted by SS (IT) AND TREASURER, CRID provided 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 clause no. 3.2 unless otherwise specified in the purchase order. Some occasions may arise that the products as indented by the department 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.

8.9. Invoicing:

i. With every dispatch of goods or materials in the order, Delivery Challan in triplet are to be sent by the successful bidder to the consignee at the time of delivery. The duplicate of Delivery Challan to be returned by the respective officers (the Nodal officer / HOD at the location) with the quantities or numbers received duly noted and signed thereon to the successful bidder.

ii. Invoice for Phase 1 to be submitted to CRID along with the duly signed Delivery Challans of received by the successful bidder from the respective officers (the Nodal Officer / HOD at the location) for further necessary action regarding payments, etc.

iii. Invoice for Phase 2 i.e. installation, configurations, testing, commissioning & Go-Live of the project to be submitted by the bidder to CRID along with installation reports and Go-live reports duly signed & stamped by the Nodal Officer / HOD at the location.

iv. Invoice for Phase 3 i.e. the payments in 2 equal instalments with Incident Report / Service Call report and SLA compliance report verified by the respective Nodal Officer at the end of each 6 monthly cycle starting from next day of completion of Phase 3.

v. Eight Invoices for Phase 4 i.e. the payments in 8 equal instalments OPEX to be submitted by the bidder to CRID along with, Incident Report / Service Call report and SLA compliance report verified by the respective Nodal Officer / HOD at the location at the end of each 6 monthly cycle starting from next day of completion of 1 year warranty.

vi. The payments in each of the above cases shall be released by CRID after receipt of inspection/ verification of the deliverables from the inspection committee.

8.10. 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.

III. In case required performance security is not submitted by the bidder within 15 days from the date of issue of Purchase order, the Earnest Money deposited by the Bidder will be forfeited.

B. forfeiture of Performance Security: -

I. The CRID 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.

II. 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.

III. In case successful bidder fails to comply with the delivery period as specified in the work order/contract, the Performance security deposited by the vendor will be forfeited.

IV. In case the vendor fails to provide services during the warranty period as per the satisfaction of CRID, the Performance security deposited by the vendor will be forfeited.

V. In case the vendor failed to supply the ordered items as per the specification mentioned in the purchase 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.

VI. 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 Purchaser / 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 Purchaser / Client.

8.11. Authenticity of submitted Documents/Information.

i. 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 Purchaser shall issue any necessary instructions, and the priority of the documents shall be in accordance with the order as listed in the Appendix.

ii. 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.

iii. If in case, any document, information & / or certificate submitted is found to be incorrect / false / fabricated, the Purchaser at its discretion may disqualify / reject / terminate the bid/contract and also forfeit the EMD / All dues.

iv. The bidders must submit an Undertaking as placed at "Annexure-12" along with the technical bid.

8.12. Consequences of Cancellation of Order:

i. Upon cancellation of order, the successful bidder shall deliver or cause to be delivered all works carried out for and on account of the department and all data and records required from or on account of the department.

ii. 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.

iii. Upon cancellation of order for any reason whatsoever, the successful bidder shall return to the Department any and all confidential information and any other property of the Department.

iv. The department 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.

v. The successful bidder shall continue the performance of the order to the extent not terminated.

vi. Upon cancellation of order for whatsoever, CRID shall have the right to perform the following penalties:

a. Forfeiture of earnest money

b. Imposition of liquidated damage.

c. Putting supplier on holiday.

d. Blacklisting of the bidder

e. Forfeiture of bank Guarantee (s)

f. Risk Purchase on the expenses of vendor.

8.13. Termination of Contract

Termination for default

i. CRID may without prejudice to any other remedy for breach of contract, by written notice of default with a notice period of 14 days, sent to the Successful Bidder, terminating the contract in whole or part,

a. 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 CRID.

b. Or, if the Successful Bidder fails to perform any of the obligations(s) under the contract; or

c. if the Successful Bidder, in the judgment of CRID, has engaged in fraudulent and corrupt practices in competing for or in executing the Contract.

ii. In the event CRID terminates the Contract in whole or in part, CRID 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 CRID for any additional costs for such similar goods. However, the Successful Bidder shall continue the performance of the contract to the extent not terminated.

iii. Upon cancellation of the contract whatever way, CRID shall have the right to perform the following penalties: -

a. Forfeiture of earnest money

b. Imposition of liquidated damage.

c. Putting supplier on holiday.

d. Black listing of the bidder

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

8.14. Termination for Insolvency

CRID 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 CRID.

8.15. Termination for Convenience

CRID may by written notice, with a notice period of 14 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 CRID'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.

8.16. Single point of contact

The Successful Bidder shall nominate and intimate CRID, 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.

8.17. 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 CRID.

8.18. Liquidated Damages (LD)

A penalty will be levied at the rate specified in the Contract Format for non-fulfillment of delivery schedule subject to the force Majeure conditions. Even If the work is not completed in full beyond this period, such performance may entail termination of contract and black listing of the Successful Bidder from participating in any of the CRID's Tender` This alone will not relieve the Successful Bidder and the difference in cost of the items purchased through other technically qualified Bidders or any other alternative sources will be recovered from the Successful Bidder.

8.19. Other Conditions

i. The final decision would be based on the technical capacity and pricing of the Bidder. CRID does not bind itself in selecting the bidder offering lowest prices.

ii. CRID reserves the right not to accept lowest price, 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 CRID for good and sufficient reasons.

8.20. Arbitration and Jurisdiction

The Sole Arbitrator shall be the Administrative Secretary of Industries Commerce Department. The seat of arbitration shall exclusive be at Chandigarh and its language wouldbe in English only.

8.21. Documents also to be included:

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

ii. 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**

Pre-Qualification-cum-technical bid
(To be submitted on its Letterhead by the bidder)

To,
Special Secretary (IT)
Citizen Resources Information Department (CRID)
SCO 109-110 Sector 17 B, Chandigarh. 160017

Dear Sir,

Subject: e-Tender/CRID/Revenue ICT Infra/2025-26

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 Procurement for upgradation of Servers, Storage & IT related Equipment through Central Public Sector Units (PSU's) –in a Single Bid System For New Haryana Secretariat, Sector-17, Chandigarh as mentioned in the Scope of work in full conformity with the said tender document no. 2025_HRY_473189
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 180 days from the closing date fixed for submission of bid as stipulated in the Tender document.
4) 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.
5) I/We understand that CRID/Department is not bound to accept/annul any bid received in response to this Tender.
6) In case, I/We are engaged by CRID as service provider contractor for supply of ordered items/goods/items of turnkey projects, I/We shall provide all assistance/cooperation required by CRID/ 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.
7) 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 CRID from time to time.
8) 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
9) Our Entity's profile is as under:-

S#	Required Details		Remarks
1.	Legal Name of Entity		
3.	Company Identification No. (CIN)		
4.	Business Address: City District State Zip code Telephone Nos.: 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		

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

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

S#	Required Details	Remarks
1.	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	

11) 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 (Undertaking) submitted that the bidder has not been blacklisted/debarred by any central/state Government department/organization	□ Yes □ No

S#	Required Details	Remarks
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:

S#	Items Descriptions	Make & Model	Qty.	UoM
1.	Server		6	Nos.
2.	Storage		1	Nos.
3.	SAN Switch		2	Nos.
4.	Virtualization Software		6	Nos.
5.	Backup Appliance & software		1	Nos.
6.	Backup software		1	Nos.
7.	SSE		1	Nos.
8.	Next Gen Firewall		2	Nos.
9.	Anti-DDoS		2	Nos.
10.	L3 Network Switch		2	Nos.
11.	Server Load Balancer		2	Nos.
12.	Virtual Web Application Firewall (WAF)		1	Nos.
13.	Server Security Solution		1	Nos.
14.	Integrated Smart Rack		2	Nos.
15.	Installation & Commissioning	Service	1	Nos.

Note: The required Licenses will be in the name of Owner department i.e. Revenue & disaster Management Department, Haryana.

BoQ Line items break up:

S#	Items Descriptions	Qty.	UoM
1.	Server	6	Nos.
2.	Storage	1	Nos.
3.	SAN Switch	2	Nos.
4.	Virtualization Software	6	Nos.
5.	Backup Appliance & software	1	Nos.
6.	Backup software	1	Nos.
7.	SSE	1	Nos.
8.	Next Gen Firewall	2	Nos.
9.	Anti-DDoS	2	Nos.
10.	L3 Network Switch	2	Nos.
11.	Server Load Balancer	2	Nos.
12.	Virtual Web Application Firewall (WAF)	1	Nos.
13.	Server Security Solution	1	Nos.
14.	Integrated Smart Rack	2	Nos.
15.	Installation & Commissioning	1	Nos.

Note: The required Licenses will be in the name of Owner department i.e. Revenue & disaster Management Department, Haryana.

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

COMMERCIAL BID

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

To,
Special Secretary (IT)
Citizen Resources Information Department (CRID)
SCO 109-110 Sector 17 B, Chandigarh. 160017

Subject: e-Tender/CRID/Revenue ICT Infra/2025-26

I/We hereby submit our bid tender for the Procurement for upgradation of Servers, Storage & IT related Equipment through Central Public Sector Units (PSU's) –in a Single Bid System For New Haryana Secretariat, Sector-17, Chandigarh 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: -

S#	Particulars	Approx. Quantity	UoM	Make & Model	Basic Unit Price (₹)	Applicable Taxes & Duties/ GST (₹)	Unit Price (₹) All inclusive	Total Price (₹)
CAPEX: Rates for items with 1 year warranty (S# 1 to 14) and installation & commissioning								
1.	Server	6	Nos.					
2.	Storage	1	Nos.					
3.	SAN Switch	2	Nos.					
4.	Virtualization Software	6	Nos.					
5.	Backup Appliance & software	1	Nos.					
6.	Backup software	1	Nos.					
7.	SSE	1	Nos.					
8.	Next Gen Firewall	2	Nos.					
9.	Anti-DDoS	2	Nos.					
10.	L3 Network Switch	2	Nos.					
11.	Server Load Balancer	2	Nos.					
12.	Virtual Web Application Firewall (WAF)	1	Nos.					
13.	Server Security Solution	1	Nos.					
14.	Integrated Smart Rack	2	Nos.					
15.	Installation & Commissioning	1	Nos.					
OPEX: Rates for warranty from 2nd Year to 5th Year								
16.	2nd year warranty for all items (S# 1 to 19)	1	Nos.					
17.	3rd year warranty for all items (S# 1 to 19)	1	Nos.					
18.	4th year warranty for all items (S# 1 to 19)	1	Nos.					

S#	Particulars	Approx. Quantity	UoM	Make & Model	Basic Unit Price (₹)	Applicable Taxes & Duties/ GST (₹)	Unit Price (₹) All inclusive	Total Price (₹)
19.	5th year warranty for all items (S# 1 to 19)	1	Nos.					
Grand Total (CAPEX + OPEX)								

Note:
1. The L1 will be discovered on total bid value.
2. The number of items may be increased/decreased at any time.
3. The price of each of the items with 1 year warranty including installation and commissioning should be less than 75% of the total price for that item e.g. total price for CAPEX should be less than 75% of the total contract price excluding Manpower Cost.
4. OPEX cost of warranty shall gradually increase or shall remain same as previous year. If any abnormality is observed such that the later year cost is less than previous year , then the bid shall be summarily rejected.
5. 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
6. 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 purchase order unless otherwise specified in the purchase order.
7. Terms of Delivery: The landed prices quoted are inclusive of current Excise Duty, Freight, Insurance, Sales Tax, etc.
8. We agree to abide by our offer for a period of 180 days from the date fixed for opening of the "commercial e-bids" and that we shall remain bound by a communication of acceptance within that time.
9. 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.
10. Validity of commercial bid: should be 180 days from the date of opening of commercial offers
11. A company and the person signing the bid/offer is the constituted attorney.
12. The CAMC of all active Data Centre related components will be as per State Govt's. Approved CAMC Policy: https://cdnbbsr.s3waas.gov.in/s35352696a9ca3397beb79f116f3a33991/uploads/2023/02/2023020883.pdf

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

Bidding Document Acknowledgement Form
(To be enclosed with technical bid)

To,
The Special Secretary (IT) and the Treasurer, CRID
Citizen Resources Information Department (CRID)
SCO 109-110 Sector 17 B, Chandigarh. 160017
Subject: e-Tender/CRID/Revenue ICT Infra/2025-26

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 CRID 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 CRID and that the said documents are to be used only for the purpose intended by CRID. 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

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

Date: _____

From (Name of bidder)
_____
_____

Subject: e-Tender/CRID/Revenue ICT Infra/2025-26.

The Special Secretary (IT) and the Treasurer, CRID
Citizen Resources Information Department (CRID)
SCO 109-110 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 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 CRID for a period of three years from participating any tender published by Haryana Government.

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

Statutory Undertaking

(To be enclosed with Technical bid)

Date: _____

The Special Secretary (IT) and the Treasurer, CRID
Citizen Resources Information Department (CRID)
SCO 109-110 Sector 17 B, Chandigarh. 160017

Subject: e-Tender/CRID/Revenue ICT Infra/2025-26

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 practices. 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

Technical Compliance

(to be enclosed with technical bid jointly by respective OEM(s) and Bidder)

Date: _____

The Special Secretary (IT) and the Treasurer, CRID
Citizen Resources Information Department (CRID)
SCO 109-110 Sector 17 B, Chandigarh. 160017

Subject: e-Tender/CRID/Revenue ICT Infra/2025-26.

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: -

Minimum Technical Specification:

1. Server

Servers Specifications		Compliance (Yes/No)
Item	**Description of Requirement**	
Chassis	2U Rack Mountable	
CPU	Dual Intel Xeon/AMD Processor each with minimum 64 Cores each	
Chipset	Intel® C741 Chipset/SOC Design	
Memory	1024 GB RAM scalable upto 4.0 TB using DDR5 Registered DIMM (RDIMM) operating at 4800MT/s	
Bus Slots	Server should support upto eight PCI-Express 5.0 x16 slots.	
Storage	2x900GB SSD Drives for Operating System	
HDD Bays	Upto 8SFF Drive Bays	
Controller	Server should be supplied with Embedded / PCIe based x16 RAID controller with 4GB Flash backed write cache, supporting RAID 0, 1, 5, 6, 10, 50, 60. Must support mix-and-match SAS, SATA, and NVMe drives to the same controller. Controller must support 6G SATA, 12G SAS, 16G NVMe.	
Networking features	4-Port 1Gb Ethernet Network Adapter , Dual Port 10/25Gb SFP+ Network Adaptor, Dual port 32Gbps Fibre Channel HBA with transreceivers	
Interfaces	Serial - 1 (Optional) USB support with Up to 5 total: 1 front, 2 rear, 2 internal. 1GbE Dedicated management port	
Power Supply	Should support hot plug redundant low halogen power supplies with minimum 94% efficiency	
Fans	Redundant hot-plug system fans	

Servers Specifications		Compliance (Yes/No)
Industry Standard Compliance	ACPI 6.3 Compliant PCIe 5.0 Compliant WOL Support Microsoft® Logo certifications PXE Support Energy Star SMBIOS 3.2 UEFI 2.7 Redfish API IPMI 2.0 Secure Digital 4.0 Advanced Encryption Standard (AES) Triple Data Encrytion Standard (3DES) SNMP v3 TLS 1.2 DMTF Systems Management Architecture for Server Hardware Command Line Protocol (SMASH CLP) Active Directory v1.0 ASHRAE A3/A4	
System Security	UEFI Secure Boot and Secure Start support Tamper-free updates - components digitally signed and verified Immutable Silicon Root of Trust Ability to rollback firmware FIPS 140-2 validation Secure erase of NAND/User data Common Criteria certification TPM (Trusted Platform Module) 1.2 option Configurable for PCI DSS compliance TPM (Trusted Platform Module) 2.0 option Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser Bezel Locking Kit option Support for Commercial National Security Algorithms (CNSA) Chassis Intrusion detection option Secure Recovery - recover critical firmware to known good state on detection of compromised firmware	
Operating Systems and Virtualizatio n Software Support	Windows Server. Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware ESXi and Morpheous VM Essential Canonical Ubuntu Oracle Linux and Oracle VM, Citrix	
Virtualisatio n Software	Bidder should offer the server with virtualisation software as per mentioned specifications for the total no of cores/sockets mentioned in CPU section for compute virtualisation with OEM support for 5 years.	
Provisioning	1. Should support tool to provision server using RESTful API to discover and deploy servers at scale	

Servers Specifications		Compliance (Yes/No)
	2, Provision one to many servers using own scripts to discover and deploy with Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows PowerShell	
Firmware security	1. For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable 2. Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware	
Embedded Remote Management and firmware security	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication 2. Server should have dedicated 1Gbps remote management port 3. Server should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware 4. Server should support agentless management using the out-of-band remote management port 5. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 6. Two factor Authentication 7. Local or Directory-based user accounts with Role based access control 8. Remote console sharing upto 6 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support.Should provide support for AES and 3DES on browser.Should provide remote firmware update functionality.Should provide support for Java free graphical remote console. 9. Should support managing multiple servers as one via Group Power Control Group Power Capping Group Firmware Update Group Configuration Group Virtual Media and Encrypted Virtual Media Group License Activation	

Servers Specifications		Compliance (Yes/No)
	10. Should support RESTful API integration 11. System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support 12. Server should have security dashboard : displaying the status of important security features, the Overall Security Status for the system, and the current configuration for the Security State and Server Configuration Lock features. 13. One-button Secure Erase designed to decommission/repurpose servers 14. NVMe wear level display 15. Workload Performance Advisor - Provides server tuning recommendations to improve server performance	
Server Management	Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resources user is authorized to view.	
	The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware • Appliance alerts	
	The Systems Management software should provide Role-based access control	
	Zero Touch Provisioning (ZTP) using SSDP with remote access	
	Management software should support integration with popular virtualization platform management software like Vmware vCenter & vRealize Operations, and Microsoft System Center & Admin Center	
	Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.	
	Should provide an online portal that can be accessible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contrats and status. The Portal should also provide a personalised dashboard to monitor device heath, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud).	
	Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.	

Servers Specifications		Compliance (Yes/No)
	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	
	The Server Management Software should be of the same brand as of the server supplier.	
Cloud Enabled Monitoring and Management	1. Secure connection from customer sites to cloud service 2. Unified Identity & Access Management 3. Manages and controls servers regardless of physical location 4. Subscription-based entitlement 5. Efficient Device Onboarding 6. Firmware Update Awareness with Intelligent delta-only based updates 7. Set Group firmware Baseline and Compliance monitoring and notification 8. Group based firmware management that can be scheduled or on-demand 9. Remote Site management with low bandwidth/high latency network connectivity 10. Role-based access and views for managed customer environments 11. GUI and Rest APIs for core features	
Warranty	Server Warranty includes 5-Year Parts, 5-Year Labor, 5-Year Onsite support with next business day response.	
OEM Brand Eligibility	The OEM brand should be in existance for last more the 20 years in India for better support services. The OEM should be present in Leaders Quardrant for servers in Latest Gartner report. The OEM should present in the top 3 brands in IDC report. The OEM should be ISO 9001, ISO 14001, ISO 20000, ISO 27001 Certified.	

2. Storage:

Enterprise SAN Storage Specifications			Compliance (Yes/No)
Sr. No	**Parameter**	**Technical Specifications**	
1	Capacity & Scalability	Offered Storage array shall be supplied minimum with **500TB usable Capacity** using NVMe drives and shall be configured in Raid 6. Vendor shall not use more than 10D+2P while sizing the array.Offered Storage shall be able to protect against at-least 2 drives failure simultaneously within a given raid group.	
2	Memory and CPU Processing Power	Offered Storage array should have at-least 512GB memory across both controllers.Offered storage controller shall be based upon at-least PCI 4.0 technology.	

Enterprise SAN Storage Specifications			Compliance (Yes/No)
Sr. No	**Parameter**	**Technical Specifications**	
3	Host Ports and Back-end Ports	The offered Storage array shall have a minimum of 24 Front-end ports where vendor shall provide 4 dedicated ports each for connectivity of Fiber Channel, ISCSI, NVMe-of/TCP, NVMe-of/FC, NFS and IP based replication respectively. The offered fiber channel ports shall be running at 32Gbps and in future shall be upgradable to 64Gbps by replacing the SFP.	
4	Operating System & Clustering Support	The storage array should support industry-leading Operating System platforms & clustering including Windows Server 2019 / 2022, VMware ESX 8.x hypervisor, HPE Morpheus VM essentials hypervisor. Red hat enterprise Linux and SUSE Enterprise Server (SLES) etc.	
5	Data Availability and All Flash	1. The offered storage shall be a unified enterprise class storage array which can provide enterprise class resiliency & 100% data availability guaranteed architecture along with all NVMe controllers. 2. 100% data availability guaranty shall be clearly mentioned on vendor web site for the offered model. If vendors are not supporting the 100% data availability as per their web site then vendor shall quote additional Controller and 10% additional capacity as cold spare along with array for mitigating the failure situations.	
6	No Single point of Failure	Offered Storage Array shall be configured in a No Single Point of failure configuration including Array Controller card,Boot drive, Cache memory, FAN, Power supply etc.	
7	Disk Enclosures	1. Vendor shall ensure that all additional drive enclosures required within the given solution or achieving 2PB raw capacity shall be directly connected to offered controllers using dedicated 100Gbps NVMe-OF redundant links. 2. Vendor shall also ensure that each additional drive enclosure shall have dual node or dual controller where each node or controller shall have dedicated CPU and at least 64GB of memory.	
8	Storage Encryption	1. Vendors shall offer only encrypted drives with appropriate encryption licenses. Vendor shall not offer any controller based or Software based encryption. 2. The offered Storage array shall support at-least external key managers from Utimaco ESKM and Thales Cipher Trust Manager. Vendor shall also offer internal Key manager engine for key management.	
9	No. of Controllers	Storage array shall be offered with at least dual controllers where each controller shall have dual number of encrypted boot drives.	

Enterprise SAN Storage Specifications			Compliance (Yes/No)
Sr. No	**Parameter**	**Technical Specifications**	
10	Architecture & Processing Power	1. Offered storage array shall be true Active-active so that every logical disk is striped across all offered drives and all drives shall be able to contribute the IOs to both controllers simultaneously. 2. Offered storage array shall have native virtualization support so that Raid can be carved out from a logical space instead of dedicating separate physical disks for each application.	
11	Cloud Native data console Management	a. Common Dashboard for all managing multiple arrays through a single cloud native data console. b. Main Dashboard shall provide the information of Total number of Arrays, Volumes, hosts, Capacity and performance information of top Arrays and Volumes. c. Common role-based access control for managing multiple arrays through a single data console instead of creating users and assigning roles individually at each array. d. Common Audit management for all arrays e. Shall have capability for tagging the Storage volume to given host applications so that performance charts can be drawn for application instance for easy management and troubleshooting. f. Offered console shall advise about Placement of application on best fit system based on workload after application tagging. g. Shall be able to provide the context aware software updates on the storage array. h. Shall be able to offer storage management and configuration as a service instead of controlling, patching, and upgrading the management application by onsite team.	
12	Cloud Enabled - Monitoring and Analytics	Cloud Enabled Monitoring and analytics engine shall have capability to provide following: a. Providing Firmware update path, previous version, readiness check before applying the update to production environment and severity level for required firmware update. b. Dashboard shall clearly highlight whether there is any issue with array and shall provide the detailed	

Enterprise SAN Storage Specifications			Compliance (Yes/No)
Sr. No	**Parameter**	**Technical Specifications**	
		information about the issue. c. The dashboard shall provide consumption and capacity forecast trend for overall capacity planning. d. Providing granular near real time performance analysis, at-least at an interval of 5 minutes. It shall allow to create custom reports in csv and PDF format without the need for enabling extra logging, installing any appliances (physical or virtual), or installing any software. e. Providing overall headroom utilization of the array while combining and analyzing various parameters like IOPS, MB/sec, Block size, Latency etc. f. Headroom utilization shall clearly provide the breakup of headroom consumed by the Volumes or tagged application at storage array g. Providing the status of at-least top 5 volumes where latency is extremely high. It shall also provide shading functionality so that more severe hotspot can be easily identified.	
13	Resource Planner	The offered Cloud native dashboard shall also provide the functionality for future workload planning on the offered storage using at least the following parameters: a. Window to provide the newer workload characteristics – Number of new volumes, type of application, Average Read and write IO size, Number of read and write IOPS, Capacity growth per week etc. b. The workload planner shall clearly advise whether the above additional workload characteristics can be serviced on the storage array offered. c. The Workload planner shall also provide the detailed report with workload inference.	

Enterprise SAN Storage Specifications			Compliance (Yes/No)
Sr. No	**Parameter**	**Technical Specifications**	
14	Cloud Enabled - Anomaly Detection	Cloud enabled Advance Analytics engine shall have capability to provide following: a. Analytics engine shall have an overall resource contention analysis page where it shall be able to highlight the CPU and disk utilization contention and associated volumes which are causing the contention. b. Analytics engine shall have in-built anomaly detection for a given storage volume so that it can provide the variance insight of high LUN latency / response time. c. Analytics engine shall clearly mark all those anomaly detection points on the given LUN / Volume latency graph and shall be applicable for both read and write operations. d. Anomaly detection shall also be applicable for a given storage volume throughput so that drift of workload can be easily identified from the usual read and write pattern. e. Sustainability metrics reports including carbon utilization emissions and energy consumption.	
15	Global Hot Spare	1. offered Storage Array shall support distributed Global hot Spare for offered Disk drives. 2. Global hot spare shall be configure as per industry practice.	
16	Quality of service	1. Offered storage array shall support quality of service for critical applications so that appropriate and required response time can be defined for application logical units at storage. It shall be possible to define different service / response time for different application logical units. 2. Quality of service engine shall allow to define minimum and maximum cap for required IOPS / bandwidth for a given logical units of application running at storage array. 3. It shall be possible to change the quality of service Response time (In both milliseconds as well as Sub-milliseconds), IOPS, bandwidth specification at real time.	

Enterprise SAN Storage Specifications			Compliance (Yes/No)
Sr. No	**Parameter**	**Technical Specifications**	
17	Capacity efficiency	1. Offered storage array shall support inline data efficiency engine (Supporting Thin Zero detect and re-claim, De-duplication and Compression) and shall be enabled by default. 2. Vendor shall have flexibility to enable / disable the data efficiency engine at the time of Volume creation. 3. Storage subsystem shall be supplied with Thin Provisioning, Thin Re-claim, Snapshot, remote replication, De-duplication, Compression, Performance Monitoring, and Quality of service on day 1 for the supplied capacity of the array.	
18	Firmware Upgrade	Offered storage shall support online non-disruptive firmware upgrade for both Controller and disk drives.	
19	Ransomware Detection	1. The offered storage shall have in-built inline data-adaptive ransomware detection engine for Block Volumes. 2. Ransomware detection engines shall be completely based upon dynamic calculation of trigger thresholds using in-built training periods and by analysing the write data path instead of using traditional approaches like measuring CPU utilization, change of data rate, data reduction efficiency ratios and data entropy. 3. It shall be possible to select a specific set of volumes or group of volumes to be enabled for Ransomware detection for block data. 4. It shall also be possible to adjust the balance between sensitivity of detection process and false positives events for effective detection process. Vendor shall provide required configurable parameters or handlers for same. 5. Ransomware detection engine shall be truly intelligent by creating an immediate creation of alert snapshots after noticing the suspicious event. 6. It shall also be possible to export the ransomware detection logs to a remote server, such as a SIEM or XDR and Call home support.	

Enterprise SAN Storage Specifications			Compliance (Yes/No)
Sr. No	**Parameter**	**Technical Specifications**	
20	Snapshot / Point in time copy, No. of Volumes and Temper-proof protection (Ransomware Protection)	1. The storage array should have support for controller-based snapshots (At-least 1024 copies for a given volume). 2. The system must provide the capability to create immutable, read-only snapshots, that cannot be modified. 3. The system shall provide the capability to create compliant, read-only snapshots, which makes it impossible to modify or delete the snapshot and its base volume by the user, a system administrator, and the manufacturer. 4. The protection period of the above snapshots must be individually configurable between 1 minute and several years. Changing the system clock must not allow the tampering of protection.	
21	Remote Replication	1. The storage array should support hardware based data replication at the array controller level across all models of the offered family. 2. Offered Storage array shall support both Synchronous and Asynchronous replication across 2 storage arrays natively without using any third party or software based solution. 3. Offered storage array shall have capability to create the application consistency group for replication operations. Shall have flexibility to have more than 256 volumes per consistency group. 6. Offered storage subsystem shall support incremental replication after resumption from Link Failure situation or during failback operations.	
22	Active / Active Stretch Clustering	1. Offered Storage array shall have capability to provide true Active / Active Replication and Stretch clustering at metro distances for Zero RPO and RTO so that a given volume pair between primary and DR location can have concurrent access to both read and write operations simultaneously. 2. Active / Active replication shall be supported for all well-known OS like VMware, Redhat, Windows etc.	
23	Multi-tenancy	Offered storage array shall be true multi-tenant and shall support at-least 128 Tenant per storage array. Every tenant shall be treated as a separate logical storage array with its own user control access.	

3. SAN Switch:

SAN Switch Specifications		Compliance (Yes/No)
Sr. No.	**Specifications**	
	Architecture/Scalability/Performance/Management/Availability:	
1	Minimum Dual SAN switches shall be configured where each SAN switch shall be configured with minimum of 24 Ports scalable.	
2	Required scalability shall not be achieved by cascading the number of switches and shall be offered within the common chassis only	
3	Should deliver 32 Gbit/Sec Non-blocking architecture with 1:1 performance for up to 24 ports in a energy-efficient fashion	
4	Should protect existing device investments with auto-sensing 16, 32, and 64 Gbit/sec capabilities.	
6	The switch should be rack mountable	
7	Offered SAN Switch shall support less than 460 nanoseconds for port to port latency with no contention.	
8	Offered switch shall support at-least 2000 dynamically allocated frame buffers.	
9	The switch shall provide Aggregate bandwidth of 1.536 Tb/sec.	
10	Switch shall have support for web based management and should also support CLI.	
11	The switch should have USB port for firmware download, support save, and configuration upload/download.	
12	Offered SAN switches shall be highly efficient in power consumption. Bidder shall ensure that each offered SAN switch shall consume less than 110 Watt of power.	
13	Switch shall support POST and online/offline diagnostics, including RAStrace logging, environmental monitoring, non-disruptive daemon restart, FCping and Pathinfo (FC traceroute), port mirroring (SPAN port).	
14	Offered SAN switch shall support services such as Quality of Service (QoS) to help optimize application performance in consolidated, virtual environments. It should be possible to define high, medium and low priority QOS zones to expidite high-priority traffic	
15	The switch shall be able to support ISL trunk up to 512 Gbit/sec between a pair of switches for optimal bandwidth utilization and load balancing.	
16	SAN switch shall support to restrict data flow from less critical hosts at preset bandwidths.	
17	It should be possible to isolate the high bandwidth data flows traffic to specific ISLs by using simple zoning	
18	The Switch should be configured with the Zoning and shall support ISL Trunking features when cascading more than 2 numbers of SAN switches into a single fabric.	
19	Offered SAN switches shall support to measure the top bandwidth-consuming traffic in real time for a specific port or a fabric which should detail the physical or virtual device.	

4. Virtualization Software

Virtualization Software Technical Specifications			Compliance (Yes/No)
Sr. No	**Parameter**	**Technical Specifications**	
1	Platform	The offered Hypervisor software shall be qualified for both Intel and AMD architecture and shall have capability to provide high availability.	
2	Hypervisor Vendor	The offered hypervisor shall be either from Broadcom VMware, HPE, Microsoft or Nutanix.	
3	Guest Operating System	The offered Hypervisor shall be supported with all leading Guest Operating Systems.	
4	Availability Features	1. The offered Hypervisor shall support migration of a running virtual machine from one host to another within the same cluster with zero downtime.	
		2. The offered Hypervisor shall automatically restart virtual machines on another host in the same cluster in the event of an unexpected host failure within the cluster.	
		3. The offered Hypervisor shall dynamically schedule the placement of virtual machines within a cluster based upon optimal workload distribution across the cluster.	
		4. The offered Hypervisor shall support migration the virtual disk(s) of a running of virtual machine from one storage datastore to another with zero downtime.	
5	Data Protection	1. The offered Hyper-visor Shall have in-built data backup solution which shall be able to protect VM and Hosts to Target Storage provider.	
		2. Native backup engine shall be able to use at least CIFS, NFS, S3 from Storage providers as a backup target.	
		3. In case vendor Hypervisor doesn't have in-built data backup solution then vendor shall provide additional backup software for the complete hardware and software configuration asked in the RFP.	
		4. The offered integrated backup software shall be deeply integrated into the instances / VM provisioning window so that all newly created instances / VMs are protected and backed up automatically.	
		5. The offered integrated backup software shall support critical features like Scheduling of backup, backup retention counts, on-demand backup etc.	

Virtualization Software Technical Specifications			Compliance (Yes/No)
Sr. No	Parameter	Technical Specifications	
		6. The offered Hypervisor shall support and integrate with storage - Object Buckets which can be used for Backup, Archives, Deployment and Virtual Images storage targets.	
		7. It shall be possible to browse, upload, download, or delete files from Bucket and shall support all well-known object storage from AWS, Azure, Google, Dell-EMC ECS, Openstack Swifts buckets etc.	
		8. The offered Hypervisor shall also allow creation of file share based NFS and CIFS protocols which can be used for Backup, Archives, Deployment and Virtual Images storage targets.	
		9. It shall be possible to browse, upload, download, or delete files from File share and shall support all various file share protocols like CIFS, NFS, Local Storage and all well-known industry leading file storage arrays.	
6	External Storage Integration	The offered Hypervisor shall support running virtual machines on external storage via iSCSI, NFS, and Fibre Channel	
7	Automation Capabilities	1. The offered Hypervisor shall execute Bash or PowerShell scripts during virtual machine provisioning to automate system bootstrapping operations.	
		2. The offered Hypervisor shall also support the execution of Bash and PowerShell scripts on provisioned and discovered virtual machines like an operational workflow.	
8	Identity Services	1. The offered Hypervisor shall have internal user management engine, integration with external directory-based providers – Active directory and LDAP, SAML based providers – Okta, Onelogin, Azure AD SAML etc.,	
		2. It shall be possible for mapping of External integration provider users with offered hypervisor roles.	
9	IP Address Management	The offered Hypervisor shall have Integration with external IPAM providers like Infoblox, phpIPAM, BlueCat, SolarWinds etc. to automate the reservation of an IP address for the virtual machine during the provisioning process.	
10	DNS Integration	The offered Hypervisor shall have Integrate with external DNS providers like Infoblox, Microsoft DNS, BlueCat, SolarWinds etc. to automate the creation of DNS records for a virtual machine during the provisioning process.	

Virtualization Software Technical Specifications			Compliance (Yes/No)
Sr. No	**Parameter**	**Technical Specifications**	
11	Resource Allocation	The offered Hypervisor management engine shall have a concept of grouping of resources into a common identity, comprises of resources like Clouds, hosts, VMs, network, resource pools, data stores etc. so that required users can be assigned to it.	
12	User Profile	The offered hypervisor management engine shall allow users to configure their photo, username, password, email, theme, 2FA, Linux and Windows VM login credentials from the console	
13	Private Cloud Integration	The offered Hypervisor management engine shall support additional private cloud provider and hypervisor, preferably VMware, from the common interface without any additional coding.	
14	Service Plans	1. The offered hypervisor Management engine shall allow administrator to create service plan or t-shirt size based on CPU, Memory and Storage and shall be available to users while creating / provisioning the instance / VMs	
		2. Services plan shall also have the option to provide custom ranges and flexibility to provisioning users for providing predefined limit for number of additional volumes, customization of Volumes, number of cores etc.	
15	Expansion / Shrink	The offered Hypervisor shall support both expansion and shrinking of VM cluster.	
16	RBAC	Access to grouping of resources shall be controlled through appropriate roles while assigning to users. Roles shall provide access to resources using appropriate permissions. At-least, it shall be possible to configure following key permissions:	
		a. Access to Native data protection configuration.	
		b. Read or full access for creation of Service plans.	
		c. Access to API to executes scripts on Instances / VM.	
		d. Access for allowing users to use Dynamic workload schedular for VM placement and pinning of VM to a specific host.	
		e. Access for creating the automation scripts.	
		f. Permission for resizing the instance.	
		g. Access to instance / VM – Console, Adding or deleting an Instance / VM.	
17	Virtual Machine Management	1. The offered Hypervisor shall support below features for Virtual Machine Management:	
		a. Create / Delete / Restart / Start / Stop / Suspend and Discovery of Virtual machines.	
		b. Snapshot operations – Create / Delete / revert of Virtual machines	

Virtualization Software Technical Specifications			Compliance (Yes/No)
Sr. No	Parameter	Technical Specifications	
		c. Tagging – Add / Delete / Edit tagging for Virtual Machines.	
		d. Live Migration of VM, VM HA and Pin virtual machine to a specific host.	
		e. Cloning of VM, Clone to VM Template.	
		f. Virtual Hardware Management - Add and remove virtual hardware such as hard disks, network interfaces, CPU and memory from a managed virtual machine.	
		2. The offered Hypervisor shall ensure that child snapshots of the restored snapshot are preserved instead of automatic deletion.	
18	Pass through Support	1. The offered Hypervisor shall have passthrough support for PCI and NVMe devices.	
		2. The offered Hypervisor shall support the passthrough support for GPU and USB devices.	
19	Credential Store	The offered Hypervisor shall support both internal and external Credential store for securely pulling in the username and password, access and secret key along with key pair and SSH certificates.	
20	Virtual Images	1. The offered hypervisor software shall provide the flexibility to bring / upload OS images.	
		2. While uploading the OS image, it shall be possible to define the location and provide the flexibility to use internal space within the hypervisor cluster or using appropriate available S3 bucket or file share.	
21	Licensing	1. Vendor shall ensure that offered Hypervisor is licensed per socket.	
		2. In case vendor is not supporting the socket-based licensing then vendor can configure Core based licensing as well however vendor shall provide at-least 128 core license per configured physical server or actual provisioned cores per server, whichever is higher.	
22	Upgrade	1. It shall be further possible to upgrade the offered Hypervisor to full-fledge Cloud management platform so that all required functionality of Cloudops (Cloud operations for VM, and Container platforms), SecOps (Security and Control), Devops (Automate and Orchestrate) and Finops (Visualize and optimize) can be achieved with appropriate RBAC controls.	
		2. After upgrading the Hypervisor to full-fledge cloud Management, it should become truly heterogenous and	

Virtualization Software Technical Specifications			Compliance (Yes/No)
Sr. No	Parameter	Technical Specifications	
		shall quickly integrate with below tools / Platforms / integrations:	
		a. Hypervisors: VMware, Nutanix, HPE VME, Microsoft etc.	
		b. Clouds: AWS, Azure, GCP, IBM, Oracle, Alibaba, Digital Ocean, Openstack etc.	
		c. Identity: Active Directory, Okta, SAML, LDAP, Onelogin etc.	
		d. Network: NSX, ACI, Infoblox, Bluecat, SolarWinds etc.	
		e. Load Balancers: F5, A10, Citrix, ALB, Azure Load Balancer etc.	
		f. Backup: Native Backup functionality, Veeam, Commvault, Zerto etc.	
		g. ITSM: ServiceNow, Cherwell, BMC-Remedy etc.	
		h. Container – AKS, EKS, GKE, Kubernetes, KVM cluster etc.	
		i. Automation – Chef, Puppet, Ansible, Ansible tower, VMware Orchestrator etc.	
23	Global Search	The offered Hypervisor shall provide global search to facilitate search of Instances, Users, cloud, group, hosts and networks.	
24	Wiki	The offered Hypervisor shall allow creation of Wiki, which shall be RBAC-controlled, auditable Wiki that allows easy access to information, notes, configurations or any other data needed to be referenced or shared with others.	
25	Dashboard	Consolidated dashboard for the offered Hypervisor shall highlight the overall environment status, System Status, Alarms, log history, Instance status, Instance status by configured clouds, cluster workloads etc.	
26	Activity Report	1. The offered Hypervisor management engine shall provide activity report like provisioning tasks , Users related tasks etc.	
		2. It shall be able to search the specific activity.	
27	Image Conversion / Migration	The offered Hypervisor shall support conversion of VMware image to offered Hypervisor supported image format from the VM Migration perspective. Vendor shall provide this functionality either natively to offered Hypervisor management engine or shall factor additional software on Day 1 to achieve it.	
28	Multi-Cluster Management	Vendor shall provision required management software for managing multiple clusters, at least 10 clusters, on day 1 for the offered configuration.	

5. Backup Appliance and Software

Purpose Built Backup Appliance		Compliance (Yes/No)
Parameter	**Minimum Specification**	
General Features	The offered purpose-built backup appliance should be sized appropriately for backup of front-end data of 600 TB (40% DB & 60% VM & File System) as per below mentioned backup policies: a. Daily incremental backup – retained for 4 weeks in the backup appliance. b. Weekly full backup for all data types – retained for 4 weeks in the backup appliance. c. Monthly full backup – retained for 12 months in the backup appliance. d. Yearly full backup - retained for 5 years in the backup appliance. The proposed purpose-built backup appliance must be sized for adequate capacity considering 2% daily data change rate for the contract period. Any additional backup storage capacity, software and any other component required as per sizing needs to be provided by the MSI and OEM at the time of bid. Bidder must provide the backup appliance sizing on OEM's letter head with seal & sign from the authorized signatory basis the backup retention policies.	
	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.	
	Must support Inline and Global data de-duplication technology (without excluding any file/part thereof) at block level using variable block length technology	
	VTL Appliance must support High Availability of multiple components like Controller, CPU, FAN, backup storage, network and FC ports etc. without single point of failure for any component. The dual controllers must be active passive so that the performance does not degrade even in case of controller failure.	
Feature	PBBA VTL Appliance should be configured with RAID 6 or DDP or equivalent along with hot spare disks.	
	The proposed appliance must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism. All file system data and Metadata must be verified continuously even if parts of the file system are never accessed for reads (Automated Data Scrubbing Process)	

Purpose Built Backup Appliance		Compliance (Yes/No)
Parameter	**Minimum Specification**	
	The proposed appliance must provide a mechanism to restrict any date and time change of the system to protect against any accidental or intentional expiration of data through change in the Network Time internally or externally to the system	
Feature	As PBBA VTL Appliance, solution 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.	
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.	
Feature	Software Licensing:	
Feature	LAN/SAN Connection: Minimum 8 x 10/25 Gig SFP+ (fully populated) along with 8 x 32Gbps FC ports with all required accessories.	
Feature	PBBA VTL appliance should have support for Encryption, Deduplication and Replication (Replication from appliances to appliances over TCP/IP network) from Day1.	
Feature	PBBA should have manual/Automated Data Integrity check for backup data on device	
Feature	The proposed appliance should be able to deliver a throughput of up to 75 TB/hr (at target side) Or more, considering with/without deduplication and compression ratio. Deduplication and compression must be ensured at source and target/backup appliance end.	
Feature	Scheduling:	
	a. Backup software used in PBBA should be able to retrieve data from tape to client server directly.	
	b. logs & reports e.g. de-duplication report, Data growth analysis report, Compute utilization report during backup etc.	
Feature	PBBA based backup solution should support following replication capabilities:	
	a. Subsequent Replication should transfer only difference data from previous successful replication.	
	b. Replication should provide the flexibility to transfer only dedup data.	
	c. should provide compression of data while replication.	
	d. Proposed appliance should support bi-directional, many-to-one, one-to-many, and one-to-one replication.	

Purpose Built Backup Appliance		Compliance (Yes/No)
Parameter	**Minimum Specification**	
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.	
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	
Protection & retention	Proposed appliance should support retention lock/retention/ Immutability feature or any other to ensure that no data is deleted/overwritten accidently and support for point-intime copies of a LUN or volumes with minimal performance impact.	
Updates and patch support	Software updates and patches: For the period of minimum 5 years and as per scope of this RFP.	
Warranty & Post warranty Support	5 years On-site comprehensive warranty with 24x7x365 solution (Hardware & associated software) support and 2 years post warranty support as per Haryana States' CAMC/AMC policy	

6. Backup Software

Backup Software		Compliance (Yes/No)
S.No.	**Minimum Specifications**	
1	The proposed Backup software must offer instance based licenses with no restrictions on type of arrays (protecting heterogenous storage technologies), front end production capacity or backup to disk target capacity restrictions.	
2	Backup software should have Capability to do trend analysis for capacity planning of backup environment, extensive alerting and reporting with pre- configured and customizable formats. Any specialized reporting modules needed must be quoted along with associated hardware to achieve this functionality. All necessary hardware resources required to run this module should be supplied.	
3	Proposed solution should support 24x7 real-time monitoring, with at-a-glance and drill-down views of health, performance and workload of the virtual hosts.	
4	Proposed solution should have security and compliance dashboard inbuilt with the product.	
	Proposed solution should support automated action for popular alarms (automated or semi-automated), with at-a-glance and drill-down views	

5	of health, performance and workload of the virtual hosts.	
6	Software should be able to restore VMs to a cloud service provider like AWS, Azure or Google directly from the backup copy.	
7	Software should be able to extend the backup repository to a public cloud service provider by moving older files to any S3 Compatible Object storage or Azure BLOB repositories.	
8	Backup software should should have capability to archive data to Amazon Galcier or Microsoft Azure storage Arhive Tier or any S3 Storage. The Software must have capability to restore the data from archive tier, it should not be dependent on cloud vendor.	
9	Backup software should support agentless backups of applications reisding in VMs like SQL, Exchange, Sharepoint, Oracle, etc. with non-staged granular recovery of all these applications. It should support crash consistent VM level backup for all other workloads. Backup software should support SAP HANA backup integrated with HANA Cockpit	
10	The software must has the functionality to backup on-prem data directly into cloud repositories such as AWS S3 or Microsoft Blob.	
11	Proposed backup software should be able to leverage Immutable Cloud based storage like S3-Immutable service to prevent backup copies of data from any corruption or ransomware attacks.	
12	The proposed soloution should have on demand scans available for malaware attacks.	
13	The backup Software must have inline detection & in guest detection via guest indexing against any malware attacks.	
14	The proposed backup software should have four eyes apporval for any backup deletion.	
15	Backup software should be a Hardware Agnostic software and it should support snapshot integration with hypervisors like VMware, Hyper-V, Nutanix AHV nad RHEV and support de-duplication on any storage target. It should be able to backup data to tapes (like LTO) or as well for long term retention on S3 storage.	
16	The proposed backup software should provide Instant recoveries for any backup to Vmware or Hyper-V or Acropolis Virtual machine.	
17	Backup software should support file level recovery from any backup of any VM or physical server. It should support a full system recovery in case of a system crash, either on a physical system or virtual machine or as a Cloud Instance(AWS, Azure or Google)	
18	The Proposed backup Software should supprot Syslog and Service Now integration.	
19	Backup software should support instant database recoveries of MS SQL and Oracle from the backup files.	
20	Backup software should support Multi factor authentication for accessing Backup console and console auto log-off functionality.	
21	Backup software must have a feature of data validation, whereby a workload (VM with OS and application) is powered-on in a sandbox environment and tested for its recoverability.	
22	Recovery verification should automatically boot the server from backup and verify the recoverability of VM image, Guest OS and Application	

	Consistency and then publish automated reports to be used in backup / recovery audits.	
23	Backup software should provide Backup and Replication capabilities in one console only and also allow users to integrate with RBAC capabilities of the hypervisor, so that users can initiate backup and restore only those VMs to which they have access, without administrator intervention, thereby delivering self serve capabilities.	
24	Proposed backup software should be able to Hardened the Linux Repository. This service will prevent backup copies of data from any corruption or ransomware attacks.	
25	The software should support Group Managed Service Accounts which should have an option to users to allow change passwords after every 30 days and allows for complex password policy.	
26	The proposed backup should have object storage backup.	
27	Proposed backup software should have the ability to perform staged restores to enable admins to comply to regulations by selectively deleting files / records which should not be restored from the backup copies. This will help in complying to "right to be forgotten" regulations like GDPR, where user data is deleted from restored backup copies in an auditable manner.	
28	The proposed Backup software must allow to configure the maximum acceptable I/O latency level for production data stores to ensure backup and replication activities do not impact storage Availability to production workloads.	
29	Backup software should provide Recovery of Application Items, File, Folder and Complete VM recovery capabilities from the image level backup within 15Mins RTO.	
30	The software should be Network-efficient, Secure backup data replication with variable-length encryption at the source, along with compression and encryption to ensure that backups are optimized for WAN transmission. This should be ensured with or without need of any other 3rd party WAN Accelerator requirements.	
31	Bidder need to provide the 40VM license. Backup software should support for Virtual machine and volume backup.	

7. SSE

S.No.	Technical Specifications & Functional Requirement	Compliance (Yes/No)
1	The proposed SSE solution must be cloud native platform and the OEM should have services hosted in atleast 2 Meity-empanelled cloud service provider's data centres in India.	
2	The proposed SSE solution must have SWG, CASB Inline, Browser Isolation and ZTNA capabilities from day 1.	

S.No.	Technical Specifications & Functional Requirement	Compliance (Yes/No)
3	The Bidder must propose the above solution from a single OEM and the OEM must be a leader in SSE Gartner Magic Quadrant in the last 2 years consecutively.	
4	The proposed solution should support integration with ADFS, Microsoft Azure AD and multiple other leading identity providers that support standard-based SAML 2.0 Identity Provider capability for user authentication.	
5	The solution provider must be certified against internationally recognized government and commercial standards - frameworks such as ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC 2 and CSA - Star	
6	The proposed solution must have the following ways to steer traffic to the cloud service - Agent based option - IPsec Tunnel - Proxy PAC File	
7	The solution must provide a dedicated data plane in the cloud where each user/application data transaction is processed through the cloud components which. are dedicated to <Name of the cutsomer>. Bidder to confirm the same by submitting a supporting document from the SSE vendor.	
8	The solution provider must provide secure access to all RFP features from a single software agent.	
9	All the mentioned SSE services in the RFP must be delivered from a single management and configuration console. The Management, Control, Data and Logging planes of the SSE service must be hosted in India for <Name of the cutsomer>.	
10	The bidder must ensure the proposed SSE platform has a built-in 1 year log retention for all the SSE services mentioned in the RFP. If this is not the case, bidder to factor additional analytics tools and log storage as part of their solution to meet the requirement. The support and warranty period and SLA's for any additional tool must be the same as the SSE platform.	
11	The SSE agent must have a password protection to prevent users from uninstalling the agent without the password.	
12	The OEM support shall be 24x7x365 and allow support calls to be raised through web portal at any time schedule.	
13	The solution must have Premium Support and include Customer Success Manager and Customer Success Engineer assistance.	
14	The proposed solution must have an uptime of 99.999 per cent per month for all proposed services/security engines.	
	Secure Web Gateway	
1	The solution must support both a tunnel and proxy deployment modes to secure internet traffic. The solution must be able to provide SSL inspection/Decryption at scale for all the internet bound HTTPS traffic.	
2	The solution must be able to secure access to all HTTP and HTTPS traffic on well known ports 443, 80 and customer ports such as TCP 8700, etc. The solution must support capability to apply controls to allow/restrict websites on custom ports.	

S.No.	Technical Specifications & Functional Requirement	Compliance (Yes/No)
3	The solution must have granular options to define the access policies. The options must include user based, group based, service based, application based, network based and device posture based policies.	
4	The SWG must have granular category based web controls for controlling access to Adult, Hacking, Cryptocurrency, Malware, Phishing, Parked, Grayware websites. The SWG must have alteast 70 predefined categories for URL filtering.	
5	The SWG must have a phishing prevention capability. It must have the feature to identify user's corporate credentials and prevent them from being submitted to those internet websites which are allowed in the organization as per the business requirement, but user's are not not authorised to be logged-in with corporate credentials. The admin must have flexibility to enable this capability for selective categories.	
6	The SWG must have firewall capabilities to secure internet traffic on all TCP and UDP ports. It must allow admin to create alteast 500 firewall rules/policies and support policies based on application signature/ID's and user identities.	
7	The SWG must provide a dedicated Public IP address to <Name of the cutsomer> at each Cloud Compute location to redirect specific Government/Other Internet Websites via these Dedicated Egress IP's.	
8	The SWG must have inline Advance Threat Protection (ATP) for the Internet and SaaS applications. The inline Malware prevention must prevent file based malware also from being downloaded. The solution must be able to prevent malware downloads on both HTTP and HTTPS websites. The sandbox must support multiple filetypes including PE, DMG, MS Office, PDF, Script, etc.	
9	The SWG should prevent fileless malware such as javascript, powershell, shell scripts, ELF.	
10	The SWG should be able to prevent unknown phishing websites that use phishing kits or stealthy techniques such as cloaking, website cloning.	
11	The SWG should prevent phishing attacks using known Saas platforms such as Onedrive, Wix, Wordpress, Google Drive etc.	
12	The SWG must have Advance DNS Security control to prevent DNS based attacks such as DNS tunneling, Domain Generation Algorithms, DNS based exfiltration, Command & Control.	
13	The SWG must prevent advanced DNS techniques such as Strategically aged domains, Slow/Ultra Slow tunneling, Dictionary DGA etc.	
14	The SWG DNS Security functionality should support enforcing sinkholing for malicious DNS requests to identify the actual source. It must also prevent DNS attacks on DoH (DNS over HTTPS), DoT (DNS over TLS). Additionally it must provide control to block or allow DoH/DoT.	
15	The SWG must have advance Sandbox capbilitie to prevent zero-day attacks. The Sandbox must support multiple filetypes including but not limited to archives, executables, msoffice files, Script (BAT, JS, VBS, PS1, and HTA) files , JAR Files, Archive (RAR, 7-Zip, ZIP) files, pdfs and other web content like adobe flash, java applet, ELF, DMG and HTML.	
16	The solution should have the capability to ingest IOC's from external sources.	

S.No.	Technical Specifications & Functional Requirement	Compliance (Yes/No)
17	The solution must have File Type control to prevent download of risky file types in the organization. The file type control must support alteast 200 filestypes.	
18	The solution must have Isolation capabilities to allow risky website access with granular conrols like copy-paste restrictions, Screenshots controls, etc. This capability must be supported for all SWG users.	
19	The SWG must have capability to block TOR and TOR Bridges, control unknown-tcp and unknown-udp based applications, protection from spyware, command & control, botnet, toolbar based threats. The solution should have a dedicated Ransomware protection.	
	Cloud Access Security Broker	
1	The solution must have detailed risk info of SaaS applications including capabilities, certifications and compliances and support a schedule based risk report.	
2	The CASB must support 70,000+ cloud applications for a better visibility and control.	
3	The CASB must support tenant restrictions on multiple applications including O365, Gmail, Github, Dropbox, etc. to restrict access to only authorized corporate tenant.	
4	The CASB must provide granular control for SaaS applications. The controls should include upload, download, allow, block, chat, streaming, share, delete, edit, etc. controls for different applications.	
5	The CASB must support controls for AI applications such as ChatGPT with restrictions for uploading/posting sensitive data.	
6	The CASB must support specific function based controls such as upload,download,sharing,editing. Examples - Dropbox upload, teams download/upload, github posting / copilot etc	
7	The CASB must support dynamic application based control Office 365, Zoom, Webex, Teams, WhatsApp, etc. SaaS applications which are being accessed through thick clients of the respective SaaS application.	
	Zero Trust Network Access	
1	The ZTNA solution should allow remote users to securely access private applications hosted in the data centre following the zero trust principle of least-privilege access.	
2	Solution must support user authentication through SAML 2.0 Identity Provider. It must support Multi-Factor Authentication through SAML.	
3	The ZTNA solution must support user authentication for private application access through LDAP, AD, Radius, OAuth, and Client Certificate authentication methods also for integration with the customer's existing user database.	
4	Users must connect to ZTNA service to ensure only authorized user traffic comes to the customer's data centre. The solution must have a zero trust architecture with seperate control plane, data plane and logging.	
5	Solution must support ZTNA: for web based and non-web client to server applications including smb for file share.	
6	Solution must support ZTNA: for server-to-client apps such as SCCM, VOIP, Inventory applications etc.	

S.No.	Technical Specifications & Functional Requirement	Compliance (Yes/No)
7	ZTNA solution must have built-in capability to do inline threat inspection of the private application traffic from day 1. The inspection capability should include antivirus, anti spyware scanning, vulnerability detection, IPS, decryption, etc.	
8	The ZTNA solution must provide a dedicated data plane in their cloud to process the customers application data. The ZTNA vendor must maintain complete isolation of data plane in their cloud ensuring the components processing one customer data is not shared with any other customer. At no point in time customer's application traffic must intermix with any other customers of the ZTNA service.	
9	The ZTNA endpoint agent must support both IPSEC and TLS protocols for tunnel establishment.	
10	The solution must have at-least 1 year built-in log retention in the ZTNA service without any limit on the log data. Additionally, the solution must be able to integrate and forward logs to the Syslog and SIEM solutions. Built-in logs retention should be part of ZTNA service, and the bidder must not propose 3rd party servers/hardware for log retention.	
11	The ZTNA solution must be able to support access to legacy private applications that do not accept connections from natted IP addresses of a connector.	
12	Solution must support Zero Trust Network Access with an outbound tunnel approach without needing to open any ports inbound to private applications from unknown Public IP address/addresses.	
13	The ZTNA solution must support Browser based acces to private web applications without the need of deploying ZTNA client. Bidde to provide browser based access license for all ZTNA users.	
14	The browser based access must support isolation with copy/paste, screenshot and watermarking controls to secure access to the private web applications as an when require with license	
15	The solution must support IPsec Tunnel capability to connect ZTNA service with Customer Datcentre. This capability is essential for data centre/site locations where deploying a virtual machine (connector) is not possible. Bidder must ensure atleast 5 IPSec tunnels are included in teh solution.	
16	The private application and internal Firewall must get visibility of the ZTNA user IP address for auditing, forensics and compliance requirements.	
17	The ZTNA solution must allow the customer to assign IP address to the ZTNA agent from their preffered IP address range or subnet.	
18	ZTNA must support high availability of connectors to ensure no disruptions in the event a connector goes down.	
19	Each ZTNA Connector must be able to support 1 Gbps throughput.	
20	The ZTNA agent must be able to check missing windows patches, OS, Antimalware, Firewall, Disk Backup, Disk Encryption, Machine Domain, Registry, Process, Certificate, DLP service on the user endpoint as part of the device posture check conditions.	
21	The user device posture must be continuously verified and systems with change in posture must be restricted from application access.	

S.No.	Technical Specifications & Functional Requirement	Compliance (Yes/No)
22	ZTNA must support TCP and UDP applications over FQDN and IP Address. Wildcard FQDNs must be supported to enable the organization to easily onboard multiple applications.	
23	The ZTNA agent must have anti-tampering capability to prevent users from uninstalling or disabling the agent without a password.	
24	The solution must have a single management console for the private and internet application access. The policy configuration and enforcement must be done from a single console.	
25	ZTNA must have automated discovery capability to discover applications within the organization for ease of onboarding.	
26	ZTNA must support routing users to the nearest application instance based on Geo-proximity to ensure the best application response time and latency. For remote users, the ZTNA solution must also be able to control internet traffic along with private application access.	
27	All security inspection including malware, sandboxing and Intrusion Prevention must happen in the ZTNA service before the traffic lands on the ZTNA connector to ensure no security risk reaches the customer datacenter.	

8. NextGen Firewall

Technical Specifications for NFGW			Compliance (Yes/No)
S.No	**Features**	**Details**	
1	**Hardware Architecture**	The solution should provide firewall, AVC, IPS, Anti-Virus, Anti-Spyware, Anti Malware, File Blocking and DNS Security functionality in a single appliance from day one.	
		Firewall must support zero-downtime inline policy changes without re-installation or full policy push. The hardware platform & Firewall with integrated SSL and IPsec.	
2		The appliance should support atleast 8 *10G RJ45, 8 * 10G and 4 * 25G ports from day one loaded with SR modules	
3		The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory and should support minimum of 32 GB of RAM	
4		Proposed firewall should not consume more than 1RU of rack space	
5	**Performance & Scalability**	Should support 10 Gbps of Thread prevention throughput (firewall, AVC, IPS Anti-Virus, Anti-Spyware, Anti Malware, File Blocking, DNS Security) real- world / production / Enterprise Testing performance / Or with app mix.	

Technical Specifications for NFGW			Compliance (Yes/No)
6		NGFW Firewall should support at least 20 M concurrent sessions on TCP or 2 M concurrent sessions on http	
7		NGFW Firewall should support at least 2,000,000 connections per second on TCP or 200,000 connections per second on http	
8		Firewall should support redundant power supply	
9		Firewall should support multiple fans	
10	**HA Capability**	High Availability Configurations shall support Active/ Passive or Active/Active-Clustering	
11	**NGFW Feature**		
12		Firewall should support static nat, dynamic nat, dynamic pat	
13		Firewall should support NAT functionality	
14		Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6	
15		Should support Multicast protocols like IGMP, PIM, etc	
16		Solution should support PBR based on parameter likes source port, destination address, destination port, protocol, applications, or a combination of these objects. Also PBR / equivalent policy should rely on flexible metrics, such as round trip time, jitter, mean opinion score, and packet loss of the interfaces to identify the best routing path for its traffic	
17		Should support capability to integrate with other security solutions to receive contextual information like security group tags/names	
18		Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.	
19		Should support more than 5000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness and should be able to create 40 or more application categories for operational efficiency	
20		Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.	
21		Should support more than 21,000 (excluding custom signatures) IPS signatures or more. Should support capability to configure correlation rule where	

Technical Specifications for NFGW			Compliance (Yes/No)
		multiple rules/event can be combined together for better efficacy	
22		Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.	
23		Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.	
24		Should be capable of detecting and blocking IPv6 attacks.	
25		Solution should be able to identify, decrypt, and evaluate both inbound & outbound Secure Sockets Layer & Secure Shell Protocol traffic on-box	
26		Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control	
27		The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor	
28		Solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist	
29		Must able to do real-time inspection of both the DNS request and DNS response can stop DNS hijacking attacks in real time. Solution should perform Inline inspection to protect from DNS threats such as DNS Tunneling, DNS Sinkholing, DNS Hijacking, DGA,Domain Shadowing, DNS Injection attacks, Compromised DNS registrar analysis, DNS Spoofing, DNS Cache Poisoning and DNS Spoofing etc. All the DNS features can be provided natively or using 3rd party solution for atleast 1 billion DNS request	
30		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.	
31		The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).	
32		Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location	
33		The 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.	

Technical Specifications for NFGW			Compliance (Yes/No)
34	**URL Filtering Features**	Should must support URL threat intelligence feeds to protect against threats	
35		Should support Reputation- and category-based URL filtering offering comprehensive alerting and control over suspect web traffic and enforces policies on more than million of URLs in more than 70 categories.	
36		The NGFW to support English, Hindi and regional languages for URL and IP database to fulfill web security needs as per Indian cybersecurity needs.	
37	**Other Capabilities**	Solution shall have capability to analyze and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN and FTP	
38		Must have required subscription AVC, IPS, Anti-Virus, Anti-Spyware, Anti Malware, File Blocking and DNS Security from day1.	
39		The management platform must be accessible via a web-based interface and ideally with no need for additional client software. The proposed firewall solution must support full-featured local policy creation, modification, and on any external centralized management system deployment directly from the firewall device without reliance	
40		The management platform must be a dedicated OEM appliance or VM running on server	
41	**Management , Reporting and Logging**	Solution must support policy audit trails and change history available locally on each firewall device.	
42		The management platform must provide a highly customizable dashboard.	
43		The management platform must provide centralized logging and reporting functionality	
44		The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows	
45		The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.	
46		Should support troubleshooting techniques like Packet tracer and capture	
47		Should support REST API for monitoring and config programmability	
48		The management platform must provide multiple report output types or formats, such as PDF/ HTML/CSV.	

Technical Specifications for NFGW			Compliance (Yes/No)
49		The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e- mail, SYSLOG).	
50		Firewall internal GUI management and management GUI platform should show unused policy and capabilities and turn them on with best practices, to understand gaps in configuration best practices, recommendations to close security gaps, detect hardware and software system issues.	
51		Solution should be able to provide insights of hosts/user on basis of indication of compromise, any license required for this to be included from day one	
52		The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports. The proposed Management platfrom solution must provide a mechanism to identify rules that are not being used or have not been hit by any traffic.	
53		The management platform support running on-demand and scheduled reports	
54		The management platform must risk reports like advanced malware, attacks and network	
55		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.	

9. Anti- DDoS

Component / Performance / Utility	Minimum Specification	Compliance (Yes/No)
Generic		
	Appliance based Solution	
	Inspection and prevention should be done in hardware.	
	Solution must support VLAN's	
	Solution must support at least 8 x 1GE Copper interfaces & 4 x 1GE SFP Interfaces from day one	
	Solution must at least support 8 Gbps of total traffic	
	Solution must have both copper & fiber interfaces.	
	Operating system should be hardenend	
	The device should support high availability	
	Device management interface must be firewalled internally.	

	System must be delivered as a single-box solution. This box must be rack-mountable in standard 19" rack.	
	Performance should not be limited by any licensing system.	
	In inline mode system must not modify MAC or IP addresses of passed frames	
	Latency should be lower than 70 microseconds	
	The solution shall support IPV6 protocol.	
	The DDoS detection capability of the solution must not be impacted by asymmetric traffic routing.	
	The system must detect the attack dynamically without the need of any static control/redirection (E.g. route maps or static routes)	
	The system must support an updated threat feed that describes new malicious traffic (botnets,phishing, etc...).	
	The system should be capable to mitigate and detect both inbound and outbound traffic.	
	The DDoS detection solution shall have the learning mode to easily identify anomalies in the network communication.	
Security		
	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	
	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	
	The system must limit number of simultaneous TCP connections on a per-client basis	
	DNS Flood Mitigation using following mechanisms DNS Query-Response matching, DNS Query/MX/ALL/ZT/fragment/ per-Source Floods, DNS Query Source validation, DNS Unexpected Query, Unsolicited DNS Response Flood,DNS Response cache under flood, DNS Query TTL checks, DNS-specific ACLs, DNS Header anomaly prevention,	
	Should support minimum 2 Million DNS Queries per second	
	Local Address Anti-spoofing	
	Adaptive Threshold Estimation and System Recommended Thresholds	
	The system must enforce minimal request speed for HTTP and SSL/TLS	
	The system must allow protection parameters to be changed while a protection is running. Such change must not cause traffic interruption	

	Solution should support security at layers 3,4 and 7	
	Solution should support for all 255 protocols at layer 3	
	Solution should support all 64k TCP and UDP ports	
	System must not use signatures, System must have methods of using behavioural and heuristic analysis	
	System must detect and block HTTP Opcode Flood	
	System must detect Excessive URL/source/second	
	System must be able to detect and block SYN Flood attacks	
	System must be able to detect and block Zombie Floods	
	System must be able to detect and block ICMP Floods	
	System must be able to detect and block Fragment Flood	
	System must be able to detect and block HTTP GET Flood	
	System must be able to detect and block Floods from Unwanted Geographical Areas	
	Slow HTTP requests (from tools like Slowloris, RUDY, Slowread)	
Deployment Options		
	Inline :- The DDoS appliance should support 'inline', meaning it is installed between the one or more protected systems and the rest of the network. In the simple network , data passes through the DDoS appliance as it travels to and from a protected system and the rest of an Ethernet local area network.	
Protection Mechanism		
	DDoS Appliance should be completely Behavourial Based	
	It should measures byte and packet counts, state transitions, fragments, checksum, flags, new connections, address pairs, and so on as Layer 3 to Layer 7 parameters to define Threshold	
	DDOS should not work on fix thresholds .It should continuously learns traffic patterns for a large group of layer 3, 4, and 7 parameters in both directions.	
	In case of threshold violation traffic should be drop	
	It should be possible to write manual ACL's to block certain IP	
	It should be possible to block Geographical Locations to prevent flooding attacks from a particular country	
	Should provide inspection NTP Query and Response traffic	
	Should support integration through RESTful API	
High Availability & ByPass Protection		
	It should support Hardware Bypass for Copper Interfaces available on Unit.	
Load Balancing to		

Increase Throughput		
	DDoS appliance should support Load Balancing Mechanism to increase througput	
	Load Balancing can be achieved by using a External Load Balancer which supports Load Balancing on bidirectional or unidirectional hashing algorithm	
	Load Balancing can also be achieved using a External Layer2 Switch using LACP	
Management		
	The system must support configuration via standard up to date web browsers. System user interface must be based on HTML without any third-party plugins such as ActiveX, Java or Flash	
	The system must support the generation of PDF and e-mail reports	
	System must support CLI access over RS-232 serial console port, SSH.	
	Dedicated management port	
	Management interfaces must be separated from traffic interfaces. System management must not be possible on traffic interfaces, management interfaces must not switch traffic	
	Management interface must be firewalled (e.g. only allow SSH from IP x and HTTPS from IP y).	
	System must have concept of users / groups / roles	
	Management certificate must be possible to change	
	Should support TLS 1.3 Management Logging	

10. L3 Network Switch

LAN Switch (48-Port)			**Compliance (Yes/No)**
S#	Parameter	Requirement / Specification	
1	General Requirement	a) Should support non-blocking Layer 2 switching and Layer 3 routing.	
		b) Should support the complete STACK of IPv4 and IPv6 services.	
		c) Switch Should have the capability to function in line rate for all ports	
2	Interface Requirement	a) Minimum 48 ports support 1/10/25 Gbps SFP/SFP+ ports for host connectivity and Minimum 6*40/100G QSFP 28 ports each supporting native 100Gig Ethernet. The switch should be populated with 24*10G fibre transceiver and 24*10G copper transceiver for downlink connectivity & 2*40/100G for uplink connectivity.	
		b) Switch should have fixed management interface console / port for local management & out of band management.	
3		a) Switch should have redundant power supply & fan.	

	Chassis & Power Supply	b) **Switch should be deployed in HA (Active Active) from day one .**	
		c) All components should be hot swappable.	
		d) The switch shall be rack mountable and be supplied with proper rack mount kit to mount.	
4	Performance	a) Modular OS with dedicated process for each routing protocol	
		b) Switch should re-converge all dynamic routing protocol at the time of routing update changes i.e. Graceful restart for fast re-convergence of routing protocols (OSPF, BGP)	
		c) Switch should support VRF instances with route leaking functionality	
		d) The switch should support LPM routes	
		e) The switch should have MAC Address table size of at least 64k	
		f) The switch should support multicast routes	
		g) Switch should support VLANs	
		h) Switch should support ECMP paths	
		i) Switch should support minimum 2 Tbps of switching capacity	
5	Network Virtualization Features	a) Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN	
		b) Switch should support VXLAN and EVPN IRB for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data center	
6	Layer2 Features	a) Spanning Tree Protocol (IEEE 802.1D, 802.1W, 802.1S)	
		b) Switch should support VLAN Trunking (802.1q)	
		c) **Switch should support MAC addresses table size of 64K or Higher**	
		d) Switch should support VLAN tagging (IEEE 802.1q)	
		e) Switch should support IEEE Link Aggregation and Ethernet Bonding functionality (IEEE 802.3ad) to group multiple ports for redundancy	
		f) Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures	
		g) Switch should support layer 2 extension over VXLAN across all Data Centre to enable VM mobility & availability	
		h) The Switch should support DC Bridging i.e. IEEE 802.1Qbb Priority Flow Control (PFC), IEEE 802.1Qaz Enhanced Transmission Selection (ETS), Explicit Congestion Notification (ECN).	
		i) Maximum number of port channel / link aggregation should be 48.	
		j) Maximum no of ports in the port channel / link aggregation should be 16/32.	

		k) The switch should support BGP EVPN Route Type 2/3 and Route Type 5 for the overlay control plane.	
7	Layer3 Features	a) Switch should support static and dynamic routing	
		b) Switch should support multi instance routing	
		c) Switch should support multicast traffic reachable	
		d) Switch should support multicast source discovery protocol (MSDP) **/ equivalent protocol.**	
		e) Switch should support IGMP v2 and v3	
8	Quality of Service	a) Switch system should support 802.1P classification and marking of packet using: CoS (Class of Service) and DSCP (Differentiated Services Code Point)	
		b) Switch should support for different type of QoS features for real time traffic differential treatment using: Weighted Random Early Detection / Deficit Weighted Round Robin or equivalent	
		c) Switch should support Rate Limiting - Policing and/or Shaping	
		d) Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy	
9	Security	a) Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy	
		b) Switch should support for external database for AAA using:	
		Ø TACACS+, RADIUS	
		c) 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	
		d) VXLAN and other tunnel encapsulation/decapsulation should be performed by switch.	
		e) Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined.	
		f) Switch should support DHCP Snooping.	
		g) Switch should support Dynamic ARP Inspection to ensure host integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol.	
		h) Switch should support IP Source Guard/lockdown to prevent a malicious host from spoofing or taking over another host's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN.	
		i) Switch should support unicast and/or multicast blocking on a switch port to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port.	
		j) Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch	

		performance from storm due to network attacks and vulnerabilities.	
		k) The Switch should support LLDP.	
		l) Switch should support Spanning tree BPDU protection	
10	Manageability	a) Switch should support for sending logs to multiple centralized syslog server for monitoring and audit trail	
		b) Switch should support for capturing packets for identifying application performance using local and remote port mirroring for packet captures	
		c) Switch should provide remote login for administration.	
		d) Switch must have Switched Port Analyzer (SPAN) with minimum 4 active session and ERSPAN on physical, Port channel, VLAN interfaces	
		e) Switch should support for management and monitoring status using different type of Industry standard NMS using:	
		a. SNMP v1 and v2, SNMP v3 with Encryption	
		f) Switch should provide different privilege for login in to the system for monitoring and management	
		g) Should have Open APIs/REST APIs to manage the switch either through remote- procedure calls (JavaScript Object Notation [JSON] or XML) over HTTPS or should support puppet for management and automation purpose	
		h) The Switch should support monitor events and take corrective action like a script when the monitored events occurs.	
		i) Should support hardware telemetry.	

11. Server Load Balancer

Sl. no	Technical Specifications	Compliance (Yes/No)
	Server Load Balancer	
1	The proposed OEM should be Parent Technology OEM(Should NOT be Whitelabled or Co-branding or 3rd Party Technology or Open Source or Reseller Agreement).	
2	The proposed appliance should be a dedicated appliance, it should not be part of any Firewall or UTM. There should not have any option to import 3rd party software on proposed appliance.	
3	**Traffic Ports:** 2 x 10G SFP+ and 8 x 1G RJ45 (Break-Out should not be used) **L4 Throughput:** 5Gbps and scalable upto 20Gbps **Layer 7 requests per second:** 250,000 **RSA CPS (2K Key):** 7,000 **ECC CPS (EC-P256):** 4,000 with TLS1.3 Support **Concurrent Connections:** 20 Million * Data should be publically available	

4	The solution must be able to decrypt SSL web traffic between clients and web servers	
5	**The proposed appliance should support the below metrics:** — Minimum Misses, — Hash, — Persistent Hash, — Tunable Hash, — Weighted Hash, — Least Connections, — Least Connections Per Service, — Round-Robin, — Response Time, — Bandwidth, etc	
6	**Following Load Balancing Topologies should be supported:** • Virtual Matrix Architecture • Client Network Address Translation (Proxy IP) • Mapping Ports • Direct Server Return • One Arm Topology Application • Direct Access Mode • Assigning Multiple IP Addresses • Immediate and Delayed Binding	
7	The proposed Hardware must have Bandwidth Mangement feature from Day 1	
8	Device must have Dynamic routing protocols like OSPF, RIP1, RIP2, BGP from Day 1	
9	The proposed device should support standard VRRP (RFC - 2338) for High Availability purpose (No Propertary Protocol). Other mode like Switch HA Mode, Extended HA Mode and Service HA Mode should also be supported.	
10	The solution should support IPv6 as well as IPv4 and have the ability to turn IPv4 traffic to IPv6 traffic on the backend	
11	Should have ability to upgrade/downgrade device software Images.	
12	The solution should support link aggregation for bonding links to prevent network interfaces from becoming a single point of failure	
13	Should support HTTP/2 and HTTP/3	
14	Supports SSL offload for the following protocols: — HTTPS — Generic SSL — SIP — SMTP (STARTTLS)* — IMAP (STARTTLS)* — POP3 (STARTTLS)* — LDAP (STARTTLS)* — FTPS*	
15	Appliance should support Local Application Switching, Server load Balancing, HTTP, TCP Multiplexing, Compression, Caching, TCP Optimization, Filter-based Load Balancing, Content-based Load Balancing, Persistency, HTTP Content Modifications	

16	The proposed device should support Content-Intelligent Cache Redirection: • URL-Based Cache Redirection, • HTTP Header-Based Cache Redirection, • Browser-Based Cache Redirection, • URL Hashing for Cache Redirection, • RTSP Streaming Cache Redirection	
17	Supports the following health check types: • Link Health Checks, • TCP Health Checks, • UDP Health Checks, • ICMP Health Checks, • HTTP/S Health Checks, • TCP and UDP-based DNS Health Checks, • TFTP Health Check, • SNMP Health Check, • FTP Server Health Checks, • POP3 Server Health Checks, • SMTP Server Health Checks, • IMAP Server Health Checks, • NNTP Server Health Checks, • RADIUS Server Health Checks, • SSL HELLO Health Checks, • WAP Gateway Health Checks, • LDAP/LDAPS Health Checks, • Windows Terminal Server Health Checks, • ARP Health Checks, • DHCP Health Checks, • RTSP Health Checks, • SIP Health Checks, • Virtual Wire Health Checks, • DSSP Health Checks, • Script-Based Health Checks, • Cluster-based Health Checks,	
18	The Solution should support native integration with Kubernetes Platforms and controller/connecter/plugin should operate within Kubernetes Cluster to automatically create service on Load Balancer. The controller/connecter/plugin should also support automatic creation, edition and deletion of service like VIP creation, Node/Real Sever Creation, Farms/Group Creation, SSL Binding etc.	
19	The controller/connecter/plugin should support at least three components with different task as follows: a. A Controller which should discovers the service objects in the Kubernetes clusters. b. An Aggregator which should aggregates inputs from all the controllers and communicates the necessary configuration changes to Configurator. c. A Configurator which should prepare a load balancing configuration file and pushes it to the device.	
20	The solution should support automatic renewal of SSL Certificate via integration with 3rd party Certification Authority such as Lets Encrypt	
21	Should support for IPv4 and IPv6 traffic along with DNS functionality from day-1	
22	Device should be accessed through the below: • Using the CLI, SSH, SCP • Using SNMP • REST API • Using the Web Based Management	

23	**Solution should provide from day1:** Application Dashboard Per Application Analytics SLA Breakdown (Network, per server) SSL Statistics (handshake and cypher breakdown, rejected handshake) SSL CPS System Dashboard Network Dashboard **Option for future use:** L4 Events Per transaction type events (delay, user agent, response, headers) SSL Events (type of handshake, cypher, TLS version)	
24	Bidder should propose Centralized Management & Reporting Solution from Day 1.	
25	The proposed solution should be EAL2 certified. OEM should be ISO 9001, ISO 14001, ISO 45001, ISO 28000 certified.	
26	Customer may ask for the demonstration of specific or all features if required.	

12. Virtual Web Application Firewall

Sl. No.	Technical Specifications	Compliance (Yes/No)
	Virtual Web Application Firewall	
1	The proposed OEM/Subsidiary should be Parent Technology OEM(Should NOT be Whitelabled or Co-branding or 3rd Party Technology or Open Source or Reseller Agreement).	
2	The proposed solution of WAF should be a dedicated solution, it should not be part of any Firewall or UTM. There should not have any option to import 3rd party software on proposed solution.	
3	The vWAF shall be entirely Software based and shall support virtualization platforms like VMware ESXi, Hyper-V, KVM, OpenStack etc	
4	The vWAF shall be able to run both IPv4 & IPv6 simultaneously (Dual Stack) from day one.	
5	**The proposed appliance should support the below metrics:** — Minimum Misses, — Hash, — Persistent Hash, — Tunable Hash, — Weighted Hash, — Least Connections, — Least Connections Per Service, — Round-Robin, — Response Time, — Bandwidth, etc	

Sl. No.	Technical Specifications	Compliance (Yes/No)
	Virtual Web Application Firewall	
6	**Following Load Balancing Topologies should be supported:** • Virtual Matrix Architecture • Client Network Address Translation (Proxy IP) • Mapping Ports • Direct Server Return • One Arm Topology Application • Direct Access Mode • Assigning Multiple IP Addresses • Immediate and Delayed Binding	
7	Shall have minimum 1Gbps throughput per instance.	
8	Shall support one-arm and two-arm mode deployment mode.	
9	Shall have minimum 8 Million concurrent connection per instance	
10	Shall have minimum 300K L4 connections / second.	
11	Shall have minimum 400K L7 Requests / second.	
12	Shall support IPv4 to IPv6 address translation and vice-versa.	
13	The solution must be able to protect both HTTP Web applications, SSL (HTTPS) web applications & Should support HTTP/2	
14	Should supports the following modes of operation for cookie-based session persistence: Insert, Passive, Rewrite mode	
15	Solution should support Role Base Access Control (RBAC) with Following User Accounts and Access Levels: User Operator Administrator Certificate Administrator	
16	The proposed Solution should be PCI Compliant WAF. It must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification.	
17	WAF should have the flexibility to be deployed in the following modes: Reverse proxy Out of Path (OOP)	
18	Solution should dynamically understand the Changes on the Web/Application Server	
19	The Proposed WAF Solution should support both a Positive Security Model Approach (A positive security model states what input and behavior is allowed and everything else that deviates from the positive security model is alerted and/or blocked) and a Negative Security Model (A negative security model explicitly defines known attack signatures) . The solution must support automatic updates to the signature database to ensure complete protection against the latest web application threats	
20	The WAF should support the following escalation modes: a) Active, b) Bypass, c) Passive	

Sl. No.	Technical Specifications	Compliance (Yes/No)
	Virtual Web Application Firewall	
21	The solution must have a database of signatures that are designed to detect known problems and attacks on web applications	
22	**Hiding Sensitive Content Parameters:** It should be able to Mask values of sensitive parameters (for example, passwords, credit card and social security details)	
23	**Auto Policy Optimization**	
	• Known Types of Attack Protection - Rapid Mode	
	• Zero Day Attack Blocking - Extended Mode	
	• Working in Learn Mode	
	• Auto Discovery	
24	**The proposed WAF should support the Activity Tracking, which should include the following:**	
	Dynamic IP	
	Anonymity	
	Scraping	
	Mimicking user behavior	
	Clickjacking	
25	**Device Fingerprint-based tracking**	
	Should support Fingerprint technology which involves various tools and methodologies to gather IP agnostic information about the source. Should also involves running JavaScript on the client side. Once a JavaScript is processed, an AJAX request is generated from the client side to WAF with the fingerprint information.	
26	Should support API Security, API Quota Management and GraphQL.	
27	Should support Auto Policy Generation with: • Full Auto, • Auto Enabled, • Auto Refinements,	
28	Should support Auto Discovery which should displays an application view that contains the server, tunnels, hosts, folders (URIs), files (pages), and parameters (Path and Query)	
29	Solution should provide: Application Dashboard Per Application Analytics SLA Breakdown (Network, per server) SSL Statistics (handshake and cypher breakdown, rejected handshake) SSL CPS System Dashboard Network Dashboard L4 Events Per transaction type events (delay, user agent, response, headers) SSL Events (type of handshake, cypher, TLS version)	
30	Shall be configured in High Availability Mode. In case of failure of one of the instance; the other available instance/s shall serve all the requests without any disruption or degradation in overall performance	
31	Shall support TCP and UDP applications.	

Sl. No.	Technical Specifications	Compliance (Yes/No)
	Virtual Web Application Firewall	
32	Should support ECC in addition to other commonly used Ciphers from day1	
33	Should support end – end SSL if required from day1	
34	System supports performing load balancing across multiple sites, complete disaster recovery among sites and optimal service delivery , Single application failure etc	
35	System supports global redirection based on DNS from day1	
36	Supports the following health check types: • Link Health Checks, • TCP Health Checks, • UDP Health Checks, • ICMP Health Checks, • HTTP/S Health Checks, • TCP and UDP-based DNS Health Checks, • TFTP Health Check, • SNMP Health Check, • FTP Server Health Checks, • POP3 Server Health Checks, • SMTP Server Health Checks, • IMAP Server Health Checks, • NNTP Server Health Checks, • RADIUS Server Health Checks, • SSL HELLO Health Checks, • WAP Gateway Health Checks, • LDAP/LDAPS Health Checks, • Windows Terminal Server Health Checks, • ARP Health Checks, • DHCP Health Checks, • RTSP Health Checks, • SIP Health Checks, • Virtual Wire Health Checks, • DSSP Health Checks, • Script-Based Health Checks, • Cluster-based Health Checks,	
37	Shall be able to support different cookie persistence methods	
38	The proposed device should support standard VRRP (RFC - 2338) for High Availability purpose (No Preoperatory Protocol). Other mode like Switch HA Mode, Extended HA Mode and Service HA Mode should also be supported.	
39	Shall support NTP for date & time synchronization from NTP Server.	
40	Shall have static routing & dynamic routing (RIP, OSPF, BGP) capabilities.	
41	The Solution should support native integration with Kubernetes Platforms and controller/connecter/plugin should operate within Kubernetes Cluster to automatically create service on Load Balancer. The controller/connecter/plugin should also support automatic creation, edition and deletion of service like VIP creation, Node/Real Sever Creation, Farms/Group Creation, SSL Binding etc.	
42	The controller/connecter/plugin should support at least three components with different task as follows: a. A Controller which should discovers the service objects in the Kubernetes clusters. b. An Aggregator which should aggregates inputs from all the controllers and communicates the necessary configuration changes to Configurator. c. A Configurator which should prepare a load balancing configuration file and pushes it to the device.	
43	The solution should support automatic renewal of SSL Certificate via integration with 3rd party Certification Authority such as Lets Encrypt	
44	Shall be manageable (both GUI and CLI) using SSH, Web based management (HTTPS) etc.	
45	Shall have feature to provide role based user's access for management.	

Sl. No.	Technical Specifications	Compliance (Yes/No)
	Virtual Web Application Firewall	
46	Shall support authentication and authorization through Radius / TACACS+.	
47	Bidder should propose Centralized Management & Reporting Solution from Day 1.	
48	The proposed solution should be EAL2 certified. OEM should be ISO 9001, ISO 14001, ISO 45001, ISO 28000 certified.	

13. Server Security Solution

S.no	Technical Specifications	Compliance (Yes/No)
	General requirements	
1	The solution should offer Antivirus, Application Control, Change Control, HIPS, and Virtualised Security functionality for servers to ensure optimal security and compliance for critical servers on single agent.	
2	The solution should be managed from a single centralized console.	
3	The solution should have a small overhead footprint such that it minimizes impact on system resource	
4	The proposed solution shall support the Windows & Linux Server platforms	
5	The proposed solution should be able to manage both Endpoint & Server Secuirty solution from the same single management console.	
	Anti-Virus & Anti Spyware For Servers	
1	Solution must provide automated and centralized download and deployment of latest virus signature updates from the Internet to desktops and servers across the organization, across different Windows platforms. Updates should be incremental with update sizes of ~100KB on average	
2	Solution must provide flexibility to install different components (Like – Management Agent, AV client, Anti-Spyware, HIPS,) separately for better use of network bandwidth	
3	Should have the ability to detect and remove unwanted programs, toolbars, adware, spyware, dialers etc & Post detection the actions that the antiviral performs must be the following: Alert / Notify , Clean, Delete / Remove, Move / Quarantine, Prompt for Action	
4	Should support file scan caching to avoid repetitive scanning of files which are unchanged since the previous scan	
5	Proposed solution must automatically scan Floppy disks, Compact disks, USB devices and Network shares in real-time when accessed.	
6	Proposed solution should provide multiple policies to lockdown the server like – change in registry, Internet Explorer file settings, Exe file execution etc to block unknown zero day attacks and reduce dependency on frequent signatures	
7	Should allow the On Demand Scanner to recognize the last scanned file and resume scanning from that file if an “On demand Scan” is interrupted	

S.no	Technical Specifications	Compliance (Yes/No)
8	Should have the ability to control the amount of CPU resources dedicated to a scan process	
9	The proposed solution should be capable of detecting and preventing buffer overflow vulnerability, irrespective of the exploit that is using the buffer overflow vulnerability. The solution should support buffer overflow detection and prevention on the following minimum applications: Windows OS Services, Media Player, Internet Explorer, SQL Server, Word, Excel, Power Point, Auto Update, Explorer, Instant Messenger, Outlook, Outlook Express etc	
10	Proposed solution should be capable of blocking TCP/IP ports on the System and also creating exceptions for specified applications to use these blocked ports.	
11	Proposed solution should be capable of blocking read, write, execute, delete & change permissions on specified file(s)/folder(s)/Network Share(s).	
12	Discover and Report the IP Address of the end-point system (infection source) that sent malicious code to the server and optionally, block further communications from the infection source end-point system for a configurable time period or indefinitely	
13	The proposed solution should provide Self protection from modifying or disabling AntiVirus Client	
14	Proposed solution should allow to configure different policies for different set of Processes	
15	The Antivirus should allow for automated rollback of virus definition, if required	
16	Should be able to lock down all anti-virus configurations at the servers.	
17	Proposed solution should be capable of detecting and blocking communication from hosts that are spreading viruses/worms.	
18	Should support unique real time update based on over the web cloud technology to provide real time signatures for dynamic and latest threats to reduce the dependency on Daily Signature updates	
19	The proposed solution should have the option to block the intruder hosts for a specific number of seconds.	
20	Sould have enhanced tamper protection that guards against unauthorized access and attacks, protecting users from viruses that attempt to disable security measures	
	Antimalware	
1	The proposed solution updates should be incremental with the option of full updates when the client is not updated for a long period	
2	The proposed solution should protect the registry of the proposed solution	
3	Solution should offer different client/server communication settings be imposed based on different groups	
4	The proposed solution should scan system memory for installed rootkits, hidden processes, and other behavior that suggests malicious code is attempting to hide itself.	
5	It should support Signature as well as behavioral based detection along with the automatic rollback features when the system is compramised with ransomeware attack.	

S.no	Technical Specifications	Compliance (Yes/No)
6	Proposed solution should support rollback feature in case machines gets compramised	
7	The system should periodically scan log files for anomalous activity andnotify the system administrator if they have detected suspicious pattern on thehosts.	
8	The proposed solution's agent should be light weight and should be able to work on the system with the 3Gb RAM & 2GHz processer or higher.	
	Application Control For Servers	
1	The solution should provide the dynamic management of execution capability of applications on a server system, prevent unauthorized registry manipulation and in memory protection of application	
2	It should prevent execution of all unauthorized software, scripts, and dynamic-link libraries (DLLs) and further defends against memory exploits	
3	The solution should provide for a real time capability to prevent execution of any authorized application to execute on the server system	
4	The solution should allow an administrator to authorize a well defined update mechanism to alter the state of gold image as being enforced currently to a new gold image.	
5	The solution should allow an administrator to remote view the constituents of a system image and hence compare the image with a well defined gold image.	
6	The solution should allow for well defined update mechanism to allow changes to the state of server system and then enforce the new state of the system	
7	The solution should not require updates to be rolled to client system in order to approve new applications to be executed.	
8	The solution should allow/ban individual application based on different characteristics such as name, checksum etc.	
9	It should restrict administrators with physical or remote access to the machine to override protection	
10	The solution should augment blacklisting, real-time reputation awareness, and behavioral approaches, helping IT to consistently enable the known good, block the known bad, and properly handle the new and unknown.	
11	The solution should prevent the tampering of application on the disk and in the memory.	
12	The solution should have a small overhead footprint which includes:	
	• Easy setup and low initial and ongoing operational overhead	
	• No file system scanning that could impact system performance	
	• Designed to work in disconnected and in “offline“ mode if necessary	
13	The solution should be able to create inventory of a target system and hence report on installed software and applications on client machines.	
14	The solution should not be dependent on any external verification of allowed/banned application. It should be able to take its input on the basis of local state of server system as verified by the system administrator	

S.no	Technical Specifications	Compliance (Yes/No)
15	The solution apart from allowing only authorised applications to run, should block any changes from being done to authorized applications, like DLL's, System files, registry etc., thus providing application treat protection	
	File Intigrity Monitoring For Servers	
1	The solution should support Real-time Change Tracking Audit log. It should Include File, User, Program name and contents that have changed. FIM should support detect and block mode.	
2	The solution should support Change Prevention as part of the core solution	
3	The solution in the event of unauthorized file change, should reports WHAT changed, WHO made the change, HOW they made it and precisely WHEN they did the changes	
4	The solution should offer intelligent filters which are pre-configured to track the relevant objects on the system, for each standard Operating System covering systems files including Windows, Solaris, and Linux. It should also include application filters for Apache, Tomcat, Websphere and JBOSS, IIS, Weblogic, Websphere , etc., and should be customizable.	
5	The solution should monitor application and operating system files in real time	
6	The solution should provide email and SNMP alerts	
7	The solution should integrate with change management, data center automation, and configuration management database (CMDB) solutions from HP, BMC, IBM, and others	
8	The solution should be capable of tracking changes to databases in two manners (1) changes to the database structures themselves (tables, indexes etc.) (2) changes to the data itself, in real time	
	HIPS for Servers	
1	It should support Signature as well as behavioral based detection	
2	It should support policies creation based on – User defined, Adaptive mode and Learn mode	
3	It should support desktop firewall capabilities to directly block unwanted traffic	
4	HIPS solution should provide facility to create different policy for different network connectivity like – LAN, DHCP.	
5	It should support firewall policy to enable cloud based network reputation lookup. For e.g. if a client is communicating with an IP address with a bad reputation or bad URL, the firewall should stop the communication without having to create a rule.	
6	HIPS Solution should provide blocking of unwanted applications trying to run	
7	HIPS solution should provide facility to create User defined signatures	
8	HIPS solution should provide protection from known attacks like – SQL injection, Cross Site scripting, Buffer Overflow without having signature updates	
9	HIPS solution should provide vulnerability shielding to the application not having patches installed	

S.no	Technical Specifications	Compliance (Yes/No)
	Virtualization security	
1	The Proposed Solution should offloads scanning, configuration, and .DAT update operations from individual guest images to an offload scan server within the premises	
2	The solution should build and maintain a global cache of scanned files to ensure that once a file is scanned and confirmed to be clean, subsequent VMs accessing the file won't have to wait for a scan.	
3	Should allows separate policies for on-access and on-demand scanning to enable fine-tuned security execution	
4	Should provide Connector for VMware vSphere provides a complete view into virtual data centers and populates key properties such as servers, hypervisors, and VMs through the same management console.	
5	The Solution should provide administrators gain visibility into the security status of all VMs and can monitor hypervisor-to-VM relationships in near real time.	
6	The Proposed Solution should work agentless on VMware workloads	
7	Solution should extend visibility and control across Amazon Web Services (AWS) and Microsoft Azure public clouds and physical servers.	
	Server Security	
1	Server security solution should be capable of integration with cloud IaaS platforms such as; AWS, GCP, Azure. Private cloud platform such as, VmWare virtual platform, Hyper-V etc.	
2	Proposed solution should support shahow IS feature. E.g. Post integration with server management platforms it should automatically discover all the tenents configured on concern management platform.	
3	Solution should display potential threats and unsafe settings so that appropriate actions can be taken.	
4	It should be capable of defining compliance policies for security assessment and view all high and low compliance events in the dedicated dashboard.	
5	It should display security group information of virtual instances across cloud accounts.	
6	It should show how many instances are associated with any firewall (security group) or network security.	
7	It should also manage these firewalls (security groups) by adding, editing, or deleting rules, and detaching firewall (security group) from an instance.	
8	It should support multiplatform environment	
	Management	
1	Proposed solution should provide single agent and console to manage all components – Threat Prevention for Windows and Linux platforms Desktop Firewall Application & Chnage Control Virtualized environment which includes both on premises and on public cloud	
2	The centralized management console must be web-based	

S.no	Technical Specifications	Compliance (Yes/No)
3	The centralized management console should be capable of deploying remotely the managed products (such as Endpoint Security).	
4	The tool should support hierarchical grouping of machines and policy deployment. The grouping could be based on IP Address of a subnet of machines or a particular site	
5	The Centralized management tool should be capable of deploying Pattern Files, Scan Engines, emergency releases of pattern files, patches, hot fixes and new product versions for all managed products	
6	The centralized management tool should be able to deploy signature files for different products at scheduled times.	
7	The management platform allows for separate deployment of components to systems. This allows for flexibility of deployment.	
8	Centralized management console should provide dashboard with multiple information & these information should also be fetched from database based on different queries	
9	Console should support tagging of information in the database to provide flexible reporting	
10	The centralized management should provide Asset Management functionality and provide complete details of managed endpoints such as, Hostname, IP address, OS type, Freee memory etc.	
11	Administrator should be able to configure the update process as automatic or manual, controlled deployment	
12	Update process should conserve WAN Bandwidth by having a distributed framework for signatures and policy updates	
13	The centralized management console should provide management reports for different managed components like – Top N reports, Trend reports, Outbreak reports, Compliance reports,	
14	The centralized management console should support a way to build custom queries on the database to create custom reports	
15	Central management console should provide automatic generation and delivery of reports to the respective administrators	
16	Central management console should provide actionable reports	
17	The proposed solution should integrate with Active Directory and other LDAP based directory services.	
18	Central management console should support granular role based access control	
20	The Centralized Management Console should deliver security threat information including current threats and the DAT and engine files necessary to protect against them	
21	Reports should be in CSV, HTML and Microsoft Excel Format	
22	Explain if your central management is based on an Open framework that unifies security management for systems, applications, networks, data, and compliance solutions	
23	Extensible platform integrates with and leverages your existing IT infrastructure	
24	Must provide native 64 bit performance for report generation from the database	
25	Must provide real time software deployment and updates to large organization networks made up of multiple subnets and vlans	

S.no	Technical Specifications	Compliance (Yes/No)
26	Must natively provide management snapshots for all managed settings, preferences and files and quicker disaster recovery and management restoration	
27	Solution must offer locally and globally sourced threat intelligence, which enriches protection through file and URL reputation	
28	Solution must have AI Capability and must not completely depend on internet based threat feeds and have its own heruristic and machine learning capability .	
29	Must report on the management server if the managed AV machine is under a VDI mode	
30	Must provide side by side policy settings and management comparison	
31	Must include the ability to Identify unknown assets on your network and bring them under control with rogue system detection	
32	Proposed solution should have separate console to manage workload on different servers. It should not be limited to server placement (e.g. On-prem or cloud only)	

14. Integrated Smart Rack

S.No	Description of Requirements	Compliance (Yes/No)
1	**Scope of Work**	
1.1	This specification covers Intelligent Integrated Smart Rack Infrastructure, standalone system design, testing at manufacturer's works, supply, delivery at site, unloading, handling, proper storage at site, erection, testing and commissioning at site of complete infrastructure for the proposed Smart Rack solution	
1.2	The critical components of the smart rack solution can be maintained easily in the events of failure. All the components of the infrastructure should be such that it can be easily dismantled and relocated to different location.	
2	**Requirements**	
2.1	The Integrated Smart Rack Solution with inbuilt hot and cold aisle containment of 1 rack should cater IT load up to 7 kW.	
2.2	Integrated Smart Rack Solution essentially should include environmental controls, Rack mounted air conditioning, smoke detection & fire suppression, Water leak detection and humidity sensors and security devices. Environmental monitoring shall be done from IP based software.	
2.3	The Integrated smart rack solution must be CE Certified.	
2.4	The critical components like Cooling unit, Rack, UPS , rack PDU & Monitoring unit should be from same & single OEM for better integration & service support.	

S.No	Description of Requirements	Compliance (Yes/No)
3	**The Intelligent integrated Infrastructure shall have following components: -**	
3.1	**Rack based closed loop Air-Conditioning**	
3.1.1	The smart rack should be equipped with rack mounted cooling unit to provide closed loop cooling system which should be able to cool the equipment's uniformly right from 1st U to 42nd U of Rack	
3.1.2	Rack Mounted Air-Cooling unit should be of 7kW/2TR capacity, (01 no. of 7kW rack-based cooling unit). The air from will be from bottom to top. The unit will have following configuration: Rack based Air Cooling with indoor - out door design, SHR >0.9, 100% Duty cycle, scroll compressor, 9U rack mountable, electronically commutated (EC) fan, High Pressure & Low-Pressure protection, Washable filter with 80% efficiency down to 20-micron, Hydrophilic evaporator coil, ON/OFF switch at indoor unit for emergency purpose, R407C/R410A Refrigerant.	
3.1.3	The unit should support indoor to outdoor copper piping distance up to 30 mtrs including vertical piping distance up to 30 mtrs.	
3.2	**Power Distribution**	
3.2.1	0U, Vertical Rack PDU, 32A, 230V, 7.3kW with 20 no. IEC C13 & 04 no. IEC C19, 3m power cord with 1P+E (IP44), Black Powder Coat.	
3.3	Electrical Distribution System	
3.3.1	Rack mountable Power Output Device with essential breakers to be provisioned. All input supply cables from POD unit to equipment's are connected with industrial socket (male - female) with suitable rating	
3.4	**Environmental Controls**	
3.4.1	Intelligent Smart Rack (01 Nos.) should include basic environmental controls: Smoke Detector Water Leak Detection system Temperature/ Humidity Sensor Door Sensor Alarm beacon	
3.5	**Rack & accessories**	
3.5.1	Rack is 42 U 19" mounting type with 2100 (Height) x 800 (Width) x 1200 (Depth) with safe load carrying capacity of 1400 Kg on enclosure frame and 1000 Kg on 19" mounting angles	

S.No	Description of Requirements	Compliance (Yes/No)
3.5.2	Front Glass door for complete 42U height visibility and rear plane/split door with stiffener for strength	
3.5.3	Cable entry provision from top & bottom both side of rack	
3.5.4	Cut outs with rubber/brush grommet on top and bottom cover of rack for cable entry	
3.5.5	Vertical Cable manager on both LHS & RHS on rear side	
3.5.6	Thermally insulated cold aisle chamber	
3.5.7	Blanking panels to prevent air mixing	
3.5.8	Status based LED light to be provided on each rack	
3.5.9	70% Blanking panels to be supplied with the Smart rack	
3.6	**U Space**	
3.6.1	Intelligent Smart rack should have Min 24U(total) space available for IT equipment's and network equipment	
3.7	**Monitoring**	
3.7.1	Detailed Monitoring & Diagnostics 1U rack mountable monitoring unit with redundant power supplies & capable of single window monitoring of all the environmental parameters along with Air conditioning through a single window dashboard over ethernet & Capable for sending Email Alerts	
3.7.2	Monitoring unit should integrate & monitor environmental parameters like temperature, humidity, door access, smoke etc. with cooling unit in a single dashboard along with other environmental parameters like temperature, humidity, smoke etc.	
3.7.3	The monitoring unit should support basic protocols like Telnet, SSH, FTP, SFTP, HTTP, HTTPS, NTP, DHCP, DNS Server, smtp, TCP/IP4. It should support network interface of 10/100M self-adaptable Ethernet ports.	
3.7.4	Air conditioning should be integrated with the monitoring unit to monitor all critical parameters (Cooling unit: Unit status, supply & return air temperature, humidity in a single dashboard.	
3.8	**Safety & Security**	
3.8.1	Rodent Repellent system Rack to be covered with rodent repellent system	
3.8.2	Access Control System The system deployed will be rack based access control system based on Biometric Technology. The front & rear rack doors will be provided with electromagnetic locks and will operate on fail-safe principle through Biometric access control system.	
3.8.3	01 no. IP Based Camera for live monitoring.	

S.No	Description of Requirements	Compliance (Yes/No)
3.8.4	Fire Detection & NOVEC 1230/FK-5-1-12 Fire Suppression system Rack to be covered with Fire alarm & gas-based suppression system. The system should have fire suppression unit mounted internally / externally on the rack. The fire suppression agent should be NOVEC 1230 / FK 5-1-12 clean agent gas based as per NFPA 2001 guidelines	
3.9	**UPS System (02 no. x 10 kVA)**	
3.9.1	UPS should be of True On-line, Double conversion and IGBT minimum 10 kVA capacity in N +N topology, 1 Phase input & 1 phase output, rack mountable (≤ 2U) with unity power factor and efficiency up to 95 % & eco mode efficiency up to 99%.	
3.9.2	Input Parameters: Input Voltage Range: 176-288VAC at full load; 100-176VAC at linear derating; 100VAC at half load Input Power factor: 0.99, at full load; ≥0.98, at half load Input frequency range (Hz): 40-70 Hz Current THD at full linear load (THDi%): <5	
3.9.3	Output parameters: Nominal output voltage (V): 220/230/240 (1-phase) Rated power factor(kW/kVA): Unity. Voltage harmonic distortion (%): <2% for Linear loads & <5% for Non-linear loads Overload capacity: At 25°C: 105% ~ 125%, 5min; 125% ~ 150%, 1min; 150%, 200ms Crest factor: 3:1 Frequency synchronization range: Rated frequency±3Hz. Configurable range: ±0.5Hz ~ ±5Hz Dynamic response recovery time: 60ms	
3.9.4	Transfer time Mains←→Battery: 0ms Inverter←→Bypass: Synchronous transfer: ≤0ms Asynchronous transfer (default): ≤20ms	
3.9.5	UPS should be RoHS certified, Energy star & BIS certified with IP20 Protection level. Noise level should be < 55dB	
3.9.6	Operating temperature for the UPS: 0°C ~ 50°C; Relative humidity: 5%RH ~ 95%RH, non-condensing	

S.No	Description of Requirements	Compliance (Yes/No)
3.9.7	Conformity & Standard Compliance: General and safety requirements - IEC/EN 62040-1, EMC - IEC/EN 62040-2; Surge protection for UPS: IEC/EN-61000-4-5, ANSI C62.41, 6kV/2Ohms	
3.9.8	UPS system should support battery backup 15 min @ rated load per UPS. Batteries to be placed in separate battery racks.	
4	**OEM Credential**	
4.1	The critical components of Integrated Smart Rack solution like Cooling unit, UPS , Rack, Rack PDU, Monitoring unit should be from same & single OEM for better integration & service support.	
4.2	The Integrated smart rack solution must be CE Certified.	
4.3	Smart Rack OEM or Manufacturer should be ISO 9001: 2000, ISO 14001, ISO/IEC 27001:2013 and ISO 45001 certified.	
4.4	Smart rack OEM should have its own manufacturing facility in India for offered or similar capacity range of Rack & Precision air conditioning units for high availability of the proposed solution. Supporting document/undertaking regarding the same to be submitted along with the bid.	
4.5	The Smart rack OEM should have at least 10 years of experience in executing similar works (Similar works means – "SITC of Integrated Smart Rack Infrastructure of minimum 01 rack configuration") in Central/State/PSU Organizations. Completion Certificate, as a proof of experience, signed by the concerned authorities to be submitted along with the bid.	
4.6	OEM or Manufacturer of the offered goods/ equipment's should be a company registered under the companies act since last 10 years. Valid company registration certificate should be submitted.	

Note:

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

The Bidder need to consolidate Compliances of respective OEMs and submit the same (counter signed) along with the forwarding format as above.

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: Certificate of Dealership/Authorization Letter/Warranty

Certificate of Dealership/Authorization Letter/Warranty

(*To be provided by the OEMs of devices as mentioned in this tender document on their Letterhead) to be enclosed with Technical bid)*

Dated: _____

The Special Secretary (IT) and the Treasurer, CRID
Citizen Resources Information Department (CRID)
SCO 109-110 Sector 17 B, Chandigarh. 160017

Subject: E-Tender/CRID/Revenue ICT Infra/2025-26

Sir,
This is to certify that I/We am/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 endorse the warranty, contracting and licensing terms provided by <Bidder> as per the requirement of this tender.
4. 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 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.
5. We also certify that the above-mentioned product being supplied by the <Bidder> meets the minimum specifications given in the Tender document.

The authorization will remain valid till <*Date of renewal of dealership*>

Sr. No.	Product Name
1	<*Fill Model number and Product name*>
2	…

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

Undertaking for honoring warranty

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

Date: _____

The Special Secretary (IT) and the Treasurer, CRID
Citizen Resources Information Department (CRID)
SCO 109-110 Sector 17 B, Chandigarh. 160017

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

This bears reference to our quotation Ref. _____ Dated _____

We warrant that,

1) All Products supplied by us shall be brand new (purchased within 2 months of the data of supply), 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) None of the components and sub-components are declared "End-of-sale" by the respective OEM in next Two (2) years as on date of submission of Bid.
4) If the infrastructure supplied by us is not-supported by the OEM during the period of contract for any reason, we will replace the product with a suitable higher alternate for which support is provided by the OEM at no additional cost to the department and without impacting the performance or timelines of this engagement
5) We would provide on-site maintenance of the installed system for a period of 5 years from the date of commissioning of the system within the price quoted by us in the Commercial Bid.
6) We, [Insert Bidder's Name], regarding our bid submitted for e-Tender<xx> declare that 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

(Checklist to be enclosed with Technical bid)

Date: _____

The Special Secretary (IT) and the Treasurer, CRID
Citizen Resources Information Department (CRID)
SCO 109-110 Sector 17 B, Chandigarh. 160017

Subject: e-Tender/CRID/Revenue ICT Infra/2025-26

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	Pg.no.
1.	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 Citizen Resources Information Department. Scanned copy of Online Payment Receipt should be uploaded with technical e-bid.		
2.	EMD should be submitted.	The EMD will be ₹2,00,000/- (Rupees two Lakh only), which shall be made by eligible bidders through Online Mode at NIC Portal in favour of Citizen Resources Information Department. Scanned copy of Online Payment Receipt should be uploaded with technical e-bid.		
3.	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.	A Certificate from CS certifying that the Bidder is authorized by Board of Directors / Managing Director / CEO.		
4.	Manufacturer Authorization Format (MAF)	The bidder must submit a valid Manufacturer Authorization Format (MAF) issued on their letter head by the Original Equipment Manufacturer (OEM) in favour of the bidder as per the Annexure-5. The OEM must be registered in India under the Indian Companies Act, 1956. (copy of Registration certificate must be submitted) (For Network, Compute, Storage, Security and cable Components)		

S#	Clause	Documents Required	Document Attached Yes/No	Pg.no.
5.	The bidder must be registered Central Public Sector Undertaking in India under the Indian Companies Act, 1956 and should be in existence in India for at least the last 3 financial years, as on date of submission of bid.	The bidder shall provide the Certificate of Incorporation for Registered Companies.		
6.	OEM Qualification Criteria The OEM should be in manufacturing of offered (or similar) products for at-least 3 out of last 5 financial years in addition to current year as on bid submission date for Active and cabling component.	Copies of Supply orders/ Invoices/ Completion Certificate from the concerned supplier/ client, conforming the total quantity/ value and destination where supplied, be considered proving at least 3 years out of 5 years in manufacturing in one each from any of the following Financial Years 2019-20, 2021-22, 2022-23, 2023-24, 2024-25 current FY/ till bid submission date. (For Network, Compute, Storage and Security Components)		
7.	The OEM should have supplied the similar equipment of 200% (Two times) of estimated tender quantity of respective items in last 3 financial years. The orders should be executed on behalf of States or Central Govt./ PSUs/ Central or State Universities/ Scheduled banks/ Nifty 100 listed companies (as on date of submission) for Active components.	Certified letter from the concerned Client(s) confirming the total amount, date of engagement and successful completion of order within the time stipulated in work order. i.e. 2022-23, 2023-24, 2024-25 current FY/ till bid submission date. (For Network, Compute, Storage and Security Components)		
8.	Bidder Qualification Criteria, they should be in the business of implementation and commissioning of data center for any 3 financial years out of last 5 financial years on behalf of States or Central Govt. / PSUs / Central or State Universities / Scheduled Banks.	Copies of work orders or contract proving at least 3 years, one each from any of the following Financial Years 2020-21, 2021-22, 2022-23, 2023-24, 2024-25, current FY/ till bid submission date.		
9.	Registered Office.	There should be at least one registered office of the bidder in Tri- city/ Haryana/ NCR.		
10.	The bidder should have executed orders of implementation and commissioning of data center in the last 3 financial years. The orders should be executed on behalf of States or Central Govt. / PSUs /	Three completed orders each costing not less than the amount equal to 50% of the estimated cost. Or Two completed orders each costing not less than the amount equal to 80% of the estimated cost. Or One completed order costing not less than the amount equal to 100% of the estimated cost.		

S#	Clause	Documents Required	Document Attached Yes/No	Pg.no.
	Central or State Universities / Scheduled Banks.	For, 2022-23, 2023-24, 2024-25, current FY/ till bid submission date. (For Network, Compute, Storage and Security Components) (Work orders & completion reports for Data Center or other projects with equivalent quantity of active component where it includes installation and commission of active components along with UTP and fiber optic cable laying).		
11.	The bidder should have positive net worth (measured as paid up capital plus free reserves) in any of two years out of 3 financial year i.e. 2021-22, 2022-23 & 2023-24	iii) CA Certificate / Statutory Auditor Certificate of the Bidder confirming the net-worth and profit after Tax for each of the last 3 financial years. i) 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.		
12.	Should not have been black listed as on date of submission of Bid.	An Undertaking as per the Annexure-2 to be submitted by bidder on non-judicial stamp paper.		
13.	Service Center	There should be at least one OEM owned or authorized service center in Tri- city/ Haryana/ NCR.(For Switches, Servers, Computers, Display, & UPS)		
14.	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. (For Network, Compute, Storage and Security Components)		
15.	Product compliance	As mentioned in the Technical Specification. The Annexure- 4 shall be cross-referenced with the OEM's official product datasheet and must include verifiable product links from the OEM's official website or documentation portal.		
16.	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 CRID. Bid of such OEM and their product/bidder will not be considered. (Annexure 13 & 14)		
17.	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)		
18.	Technical Bid	Format 1		
19.	Commercial Bid	Format 2		
20.	Acknowledgement of bid document	Annexure 1		
21.	Self-Declaration on not being blacklisted	Annexure 2		
22.	Statutory undertaking	Annexure 3		

S#	Clause	Documents Required	Document Attached Yes/No	Pg.no.
23.	Technical Compliance	Annexure 4		
24.	Certificate of Dealership/ Authorization	Annexure 5		
25.	Undertaking for honoring warranty	Annexure 6		
26.	Checklist	Annexure 7		
27.	After Sales Service Certificate	Annexure 8		
28.	Undertaking of Rates	Annexure 9		
29.	Format for Relaxations to Micro Small Enterprise registered in Haryana	Annexure 10		
30.	Format for Relaxations to Medium Enterprise registered in Haryana	Annexure 11		
31.	Authenticity of submitted documents/information	Annexure 12		
32.	Undertaking	Annexure-13		
33.	Undertaking Compliance regarding restrictions under Rule 144 (xi) of the General Financial Rules (GFRs),2017	Annexure-14		
34.	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: After Sales Service Certificate
(To be enclosed with Technical bid)

AFTER SALES SERVICE CERTIFICATE

Dated: _____

The Special Secretary (IT) and the Treasurer, CRID
Citizen Resources Information Department (CRID)
SCO 109-110 Sector 17 B, Chandigarh. 160017

Subject: E-Tender/CRID/Revenue ICT Infra/2025-26

Whereas, we M/s (Bidder Name) are established for sales & services of (Make of items) of [items name] having service offices at following locations. Details are as under:

S#	OEM Name	Address of Service Centre	Phone No
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: Undertaking Of Rates

(To be enclosed/uploaded with the commercial bid)

UNDERTAKING OF RATES

Dated: _____

The Special Secretary (IT) and the Treasurer, CRID
Citizen Resources Information Department (CRID)
SCO 109-110 Sector 17 B, Chandigarh. 160017

Subject: E-Tender/CRID/Revenue ICT Infra/2025-26

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, we quote less rates than this offer to any other customer within 1 month of the due date of this offer, then double of the difference in amount will be refunded to CRID. We also confirm that in case our Company/principal officially reduce the price before the delivery or within 15 days from the date of delivery, then the benefit for the same will be passed to CRID.

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 CRID or from the 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: Relaxations to Haryana based manufacturing Micro & Small Enterprises

(To be submitted on its Letterhead by the bidder)

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

Subject: e-Tender/CRID/Revenue ICT Infra/2025-26

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 Undertaking) 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 Undertaking)

   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 Undertaking.
4. That in case the purchase 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: Relaxations to Haryana based manufacturing Medium Enterprise

(To be submitted on its Letterhead by the bidder)

Format for Relaxations to Haryana based manufacturing Medium Enterprise
(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/CRID/Revenue ICT Infra/2025-26

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 Undertaking)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 purchase 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 Undertaking.
4. That in case the Purchase 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 based in Haryana, (address mentioned as at Sr. No.1).
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: Authenticity of submitted documents/information

(To be submitted on its Letterhead by the bidder)

Authenticity of submitted documents/information

Subject: e-Tender/CRID/Revenue ICT Infra/2025-26

Undertaking 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 CRID are genuine and true and nothing has been concealed.
3. I shall have no objection in case the CRID verifies them from issuing authority (ies). I shall also have no objection in providing the original copy of the document(s), in case the CRID 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 CRID 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 CRID 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 CRID 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 CRID 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 Undertakings 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: No Conviction

(To be submitted on its Letterhead by the bidder)

Subject: e-Tender/CRID/Revenue ICT Infra/2025-26

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 non-bail able offence, by any of the courts.
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 offence under any of the laws applicable in the country.
3. That I hereby confirm and declare that none of my/ our group/ sister concern/ associate company is participating/ submitting this tender.
4. 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./ Public Sector Undertaking, as on bid submission date.
5. 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.
6. 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.
7. 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.
8. 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.
9. I hereby confirm that in case, any document, information & / or certificate submitted by me found to be incorrect / false / fabricated, the CRID 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: Compliance regarding Rule 144 (xi) of the (GFRs),2017

(To be Provided on letterhead along with Technical bid)

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

Dated: _____

The Special Secretary (IT) and the Treasurer, CRID
Citizen Resources Information Department (CRID)
SCO 109-110 Sector 17 B, Chandigarh. 160017

Subject: Tender No: - e-Tender/CRID/Revenue ICT Infra/2025-26

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

v. 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)

Appendix 1: Request for clarification

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

Date: _____

To
The Special Secretary (IT) and the Treasurer, CRID
Citizen Resources Information Department (CRID)
SCO 109-110 Sector 17 B, Chandigarh. 160017

Subject: e-Tender/CRID/Revenue ICT Infra/2025-26

Bidder's Request for Clarification/ Pre-bid Queries format {to be filled by the bidder}				
Name of the Bidder/ Company/ Firm /Agency:				
Name of Person(s) Representing the Bidder/ Company/ Firm / Agency:	Name of Person	Designation	Email-Id(s)	Tel. Nos. & Fax Nos.
Bidder/ Company/ Firm / Agency Contacts:	Contact Person(s)	Address for Correspondence	Email-Id(s)	Tel. Nos. & Fax Nos.
Query / Clarification Sought:				
S. No.	RFP Page No.	RFP Section No.	Content of Section (Details from RFP document)	Query/ Suggestion/ Clarification required
1.				
2.				
3.				

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)

Appendix 2: Format for Performance Bank Guarantee

Performance Bank Guarantee

Ref: _____ Date: _____

Bank Guarantee No.: _____

To
The Special Secretary (IT) and the Treasurer, CRID
Citizen Resources Information Department (CRID)
SCO 109-110 Sector 17 B, Chandigarh. 160017

Dear Sir,
PERFORMANCE BANK GUARANTEE – For

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 in your favor for an amount of _____% 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 ____% 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 ……. 2025.

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
The Special Secretary (IT) and the Treasurer, CRID
Citizen Resources Information Department (CRID)
SCO 109-110 Sector 17 B, Chandigarh. 160017

(hereinafter referred to as Beneficiary / Government)

BANK GUARANTEE FOR EMD against e-Tender for Procurement for upgradation of Servers, Storage & IT related Equipment through Central Public Sector Units (PSU's) –in a Single Bid System For New Haryana Secretariat, Sector-17, Chandigarh.

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: ₹85,00,000/- (Rupees Eighty Five Lakh only)
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 of Special Secretary (IT) and the Treasurer, Citizen Resources Information Department (CRID), Chandigarh 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 ₹85,00,000/- (Rupees Eighty Five Lakh only 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 12months from the Bid Submission date up to ₹85,00,000/- (Rupees Eighty Five Lakh only in words) and any demand in respect thereof should reach the Bank not later than the above date.

Dated .....

For.....

(Indicate the name of the Bank)

Signature.....

Name of the Officer.....

Designation of the officer .....

Code no .....

Name of the Bank and Branch.....

Appendix 4: Make in India preference exemption order

Haryana Government
Citizen Resources Information Department

हरियाणा सरकार
नागरिक संसाधन सूचना विभाग

Order

No. Admin/14-B/1SIT/ 18895
Dates 06.06.2023

Pursuant to the decisions of Joint Tender Committee to finalize the two RFPs for **revamping of Local Area Networks of Haryana Civil Secretariat, Chandigarh, Haryana New Secretariat, Chandigarh and 25 mini secretariat buildings in 21 districts of Haryana except CharkhiDadri** and decision of the State Technical Committee in its 132nd meeting, the joint tender committee is seeking exemption from Public Procurement (Preference to Make in India) Clause for the RFPs. The RFPs along with its clauses have been approved by following the due procedure of the Government.

1. The exemption referred to in the above-cited subject was requested by the constituted committee for the above mentioned LANs RFPs (i.e. RFPs for revamping of Local Area Networks of Haryana Civil Secretariat, Chandigarh, Haryana New Secretariat, Chandigarh and 25 mini secretariat buildings in 21 districts of Haryana except Charkhi Dadri)along with their justification which is mentioned hereunder as follows:

    a) The secretariat building LANs are critical for Government processes and day-to-day functioning of offices located in these buildings.
    b) The data and files stored on systems connected to these LANs and transmission of such data over networks necessitates latest security features be built into the active components i.e. Network Switches.
    c) The LANs to be established will be integrated with NKN/NICNET and HSWAN also, which necessitates that all active components and cabling components should be compatible with the existing networking equipment installed in NKN/NICNET and HSWAN.
    d) As Video conferencing services are also being revamped in all Districts Mini Secretariats, the high-end equipment under VC services and the proposed Intrusion Prevention Systems (IPS) must integrate seamlessly with the LAN switches.
    e) Sufficient availability of spares, replacements and active support system is required for smooth functioning of the LANs.

2. On the above basis and based on the recommendation of the Administrative Secretary to the Government of Haryana, Electronics & Information Technology Department (now CRID), the Hon'ble Chief Minister (concerned Minister-in-Charge)has granted exemption from Public Procurement (Preference to Make in India- MII) for procurement of the items/services as mentioned in the RFPs(refer to para 1 above) as per Clause 13 of the

9th Floor, Haryana Civil Secretariat, Sector-1, Chandigarh. 160001
Tel: PS(CRID)0172 2740441, Director (Admn): 2748142
E-mail: psit@hry.in Website.www.haryanait.nic.in

Haryana Government
Citizen Resources Information Department

हरियाणा सरकार
नागरिक संसाधन सूचना विभाग

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. The following conditions shall be applicable:

i. The bid should not be restrictive to any MII OEM thereby allowing wider participation of the OEMs and at the same time not restricting any MII OEMs to participate in the tenders.
ii. Exemption is 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.:Admn/14-B/1SIT/ 18896

Chandigarh Dated, the 16.06.2023

A copy is forwarded to the following:

1. Secretary, SSIT for information of SSIT.
2. State Informatics Officer, NIC Haryana

19/06/23 Neeraj 19/06/23

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

OK

9th Floor, Haryana Civil Secretariat, Sector-1, Chandigarh. 160001
Tel: PS(CRID)0172 2740441, Director (Admn): 2748142
E-mail: psit@hry.in Website.www.haryanait.nic.in

The exemption to Make In India (MII) preference as per the OM on pre-page will be applicable for the following LAN Items only:

S#	Items Descriptions
1	Core Switches
2	Distribution Switches
3	Edge Switches
4	Rack Servers for NMS Software With 55" LED Display
5	Computers with 55" Display for NMS Software
6	25G SFPs Transceivers (Single Mode)
7	6 Core Fiber Cable (Single Mode)
8	24 Port LIU Fully Loaded
9	12 Port LIU Fully Loaded
10	6 Port LIU Fully Loaded
11	Fiber Patch Cord 3M (Single Mode)
12	10G SFP Transceivers MM
13	6 Core Fiber Cable MM
14	24 Port LIU Fully Loaded
15	12 Port LIU Fully Loaded
16	6 Port LIU Fully Loaded
17	Fiber Patch Cord 3M
18	Cat 6A Cable
19	Cat 6A 24 Port Fully Loaded Jack Panel
20	Cat 6A I/O Complete Set
21	Cat 6A Patch Cord 1M
22	Cat 6A Patch Cord 3M
23	Cat 6 Cable
24	Cat 6 24 Port Fully Loaded Jack Panel
25	Cat 6 I/O Complete Set
26	Cat 6 Patch Cord 1M
27	Cat 6 Patch Cord 3M