Sr. No.	RFP Pg No.	RFP Clause No	RFP Clause	Clarification	UPCL Response
1			We understand that this RFP is critical for billing and revenue to UPCL and APM has much more to deliver and add value in the IT and application environment, hence we request and suggest UPCL team to add below generic APM requirement to get most optimistic ROI on the solution (along with related features)		As per RFP (As per solution proposed by SI)
2	BoQ1 & BoQ2		Annual Technical Support (ATS) Cost after Go- live period	Kindly let us know where the bidder should quote ATS/AMC cost for 5 years post Go-live for DC & DR in BoQ1 and BoQ2.	As per RFP (Refer BoQ)
3	BoQ1 & BoQ2		Facility Management Service (FMS) Cost	Kindly let us know where the bidder should quote FMS cost for DC & DR in BoQ1 and BoQ2.	As per RFP (Refer BoQ)
4	326-328	Annexure-VI/Specification-Compute	10. Ethernet ports: Min 2 x 10G BaseT and 2*Quad Port 10/25G Ethernet Ports.	Min 2 x 10G BaseT and 2*Dual Port 10/25G Ethernet Ports.	10. Ethernet ports: Min 2 x 10G BaseT and 8X Port 10/25G SFP+ Ethernet Ports with Transceiver/cable.
5	326-328	Annexure-VI/Specification-Compute	14. Configuration & Management : Zero-touch repository manager and self-updating firmware system, Automated hardware configuration and Operating System deployment to multiple servers	Zero Touch Provisioning (ZTP) using SSDP with remote access	Zero-touch provisioning with Automated hardware configuration and Operating System deployment to multiple servers.
6	326-328	Annexure-VI/Specification-Compute	17. Application Resource Management	pls do remove this, as this not related to Server hardware specification.	The solution should provide a workload automation solution that dynamically defines and controls the environment based on real time analytics to assure application performance at maximum efficiency by ensuring underlying infrastructure is at optimal state. The solution should be an agentless architecture which should provide full stack visibility with intelligent operations with capacity uitlization metrics with cluster, CPU, memory storage runway & time series analysis with critical alterts, warning & events. The solution should provide dynamic resource allocation to ensure demand of applications is matched with available resources in real time. The solution should also provide a self service portal with low code automation with built in tasks for server, virtualizatoin provisioning the solution should have vertical and horizontal scaling of workloads and automate provisioning of infrastructure resources. The solution should also provision porposed network switches, storage , firewalls and load balancers to ensure seamless provisioning.
7	326-328	Annexure-VI/Specification-Compute	18. Server Node Security : Automatic BIOS recovery - Rapid OS recovery	BIOS recovery OS recovery	18. Server Node Security : BIOS recovery, OS recovery
8	326-328	Annexure-VI/Specification-Compute	3. Memory Slot : 32 DDR4/DDR5 DIMM slots RDIMMS& LR DIMMS supporting speeds up to 4800MT/s. System should support Intel Optane DC Persistent memory and scalable up to 8TB of Memory	24 DDR4/DDR5 DIMM slots RDIMMS& LR DIMMS supporting speeds up to 4800MT/s.	32 DDR4/DDR5 DIMM slots RDIMMS& LR DIMMS supporting speeds up to 4800MT/s and scalable up to 4TB of Memory.

9	112		Hardware Technical specifications Annexure-VI Specification- DDoS Sr. No. 4	Every DDoS appliane has some capacity to mitigate attacks as well along with legit throughput handling. Inbound and Outbound traffic should be considered for sizing. Suggested Clause: Mitigation Capacity: 20Gbps * Data should be publically available	DDoS Flood Attack Prevention Rate: 25MPPS (In addition to Legitimate throughput) Legitimate throughput handling: 2Gbps from day-1 and scalable upto 12Gbps Attack Concurrent Sessions : Unlimited Inspection Ports supported : 6 x 10G Fiber and 4 x 1G Fiber from day-1 Latency should be less than 80 microseconds. The appliance should have dedicated 2 x 1G RJ45 Out-of-band Management Port and RJ45 Console Port Mitigation Capacity: 20Gbps Redundant Power Supply : Yes * Data should be publically available
10	417 of 479		Specification- DDoS 4. DDoS Flood Attack Prevention Rate: 25MPPS (In addition to Legitimate throughput) Legitimate throughput handling: 2Gbps from day-1 and scalable upto 12Gbps Attack Concurrent Sessions : Unlimited Inspection Ports supported : 6 x 10G Fiber and 4 x 1G Fiber from day-1 Latency should be less than 80 microseconds. The appliance should have dedicated 2 x 1G RJ45 Out-of-band Management Port and RJ45 Console Port * Data should be publically available	New Gehration hardware wont support 1gig connectivity. We can achive 1gig copper or fiber connectivity by placing a Layer 2 switch. Please change the port count as 10gig fiber, 25Gig 40Gig and 100Gig support. As department is looking for an appliance based solution which will be able to handle the traffic based on its throughput capacity. Appliance/Hardware performance depends upon its resources like CPU, Memory, Max. throughput etc. thus will be able to handle traffic maximum to its hardware resources capacity and not to Unlimited attack concurrent session. Please change to 1 x 10/100/1000 Copper Ethernet Out-of-band Management Port as its specific to OEM. Kindly modify clause as" 4. DDoS Flood Attack Prevention Rate: 25MPPS (In addition to Legitimate throughput) Legitimate throughput handling: 2Gbps from day-1 and scalable upto 12Gbps ~~Attack Concurrent Sessions : Unlimited~~ Inspection Ports supported : 8 x 10G Fiber and 2 x 40G Fiber from day-1 Latency should be less than 80 microseconds. ~~The appliance should have dedicated 1 x 1G RJ45 Out-of-band~~	As per RFP
11	417 of 479		Specification- DDoS 5. System should support horizontal and vertical port scanning behavioral protection.	Please change Equivalent feature as mentioned clause is specific to one OEM. Kindly modify clause as" 5. System should support horizontal and vertical port scanning behavioral protection. or Equivalent features.	As per RFP
12	New Clause		Hardware Technical specifications. Annexure-VI Specification- DDoS	As DDoS appplaicnea asked in Dc same compement should be asked in DR site as well to ensure protection as well as their availability of DR site .	Accepted.

13	Page 112	Suggestive clause	Page 112 / Specification- DDoS	As all internet facing web applications will be over SSL/TLS, we recommend to add the following clause in DDoS mitigation solution: Suggestive Clause The solution should be able to inspect and detect DDoS attacks on encrypted packets over any SSL/TLS protocols including 1.1, 1.2 and 1.3.	As per RFP
14	Page 112	Suggestive clause	Page 112 / Specification- DDoS	Geo Fencing is a critical component of DDoS protection. Based on our experience in preventive actions against DDoS attacks, we request the following modification to the existing clause: Suggestive Clause It should be possible to block Geographical Locations to prevent flooding attacks from a particular country / countries. The geo blocking should support blocking only inbound traffic, only outbound traffic and/or both.	As per RFP
15		DDoS	Addition of Clause	IPV6 certification provides the full feature after approximately 450 tests done by Department of Telecommunications approved LAB. So It is suggested to add the clause as "The device should support for IPv4 and IPv6 traffic have the ability to run in dual stack mode and solution should be IPv6 ready logo certified from day 1"	As per RFP
16		DDoS/ Point 4	DDoS Flood Attack Prevention Rate: 25MPPS (In addition to Legitimate throughput) Legitimate throughput handling: 2Gbps from day-1 and scalable upto 12Gbps Attack Concurrent Sessions : Unlimited Inspection Ports supported : 6 x 10G Fiber and 4 x 1G Fiber from day-1 Latency should be less than 80 microseconds. The appliance should have dedicated 2 x 1G RJ45 Out-of-band Management Port and RJ45 Console Port * Data should be publically available	As per the present datacentre/It infra requirement standard, 10G ports are recommended over 1G, For a DDoS Miti gation device which will placed at the perimeter it's highly recommended to go with SFP+ ports which gives the flexibility to adopt to 1G ports as well as 10 G ports as per the requirements and there is no use case of ask of MGMT port redundancy. For Application DDOS, SSL parameter is very important and Now a days, Application traffic is 100% SSL based.] It is suggested to amend the clause as :- DDoS Flood Attack Prevention Rate: 25MPPS (In addition to Legitimate throughput) Legitimate throughput handling: 2Gbps from day- 1 and scalable upto 12Gbps Attack Concurrent Sessions : Unlimited Inspection Ports supported : 6 x 10G Fiber. RSA CPS(2K Key): 50 K ECC CPS (EC-P256): 35 K with TLS1.3 Support HDD - 4 TB Latency should be less than 80 microseconds. The appliance should have dedicated 1G RJ45 Out-of-band Management Port and RJ45 Console Port * Data should be publically available	As per RFP

17	102		Proposed Appliance should have atleast 4 TB of Storage on the box.	Specific to an OEM appliance, hence requesting change for wider participation. Revised Clause:Proposed Appliance should have at least 2 TB of Storage on the box.	Proposed Appliance should have atleast 2 TB or higher of Storage on the box.
18	102	Email Security 2	Proposed solution must be hardware Appliance based with hardened operating system.	We hereby request to consider the point" The solution should be hardware based or software deployed on a dedicated hardware"	Proposed solution must be hardware Appliance or software deployed on a dedicated hardware.
19	102		The proposed solution must support both 32-bit / 64-bit Windows 8,8.1 & 10, Windows 2003 ,2008 & 2016 server sandbox images and should allow atleast three types of sandbox images for virtual analysis.	As there are multiple security tools thus as a solution there has to be a unified sandbox platform which allows to have a single source of truth for malware and ransomware detection rather than having multiple sandbox appliance which do not offer end to end integration. hence requesting change	As per RFP
20	102		The Proposed solution must support deployment modes in SPAN/TAP, BCC and MTA mode.	Email Security appliance should be an MTA appliance, SPAN and TAP mode can not block malicious emails natively and would depend on external agents hence requesting change. Revised Clause:The Proposed solution must support deployment modes in BCC and MTA mode.	The Proposed solution must support deployment modes in SPAN/TAP/BCC and MTA mode.
21	103		Solution must support Custom Sandbox Domain Check, Software Check, User Settings check, Prequisite file check, Office version check, Windows License check, Browser Check (Sandbox Customized with OS and Applications in the Environment to maximise targeted attack detection capabilities)	The change doesn't do any functional change but allow more vendors to participate and thus requesting change. Revised Clause:Solution must support sandbox Domain Check, Software Check, User Settings check, Perquisite file check, Office version check, Windows License check, Browser Check and application in the environment to maximise targeted attack detection capabilities	Solution must support sandbox Domain Check, Software Check, User Settings check, Perquisite file check, Office version check, Windows License check, Browser Check and application in the environment to maximise targeted attack detection capabilities
22	103		Solution must support YARA Rules for malware identification.	YARA rule on email is specific to a vendor, thus to allow more vendors to participate requesting change Revised Clause:Solution must support YARA/SNORT/Customer Rules for malware identification.	Solution must support YARA/SNORT/Customer Rules for malware identification.
23	105		The Proposed solution should allow atleast three types of sandbox images	Repeat of above point S.No 13.Kindly remove this clause	Deleted
24	105		The Proposed solution should have an option for timeout/ release of an email, if the file analysis on the sandbox if over 20 mins.	Timeout value should be configurable as 20mins is too large of time to hold emails for analysis so depending on the severity and user it should be configurable thus requesting change. Revised Clause:The Proposed solution should have an option for configurable timeout/ release of an email, if the file analysis on the sandbox if over configured timer.	The Proposed solution should have an option for configurable timeout/ release of an email, if the file analysis on the sandbox if over configured timer.

25	105		The Proposed solution should support Windows 2003 ,2008 & 2016, 2019 server sandbox images	Repeat of above point S.No 13.Kindly remove this clause	Deleted
26	105		The Proposed solution should support Windows 8 ,8.1 & 10 sandbox images	Repeat of above point S.No 13.Kindly remove this clause	Deleted
27	108		Solution should be able to centrally manage and deploy sandbox image update to managed products.	As government domains are migrating to local language and domains, it is imp to have them included as solution so that IDN based emails can be processed and analysed in the solution thus requesting change. Revised Clause:The solution should support multi-language in English, Hind, Tamil & Odia. The bidder must provision for support in other regional languages. The current Email service is configured with Hindi domains i.e., with user id as which is being provided based on user requirements. The bidder should provision for feature of IDN with support in more Indian regional language	As per RFP
28		Email Security 8,9,11,13,15,42,47 ,48,49,82		We hereby request to consider emulation based sandbox for dynamic/behvioral analysis	As per RFP Bidders are free to quote any addtional features and functionalities in addtion to defined functional scope.
29	134		All Annexure Document Specification- EMS/NMS Solution (For Minimum 500 devices) Sr NO-4 :	Existing Clause:Mapping Features: Automated map creation, Customizable topology maps, Multi-level topology views and on-demand map creation with lat long GIS plotting in-built on the tool. Query: As the Topology can be created on 2d Flat map for network visualization. Here providing Map Creation with Lat long GIS Plotting is GIS map tool funtionality. However individual devices can be plotted on Geo Map but Topology is not standard function of Map, hence we request authority to modify this clause as mentioned below: Suggested Clause: Mapping Features: Automated map creation, Customizable topology maps, Multi-level topology views.	As per RFP
30	138		All Annexure Document - Specification- EMS/NMS Solution (For Minimum 500 devices) Part B Out of box Support for following: Sr NO-27	Existing Clause:Web Server/Services: Real Browser Monitoring with Web User Experience, Secure Apache Server, HTTP(s) URLs, HTTP(s) URL Sequence, IIS Server, SSL Certificate Monitor, Web Servers, Web Services, Website Content Monitor etc. Query: As the functionality Real Browser Monitoring with Web User Experience is of APM tool, requesting you to please clarify if APM is required here or not? if yes please let us know howmany number of APM agents will be require based on Application instances.	As per solution proposed by SI

31			"General Monitoring Features: Able to support instant diagnosis of the node status through Ping, SNMP Walk / Mib Walker, Telnet, SSH, MAC Filtering, Trace route and Remote Desktop, WMI application monitoring, Blackout period to suspend specific actions during the scheduled period of time, Configurable Alert and Notification escalation policies, Mobile Interface, Configurable role-based management with granular control over the user roles, groups roles, user/group attributes, Scheduling of automatic on-demand custom and recurring reports, Support of wild card search with regular expression matching and filtering with attributes for device configuration, inventory or other device specific information"	Request to give more clairity on Blackout period under General Monitoring feature	As per RFP
32		EMS/NMS Solution (For Minimum 500 devices)- General Monitoring Features	General Monitoring Features: Able to support instant diagnosis of the node status through Ping, SNMP Walk / Mib Walker, Telnet, SSH, MAC Filtering, Trace route and Remote Desktop, WMI application monitoring, Blackout period to suspend specific actions during the scheduled period of time, Configurable Alert and Notification escalation policies, Mobile Interface, Configurable role- based management with granular control over the user roles, groups roles, user/group attributes, Scheduling of automatic on- demand custom and recurring reports, Support of wild card search with regular expression matching and filtering with attributes for device configuration, inventory or other device specific information	Request to give more clarity on Blackout period under General Monitoring feature	As per RFP
33		EMS/NMS Solution (For Minimum 500 devices)>> IT Operations Monitoring Features >> Monitoring	Monitoring: ICMP Ping Check, TCP Based Status Polling (for Non ICMP Environment), Schedule downtime, Service Level Management Dashboards, Support for adding custom device types, Real-time Perf. and Traffic Monitoring via SNMP, Management Console with reporting tool, Web and Windows based management console. The portal should support dynamic gadgets and widgets for data representation with live animations and live data representation.	Request to modify this clause as per following: ICMP Ping Check, TCP Based Status Polling (for Non ICMP Environment), Schedule downtime, Service Level Management Dashboards, Support for adding custom device types, Real-time Perf. and Traffic Monitoring via SNMP, Management Console with reporting tool, Web Or Windows based management console. The portal should support dynamic gadgets and widgets for data representation with live animations and live data representation.	Monitoring: ICMP Ping Check, TCP Based Status Polling (for Non ICMP Environment), Schedule downtime, Service Level Management Dashboards, Support for adding custom device types, Real-time Perf. and Traffic Monitoring via SNMP, Management Console with reporting tool, Web Or Windows based management console. The portal should support dynamic gadgets and widgets for data representation with live animations and live data representation.

34		EMS/NMS Solution (For Minimum 500 devices)>> IT Operations Monitoring Features >> Reporting	Reporting: SLA Dashboards for Servers, Routers, Switches etc. All Servers Availability / Outage Report, Health Report for Servers, Routers, Switches etc. TopN Servers by CPU, Memory and Disk, Top N Servers by Interface traffic report, Server access report through firewall logs. TopN report for routers by CPU and Memory Utilization, Interface Traffic/Utilization/Error Reports, Peak time reports (Eg. 8:00am to 8:00pm), WAN Link availability/ RTT report, Forensic reports, Bandwidth capacity planning reports, Traffic reports, User audit reports, Schedule Reports, Custom Reports, Export Reports (PDF,XLS, CSV formats), Email/Print report directly to printer..	Request to give more clarity on Forensic reports under Reporting feature	As per RFP
35	19		Should have seamless native integration with Anti – APT solution bi-directionally to detect and mitigate zero day threats having common threat sharing platform for holistic visibility and control also should have seemless integration with existing running endpoint security solution having common management platform also proposed solution should be able to generate out of box reports to highlight Infections, C&C behavior, Lateral Moment, Asset and data discovery and data Exfiltration.	Remove point	Deleted
36	91		Ransomware rollback: Detects ransomware with runtime machine learning and expert rules to block encryption processes in milliseconds. Rollback/restores any files by taking backup of ransom ware encrypted files and restoring the same before detection also detects script emulation, zero-day exploits, targeted and password-protected malware commonly associated with ransomware having a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.	Rollback capability works only on windows device using shadow copy feature which is not scalable and can easily be bypassed. Hence requesting change. Revised Clause:Ransomware rollback: Detects ransomware with runtime machine learning and expert rules to block encryption processes in milliseconds.	Proposed solution should have capability to protect any Ransomeware infection along with rollback/restores capability.
37	91		Should detect from Targeted and known ransomware attacks, Zero- day malware and document exploits, Attacker behavior and network activity, Web threats, including exploits and drive-by downloads, Phishing, spear phishing, and other email threats, Data exfiltration, Bots, Trojans, worms, keyloggers and Disruptive application having capability to do retrospective scan on CnC, Script Analyzer, Automatically send executable to virtual analyzer and can crack password protected compressed files	Specific to an OEM appliance, hence requesting change for wider participation. Revised Clause:Should detect and prevent from attacks like Targeted and known ransomware attacks, Zero- day malware and document exploits, Attacker behaviour and network activity, Web threats, including exploits and drive-by downloads, Phishing, spear phishing, and other email threats, Data exfiltration, Bots, Trojans, worms, keyloggers and Disruptive application having capability to do retrospective scan on CnC, Script Analyzer, Automatically send executable to virtual analyser and can crack password protected compressed files	As per RFP

38	92		Includes a granular list of truly international identifiers to identify specific data by patterns, formulas, positioning, and more. Identifiers can also be created from scratch and should offers visibility and control of data in motion of sensitive information— whether it is in email, webmail, instant messaging (IM), SaaS applications, and most networking protocols such as FTP, HTTP/HTTPS, and SMTP and continuously monitors data at rest, in use, and in motion to prevent data loss	DLP should be looked as a holistic solution covering endpoint , network and data at rest thus requesting change. Kindly remove this clause.	As per RFP
39	92		Should have data loss prevention capability with pre-defined templates for HIPAA, PCI-DSS, GLBA etc. for compliance requirements and should have capability to create policies on basis of regular expression, key word and dictionary based having visibility and control of data that's being used in USB ports, CDs, DVDs, COM and LPT ports, removable disks, infrared and imaging devices, PCMCIA, and modems. It can also be configured to monitor copy and paste and print screen and capability with pre- defined templates for HIPAA, PCI-DSS, GLBA etc. for compliance requirements and should have capability to create policies on basis of regular expression, key word and dictionary based	DLP should be looked as a holistic solution covering endpoint , network and data at rest thus requesting change. Kindly remove this clause.	As per RFP
40	92		Should empowers IT to restrict the use of USB drives, USB attached mobile devices, CD/DVD writers, cloud storage, and other removable media with granular device control and DLP policies and ability to Detects and reacts to improper data use based on keywords, regular expressions, and file attributes having granular device control with the following control actions: Read only, Read and write, Read, write and execute	DLP should be looked as a holistic solution covering endpoint , network and data at rest thus requesting change. Kindly remove this clause.	As per RFP
41	92		The Proposed solution should monitor (East-West) traffic of attack for inspection to detect lateral movement (attack activities) inside the network (beyond C&C connections) also solution should have threat emulation capability to cater zero day threat by simulating at least 20 virtual machines scalable up to 60 on same appliance running simultaneously having OS support i.e. Windows XP, Win7, Win8/8.1, Win 10, Windows Server 2003, 2008, 2012, 2016,2019 and Linux complete solution should have common threat sharing platform	As there are multiple security tools thus as a solution there has to be a unified sandbox platform which allows to have a single source of truth for malware and ransomware detection rather than having multiple sandbox appliance which do not offer end to end solution. Revised Clause:The Proposed solution should monitor (East-West) traffic of attack for inspection to detect lateral movement (attack activities) inside the network (beyond C&C connections) also solution should have threat emulation capability to cater zero day threat by simulating at least 20 virtual machines scalable up to 60 on same appliance running simultaneously having OS support i.e. Windows OS/Server solution should have common threat sharing platform	As per RFP

42	93		Discover, monitor, block and encrypt private data with real-time view of endpoint status and broad coverage of communication systems: email, webmail, IM, P2P, FTP, Skype, Windows File Share, ActiveSync, and detect data-stealing malware: Identify botnets, hidden FTP processes, keyloggers, spyware, and Trojans that attempt to collect and send data and should offers visibility and control of data in motion of sensitive information—whether it is in email, webmail, instant messaging (IM), SaaS applications, and most networking protocols such as FTP, HTTP/HTTPS, and SMTP.	DLP should be looked as a holistic solution covering endpoint , network and data at rest thus requesting change. Kindly remove this clause.	As per RFP
43	93		Prevents potential damage from unwanted or unknown applications (executables, DLLs, Windows App store apps, device drivers, control panels, and other Portable Executable (PE) files) also Should have dynamic policies that still allow users to install valid applications based on reputation-based variables like the prevalence, regional usage, and maturity of the application	DLP should be looked as a holistic solution covering endpoint , network and data at rest thus requesting change. Kindly remove this clause.	As per RFP
44	93		Uses application name, path, regular expression, or certificate for basic application whitelisting and blacklisting containing broad coverage of pre-categorized applications that can be easily selected from application catalog (with regular updates) having features roll- your-own application whitelisting and blacklisting for in-house and unlisted applications, ensures that patches/updates associated with whitelisted applications can be installed, as well as allowing your update programs to install new patches/updates, with trusted sources of change.	DLP should be looked as a holistic solution covering endpoint , network and data at rest thus requesting change. Kindly remove this clause.	As per RFP
45	94		Should protect storage devices i.e. EMC, NetApp, Hitachi Data Systems storage systems also should encrypt private data with fully integrated full disk, file folder, USB, and removable media encryption also should manage encryption policies and protect data on PCs, Macs, laptops, desktops, USBs, and removable media also Solution must support CPU usage performance control during scanning -Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer i.e. High, Medium and low also should be APT ready capable of submitting SO (Suspicious Objects) to On-Premise Sandbox appliance for analysis without additional License on Endpoint.	DLP should be looked as a holistic solution covering endpoint , network and data at rest thus requesting change. Kindly remove this clause.	As per RFP

46	95		Should have IOA Behavioral Analysis detects behavior that matches known indicators of attack (IOA), including ransomware encryption behaviors, script launching, In-memory runtime analysis malicious script detection, malicious code injection, runtime un- pack detection, Isolation, Quarantine, Process kill, Execution block and Damage rollback, achieve context-aware endpoint investigation and response (EDR), recording and detailed reporting of system- level activities to allow threat analysts to rapidly assess the nature and extent of an attack. Custom detection, intelligence, and controls, Record detailed system-level activities and perform multi- level search across endpoints using rich-search criteria such as OpenIOC, Yara, and suspicious objects, Detect and analyze advanced threat indicators such as fileless attacks.	Specific to an OEM appliance, hence requesting change for wider clause. Revised Clause:Should have IOA Behavioural Analysis detects behaviour that matches known indicators of attack (IOA), including ransomware encryption behaviours, script launching, In-memory runtime analysis malicious script detection, malicious code injection, runtime un- pack detection, Isolation, Quarantine, Process kill, Execution block, achieve context-aware endpoint investigation and response (EDR), recording and detailed reporting of system- level activities to allow threat analysts to rapidly assess the nature and extent of an attack. Custom detection, intelligence, and controls, Record detailed system-level activities and perform multi- level search across endpoints using rich-search criteria such as OpenIOC, Yara, SNORT and suspicious objects, Detect and analyze advanced threat indicators such as fileless attacks.	As per RFP
47	96		Proposed OEM should be leader in advance Global Vulnerability Research and Discovery market share as per Frost & Sullivan Reports and should be in Leader Quadrant as per Gartner Magic Quadrant of EPP category from last 5 consecutive years and OEM must have contributed at least 30 zeroday/undisclosed vulnerabilities of Microsoft continuously from past 5 years and data should be publically available.	Specific to an OEM appliance, Kindly remove this clause.	As per RFP
48	Page 90	Specification- Endpoint Protection (EPP) Antivirus -> 1	Proposed solution should have capability of AV, Vulnerability Protection, Firewall, Device control, Application Control, Virtual Patching, EDR and DLP in a single agent and should be completely On-premise and should not send any file/sample with cloud to inspect and analyze any threat	Requesting to consider the suggestion and make the changes to exisitng technical statement for maximum participation in the RFP. Suggested Statement- Proposed solution should have capability of AV, Vulnerability Protection, Firewall, Device control, Application Control, EDR and DLP in a single agent and should be completely On-premise and should not send any file/sample with cloud to inspect and analyze any threat	Proposed solution should have capability of AV, Vulnerability Protection, Firewall, Device control, Application Control, Virtual Patching/Automatic Vulnerability shielding having auto rules provisioning and de-provisioning capability, EDR and DLP in a single agent and should be completely On-premise and should not send any file/sample with cloud to inspect and analyze any threat
49	Page 91	Specification- Endpoint Protection (EPP) Antivirus -> 5	Comprehensive storage security uses the industry-standard ICAP protocol to complement support for traditional RPC communication protocols to safeguards a wide range of network attached storage systems by detecting and removing viruses and spyware in real time while users accessing documents	Requesting to remove this pointer as it's not related to EPP solutions and does belongs to storage.	As per RFP

50	Page 92	Specification- Endpoint Protection (EPP) Antivirus -> 8	Should have data loss prevention capability with pre-defined templates for HIPAA, PCI-DSS, GLBA etc. for compliance requirements and should have capability to create policies on basis of regular expression, key word and dictionary based having visibility and control of data that's being used in USB ports, CDs, DVDs, COM and LPT ports, removable disks, infrared and imaging devices, PCMCIA, and modems. It can also be configured to monitor copy and paste and print screen and capability with pre- defined templates for HIPAA, PCI-DSS, GLBA etc. for compliance requirements and should have capability to create policies on basis of regular expression, key word and dictionary based	The identified solution solution offers comprehensive data loss prevention functionality. Requesting to ammend the technical specification stetement to; Recommended Statement- Should have data loss prevention capability with pre-defined templates for HIPAA, PHI, PII, PCI, ITAR, Industry etc. for compliance requirements and should have capability to create policies on basis of regular expression (PAN card, Adhar Card), key word, dictionary, source code, based having visibility and control of data that's being used in USB ports, CDs, DVDs, COM and LPT ports, removable disks, infrared and imaging devices, PCMCIA, and modems, printer, web uploads, email. It can also be configured to monitor copy and paste and print screen and capability with pre- defined templates for HIPAA, PHI, PII, PCI, ITAR, Industry etc. for compliance requirements and should have capability to create policies on basis of regular expression (PAN card, Adhar Card), key word and dictionary, source code based etc.	As per RFP
51	Page 92	Specification- Endpoint Protection (EPP) Antivirus -> 8	Should have data loss prevention capability with pre-defined templates for HIPAA, PCI-DSS, GLBA etc. for compliance requirements and should have capability to create policies on basis of regular expression, key word and dictionary based having visibility and control of data that's being used in USB ports, CDs, DVDs, COM and LPT ports, removable disks, infrared and imaging devices, PCMCIA, and modems. It can also be configured to monitor copy and paste and print screen and capability with pre- defined templates for HIPAA, PCI-DSS, GLBA etc. for compliance requirements and should have capability to create policies on basis of regular expression, key word and dictionary based	The identified solution solution offers comprehensive data loss prevention functionality. Requesting to ammend the technical specification stetement to; Recommended Statement- Should have data loss prevention capability with pre-defined templates for HIPAA, PHI, PII, PCI, ITAR, Industry etc. for compliance requirements and should have capability to create policies on basis of regular expression (PAN card, Adhar Card), key word, dictionary, source code, based having visibility and control of data that's being used in USB ports, CDs, DVDs, COM and LPT ports, removable disks, infrared and imaging devices, PCMCIA, and modems, printer, web uploads, email. It can also be configured to monitor copy and paste and print screen and capability with pre- defined templates for HIPAA, PHI, PII, PCI, ITAR, Industry etc. for compliance requirements and should have capability to create policies on basis of regular expression (PAN card, Adhar Card), key word and dictionary, source code based etc.	As per RFP

52	Page 92	Specification- Endpoint Protection (EPP) Antivirus -> 7	The Proposed solution should monitor (East-West) traffic of attack for inspection to detect lateral movement (attack activities) inside the network (beyond C&C connections) also solution should have threat emulation capability to cater zero day threat by simulating at least 20 virtual machines scalable up to 60 on same appliance running simultaneously having OS support i.e. Windows XP, Win7, Win8/8.1, Win 10, Windows Server 2003, 2008, 2012, 2016,2019 and Linux complete solution should have common threat sharing platform	Requesting to consider the suggestion and make the changes to exisitng technical statement for maximum participation in the RFP. Suggested Statement- The Proposed solution should monitor (East-West) traffic of attack for inspection to detect lateral movement (attack activities) inside the network (beyond C&C connections) also solution should have threat emulation capability to cater zero day threat by simulating at least 20 virtual machines scalable up to 60 on same/different appliance running simultaneously having OS support i.e. Windows XP, Win7, Win8/8.1, Win 10, Windows Server 2003, 2008, 2012, 2016,2019 and Linux complete solution should have common threat sharing platform	The Proposed solution should monitor (East-West) traffic of attack for inspection to detect lateral movement (attack activities) inside the network (beyond C&C connections) also solution should have threat emulation capability to cater zero day threat by simulating at least 20 virtual machines scalable up to 60 on same/different appliance running simultaneously having OS support i.e. Windows XP, Win7, Win8/8.1, Win 10, Windows Server 2003, 2008, 2012, 2016,2019 and Linux complete solution should have common threat sharing platform
53	Page 94	Specification- Endpoint Protection (EPP) Antivirus -> 14	Endpoint vulnerability protection should scan the machine and provide CVE number visibility and accordingly create rule for virtual patch against vulnerability and capable of recommending rules based on vulnerabilities on endpoint and create dynamic rules automatically based on System posture and endpoint posture also blends signature-less techniques, including high-fidelity machine learning, behavioral analysis, variant protection, census check, application control, exploit prevention, and good file check with other techniques like file reputation, web reputation, and command and control (C&C) blocking.	The said statement is favouring specific single OEM and will give dis-advantage to other strong technology vendors to participate in the RFP. Requesting to remove the statement for maximum participation in the RFP	As per RFP
54	Page 96	Specification- Endpoint Protection (EPP) Antivirus -> 22	Proposed OEM should be leader in advance Global Vulnerability Research and Discovery market share as per Frost & Sullivan Reports and should be in Leader Quadrant as per Gartner Magic Quadrant of EPP category from last 5 consecutive years and OEM must have contributed at least 30 zeroday/undisclosed vulnerabilities of Microsoft continuously from past 5 years and data should be publically available.	We would kindly request to remove reference to analyst reports in existing clause as per Indian Government norms. Kindly revise the clause as per below Suggested Clause :- OEM must have contributed at least 30 zeroday/undisclosed vulnerabilities of Microsoft continuously from past 5 years and data should be publically available.	As per RFP
55	Page 96	Specification- Endpoint Protection (EPP) Antivirus -> 22	Proposed OEM should be leader in advance Global Vulnerability Research and Discovery market share as per Frost & Sullivan Reports and should be in Leader Quadrant as per Gartner Magic Quadrant of EPP category from last 5 consecutive years and OEM must have contributed at least 30 zeroday/undisclosed vulnerabilities of Microsoft continuously from past 5 years and data should be publically available.	We would kindly request to remove reference to analyst reports in existing clause as per Indian Government norms. Kindly revise the clause as per below Suggested Clause :- OEM must have contributed at least 30 zeroday/undisclosed vulnerabilities of Microsoft continuously from past 5 years and data should be publically available.	As per RFP
56	2		Solution must support minimum 25 Gbps of Firewall throughput under enterprise test conditions	Solution must support minimum 25 Gbps of Firewall throughput	Solution must support minimum 25 Gbps of Firewall throughput under Throughput (Real World/Production Performance)

57	2		Solution must support minimum 5 Gbps of Threat Prevention throughput and 13 Gbps of NGFW throughput.	Solution must support minimum 10 Gbps of Threat Prevention throughput	As per RFP
58	2		Solution must support minimum 500Mbps of Threat Prevention throughput and 900 Mbps of NGFW throughput.	Solution must support minimum 500Mbps of Threat Prevention throughput and 800 Mbps of NGFW throughput.	As per RFP
59	2		The appliance should have minimum : 8x 1 Gbps Copper/SFP, 4x 10 Gbps SFP+ 1 x RJ45 Management Interface 1 x Dedicated HA/Sync port 1 x Console Port 1 x Additional LOM Port for Out of Band Management connectivity Interfaces/Port must be populated with transceiver as per solution requirement from day one. If any additional interfaces/ports and transceivers are required for implementation of solution, the bidder shall provide the same. The ports provided in the firewall should be configurable in to the WAN/LAN ports as per requirement.	The appliance should have minimum : 8x 1 Gbps Copper, 8x 1Gbps SFP, 4x 10 Gbps SFP+ 1 x RJ45 Management Interface 1 x Dedicated HA/Sync port 1 x Console Port 1 x Additional LOM Port for Out of Band Management connectivity Interfaces/Port must be populated with transceiver as per solution requirement from day one. If any additional interfaces/ports and transceivers are required for implementation of solution, the bidder shall provide the same. The ports provided in the firewall should be configurable in to the WAN/LAN ports as per requirement.	As per RFP
60	3		Solution must not have Application specific chips like ASICs that doesn't allow future firmware and feature expansions on the same hardware. Solution must not use proprietary ASIC chips.	Remove the Point	Deleted
61	4		Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU’s to protect & scale against dynamic latest security threats	Proposed Firewall can be ASIC based in nature / open architecture based on multi-core cpu to protect & scale against dynamic latest security threats.	Proposed Firewall should be open architecture based on multi-core CPU’s / ASIC to protect & scale against dynamic latest security threats.
62	6		The Solution/appliance shall have Threat Prevention throughput of at least 9 Gbps with Application Control, FW, IPS , Anti malware/Anti Virus, Antibot & URL/web protection/Filtering with logging enabled in Enterprise Mix / Application Mix traffic on day 1 and scalable upto 14 Gbps to meet future requirements without replacing the existing hardware.	The Solution/appliance shall have Threat Prevention throughput of at least 9 Gbps with Application Control, FW, IPS , Anti malware/Anti Virus, Antibot & URL/web protection/Filtering with logging enabled in Enterprise Mix / Application Mix traffic on day 1. All the throughput number should be achieved from single device no stacking will be allowed.	As per RFP
63	7		The platform /appliance shall have Next Generation Firewall throughput of at least 22 Gbps with Application Control, FW and IPS with logging enabled in Enterprise Mix / Application Mix traffic on day 1 and scalable upto 30 Gbps to meet future requirements without replacing the existing hardware.	The platform /appliance shall have Next Generation Firewall throughput of at least 11 Gbps with Application Control, FW and IPS with logging enabled in Enterprise Mix / Application Mix traffic on day 1. All the throughput number should be achieved from single device no stacking will be allowed.	As per RFP
64	8		Proposed solution should support at least 16 million concurrent sessions/connections	Proposed solution should support at least 8 million concurrent sessions/connections or higher	As per RFP
65	24		The appliance hardware should be a multi-core CPU architecture with a hardened 64-bit operating system to support 64 GB RAM from day1.	The appliance hardware should be a multi-core CPU architecture with a hardened 64-bit operating system.	As per RFP

66	24		The appliance should have minimum : 8x 1 Gbps Copper/SFP, 4x 10 Gbps SFP+ 1 x RJ45 Management Interface 1 x Dedicated HA/Sync port 1 x Console Port 1 x Additional LOM Port for Out of Band Management connectivity Interfaces/Port must be populated with transceiver as per solution requirement from day one. If any additional interfaces/ports and transceivers are required for implementation of solution, the bidder shall provide the same. The ports provided in the firewall should be configurable in to the WAN/LAN ports as per requirement.	The appliance should have minimum : 8x 1 Gbps Copper, 8x 1Gbps SFP, 4x 10 Gbps SFP+ 1 x RJ45 Management Interface 1 x Dedicated HA/Sync port 1 x Console Port 1 x Additional LOM Port for Out of Band Management connectivity Interfaces/Port must be populated with transceiver as per solution requirement from day one. If any additional interfaces/ports and transceivers are required for implementation of solution, the bidder shall provide the same. The ports provided in the firewall should be configurable in to the WAN/LAN ports as per requirement.	As per RFP
67	24		The appliance should have minimum : 8x 1 Gbps Copper/SFP, 4x 10 Gbps SFP+ 1 x RJ45 Management Interface 1 x Dedicated HA/Sync port 1 x Console Port 1 x Additional LOM Port for Out of Band Management connectivity Interfaces/Port must be populated with transceiver as per solution requirement from day one. If any additional interfaces/ports and transceivers are required for implementation of solution, the bidder shall provide the same. The ports provided in the firewall should be configurable in to the WAN/LAN ports as per requirement.	The appliance should have minimum : 8x 1 Gbps Copper, 8x 1Gbps SFP, 4x 10 Gbps SFP+ 1 x RJ45 Management Interface 1 x Dedicated HA/Sync port 1 x Console Port 1 x Additional LOM Port for Out of Band Management connectivity Interfaces/Port must be populated with transceiver as per solution requirement from day one. If any additional interfaces/ports and transceivers are required for implementation of solution, the bidder shall provide the same. The ports provided in the firewall should be configurable in to the WAN/LAN ports as per requirement.	As per RFP
68	24		The platform /appliance shall have Next Generation Firewall throughput of at least 22 Gbps with Application Control, FW and IPS with logging enabled in Enterprise Mix / Application Mix traffic on day 1 and scalable upto 30 Gbps to meet future requirements without replacing the existing hardware.	The platform /appliance shall have Next Generation Firewall throughput of at least 11 Gbps with Application Control, FW and IPS with logging enabled in Enterprise Mix / Application Mix traffic on day 1. All the throughput number should be achieved from single device no stacking will be allowed.	As per RFP
69	24		The platform /appliance shall have Next Generation Firewall throughput of at least 22 Gbps with Application Control, FW and IPS with logging enabled in Enterprise Mix / Application Mix traffic on day 1 and scalable upto 30 Gbps to meet future requirements without replacing the existing hardware.	The platform /appliance shall have Next Generation Firewall throughput of at least 11 Gbps with Application Control, FW and IPS with logging enabled in Enterprise Mix / Application Mix traffic on day 1. All the throughput number should be achieved from single device no stacking will be allowed.	As per RFP
70	24		The platform /appliance shall have Next Generation Firewall throughput of at least 22 Gbps with Application Control, FW and IPS with logging enabled in Enterprise Mix / Application Mix traffic on day 1 and scalable upto 30 Gbps to meet future requirements without replacing the existing hardware.	The platform /appliance shall have Next Generation Firewall throughput of at least 22 Gbps with Application Control, FW and IPS with logging enabled in Enterprise Mix / Application Mix traffic on day 1.	As per RFP
71	24		The Solution/appliance shall have Threat Prevention throughput of at least 9 Gbps with Application Control, FW, IPS , Anti malware/Anti Virus, Antibot & URL/web protection/Filtering with logging enabled in Enterprise Mix / Application Mix traffic on day 1 and scalable upto 14 Gbps to meet future requirements without replacing the existing hardware.	The Solution/appliance shall have Threat Prevention throughput of at least 9 Gbps with Application Control, FW, IPS , Anti malware/Anti Virus, Antibot protection with logging enabled in Enterprise Mix / Application Mix traffic on day 1.	As per RFP

72	24		The Solution/appliance shall have Threat Prevention throughput of at least 9 Gbps with Application Control, FW, IPS , Anti malware/Anti Virus, Antibot & URL/web protection/Filtering with logging enabled in Enterprise Mix / Application Mix traffic on day 1 and scalable upto 14 Gbps to meet future requirements without replacing the existing hardware.	The Solution/appliance shall have Threat Prevention throughput of at least 9 Gbps with Application Control, FW, IPS , Anti malware/Anti Virus, Antibot & URL/web protection/Filtering with logging enabled in Enterprise Mix / Application Mix traffic on day 1. All the throughput number should be achieved from single device no stacking will be allowed.	As per RFP
73	25		20. Proposed solution must be provided with 4000 or more predefined application signatures (without any customization) from day 1	Changes Require: Proposed solution must be provided with 10000 or more predefined application signatures (without any customization) from day 1. Justification: Pre-Define custom signatures reduces the risk by allowing or blocking the applications based on signature itself which is avoding the dependency of URL filtering and custom application which may open a channel to a threat. Therefore, request to amend the changes as suggested.	As per RFP
74	26		31. The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques.	Changes Require: 31. The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. Solution must detect and block access to Zero phishing sites by scanning all form fields. Justification: Phishing attacks are very common these days and new website are created on daily basis on order to initate phishing attacks which are not in the list of bad URLs, therefore, firewall should be able to scan form fields of the URL to identify the autheticity of the asked credentials by website.	As per RFP
75	26		Proposed solution must have integrated DLP features and can be activated in future with additional licenses also solution must support ICAP/ Rest API integration with third party DLP solution	Proposed solution must have integrated DLP features and can be activated in future with additional licenses also solution must support ICAP/ Rest API integration.	Proposed solution must have integrated DLP features and can be activated in future with additional licenses also solution must support ICAP/ Rest API integration.
76	26		The proposed Anti-APT device must be On-Prem solution and must be managed from same management server.	The proposed Anti-APT device must be On-Prem solution and must be managed from management server or GUI.	The proposed Anti-APT device must be On-Prem solution and must be managed from same management server / same GUI Management.
77	26		The Solution must be able to support 10 Virtual Contexts/ VRF's from day-1 and should be scalable to 20 in future with addition of license if required	The Solution must be able to support 10 Virtual Contexts/ VRF's from day-1.	As per RFP
78	28		Deployment modes - Inline with NGFW, ICAP, Inline w/o NGFW,API & MTA	Anti APT sandbox should be central solution not an inline like a firewall device. Hence requesting change as the said clause is for firewall. Revised Clause:Deployment modes API, Native integration with NGFW, Email MTA, Web Security, NIPS and EDR	As per RFP

79	28		Following Specifications are must :- Unique files per hour:1,000 Form Factor: 1U Virtual Machines: 8 Storage: 1x960 GB SSD Memory: 64 GB	Following Specifications are must :- Unique files per hour:1,000 Form Factor: 1U Virtual Machines: 8 Storage: 1x960 GB SSD	Following Specifications are must :- Unique files per hour:1,000 Form Factor: 1U Virtual Machines: 8 Storage: 1x960 GB SSD Memory: 16 GB
80	28		The proposed solution should able to work with the existing technologies for advance threat protection through web (HTTP & HTTPS) & email protocol. For email APT solution should act as MTA for extraction of active malicious active content and provide real time threat prevention. For HTTPS traffic appliance should support integrated SSL interception/integration with NGFW and should not rely on external SSL unit	Depending on the solution requirement bidder should have a flexibility to enable SSL on the box or outside as in current form it is restricting hence requesting change. Revised Clause:The proposed solution should able to work with the existing technologies for advance threat protection through web (HTTP & HTTPS) & email protocol. For email APT solution should act as MTA for extraction of active malicious active content and provide real time threat prevention. For HTTPS traffic appliance should support integrated SSL interception/integration with NGFW	The proposed solution should able to work with the existing technologies for advance threat protection through web (HTTP & HTTPS) & email protocol. For email APT solution should act as MTA for extraction of active malicious active content and provide real time threat prevention. For HTTPS traffic appliance should support integrated SSL interception/integration with NGFW
81	28		The solution must be able to emulate and extract files embedded in documents. CDR must provide immediately a safe version of potentially malicious content to users. Exploitable content,including active content and various forms of embedded objects must extracted out of the reconstructed file to eliminate potential threats.Access to the original suspicious version must be blocked, until it can be fully analyzed by Zero-Day Protection. CDR functionality can be offered as 3rd party if not available natively.	Specific to OEM hence requesting change. Revised Clause:The solution must be able to emulate and extract files embedded in documents	As per RFP
82	28		Unique files per hour:1,000	Different vendor have different file sandbox measurement per hour file limit is for solutions which scan all the files and not unique files which only requires sandboxing thus requesting change. Revised Clause:Unique files per day:10000	As per RFP
83	29		The solution must monitor for suspicious activity in: API calls, File system changes, System registry, Network Connections, System processes, File creation and deletion, File modification, Kernel code injection , Detect Privilege escalation attempts, Kernel modifications (memory changes performed by kernel code, not the fact that a driver is loaded - this is covered by the item above), Kernel code behavior (monitor activity of non user-mode code), Direct physical CPU interaction , UAC(user access control) bypass detection	The solution must monitor for suspicious activity in: API calls, File system changes, System registry, Network Connections, System processes, File creation and deletion, File modification, Kernel code injection , Detect Privilege escalation attempts, Kernel modifications.	As per RFP
84	29		The solution must monitor for suspicious activity in: API calls, File system changes, System registry, Network Connections, System processes, File creation and deletion, File modification, Kernel code injection , Detect Privilege escalation attempts, Kernel modifications (memory changes performed by kernel code, not the fact that a driver is loaded - this is covered by the item above), Kernel code behavior (monitor activity of non user-mode code), Direct physical CPU interaction , UAC(user access control) bypass detection	The solution must monitor for suspicious activity in: API calls, File system changes, System registry, Network Connections, System processes, File creation and deletion, File modification, Kernel code injection , Detect Privilege escalation attempts, Kernel modifications.	The solution must monitor for suspicious activity in: API calls, File system changes, System registry, Network Connections, System processes, File creation and deletion, File modification, Kernel code injection , Detect Privilege escalation attempts, Kernel modifications , Kernel code behavior, Direct physical CPU interaction , UAC(user access control) bypass detection

85	29		The solution must monitor for suspicious activity in: API calls, File system changes, System registry, Network Connections, System processes, File creation and deletion, File modification, Kernel code injection , Detect Privilege escalation attempts, Kernel modifications (memory changes performed by kernel code, not the fact that a driver is loaded - this is covered by the item above), Kernel code behavior (monitor activity of non user-mode code), Direct physical CPU interaction , UAC(user access control) bypass detection	The solution must monitor for suspicious activity in: API calls, File system changes, System registry, Network Connections, System processes, File creation and deletion, File modification, Kernel code injection , Detect Privilege escalation attempts, Kernel modifications.	The solution must monitor for suspicious activity in: API calls, File system changes, System registry, Network Connections, System processes, File creation and deletion, File modification, Kernel code injection , Detect Privilege escalation attempts, Kernel modifications.
86	29		The solution must provide the ability to be centrally managed and a detailed report must be generated for each one of the malicious files. The detailed report must include: Screen shots, Registry key creation/modifications, Standard security reports , Time lines, Network activity detected	The solution must provide the ability to be centrally managed or GUI and a detailed report must be generated for each one of the malicious files. The detailed report must include: Registry key creation/modifications, Standard security reports , Time lines, Network activity detected	As per RFP
87	29		The solution must provide the ability to be centrally managed and a detailed report must be generated for each one of the malicious files. The detailed report must include: Screen shots, Registry key creation/modifications, Standard security reports , Time lines, Network activity detected	The solution must provide the ability to be centrally managed or GUI and a detailed report must be generated for each one of the malicious files. The detailed report must include: Registry key creation/modifications, Standard security reports , Time lines, Network activity detected	The solution must provide the ability to be centrally managed or GUI and a detailed report must be generated for each one of the malicious files. The detailed report must include: Registry key creation/modifications, Standard security reports , Time lines, Network activity detected
88	29		The supporting operating system for sandboxing must have minimum win 7, Win 8 and Win 10. NGFW should be able to remove executables with content disarm and reconstruction(CDR) capabilities with an integration with Anti-APT device	Specific to OEM hence requesting change. Revised Clause:The supporting operating system for sandboxing must have minimum windows.	As per RFP
89	32		20. Proposed solution must be provided with 4000 or more predefined application signatures (without any customization) from day 1	Changes Require: Proposed solution must be provided with 10000 or more predefined application signatures (without any customization) from day 1. Justification: Pre-Define custom signatures reduces the risk by allowing or blocking the applications based on signature itself which is avoding the dependency of URL filtering and custom application which may open a channel to a threat. Therefore, request to amend the changes as suggested.	As per RFP
90	44		Internal and External NGFW & Anti-APT appliances must be managed from a single centralized dedicated management system separate from the NGFW appliance. The proposed Management must be hardware based appliance.	External NGFW/ Anti-APT appliances must be managed from a centralized dedicated management system or GUI. The proposed Management must be hardware based appliance.	NGFW & Anti-APT appliances must be managed from management system separate from the NGFW appliance. The proposed Management must be hardware based appliance.
91	66		The solution must monitor for suspicious activity in: API calls, File system changes, System registry, Network Connections, System processes, File creation and deletion, File modification, Kernel code injection , Detect Privilege escalation attempts, Kernel modifications (memory changes performed by kernel code, not the fact that a driver is loaded - this is covered by the item above), Kernel code behavior (monitor activity of non user-mode code), Direct physical CPU interaction , UAC(user access control) bypass detection	The solution must monitor for suspicious activity in: API calls, File system changes, System registry, Network Connections, System processes, File creation and deletion, File modification, Kernel code injection , Detect Privilege escalation attempts, Kernel modifications.	The solution must monitor for suspicious activity in: API calls, File system changes, System registry, Network Connections, System processes, File creation and deletion, File modification, Kernel code injection , Detect Privilege escalation attempts, Kernel modifications.

92	67		The solution must provide the ability to be centrally managed and a detailed report must be generated for each one of the malicious files. The detailed report must include: Screen shots, Registry key creation/modifications, Standard security reports , Time lines, Network activity detected	The solution must provide the ability to be centrally managed or GUI and a detailed report must be generated for each one of the malicious files. The detailed report must include: Registry key creation/modifications, Standard security reports , Time lines, Network activity detected	The solution must provide the ability to be centrally managed/ same GUI and a detailed report must be generated for each one of the malicious files. The detailed report must include: Screen shots, Registry key creation/modifications, Standard security reports , Time lines, Network activity detected
93	329		Internal and External Firewall with Anti APT Device, Point No. 37,38,44 & 56-69	As per mentioned functional scope for External & Internal Firewall with Anti - APT component you have asked for a bundled solution having Firewall and partial Anti - APT capability but this is violating NCIIPC, Cert-In, NIST and DSCI cyber security guidelines which recommend to adopting defence in depth layerd security architecture which is very much required to avoid single point of failure considering current threat landscape but RFP functional scope is designed in such a way where NGFW vendors can only participate in both FW & Anti APT segments restricting dediacted Anti APT providers and this is giving them undue commercial advantage at the cost of security effectiveness. Anti - APT is a dedicated technology require dedicated hardware resources to detonate and analyze unknown objects in sandbox environemtn to mitigate zero day attacks. NGFW vendors hosting multiple security layers having partial functionalities using common signatures and common hardware and Firmware platform can work as a single point of failure and not recommended considering Data Center cyber security best practices. Also as per ""Web Application Firewall"" component functional scope you have himself asked for a dedicated WAF solution which should not be hosted on NGFW (RFP clause :""The proposed appliance should be a dedicated appliance with dual power supply, it should not be part of any Firewall or UTM""). Hence it's a humble request to adhere NCIIPC, Cert-In, NIST and DSCI layered security guidelines by removing Anti - APT functional scope from	As per RFP

94	329	Hardware Technical specifications	Internal and External Firewall with Anti APT Device, Point No. 37,38,44 & 56-69	As per mentioned functional scope for External & Internal Firewall with Anti - APT component you have asked for a bundled solution having Firewall and partial Anti - APT capability but this is violating NCIIPC, Cert-In, NIST and DSCI cyber security guidelines which recommend to adopting defence in depth layerd security architecture which is very much required to avoid single point of failure considering current threat landscape but RFP functional scope is designed in such a way where NGFW vendors can only participate in both FW & Anti APT segments restricting dediacted Anti APT providers and this is giving them undue commercial advantage at the cost of security effectiveness. Anti - APT is a dedicated technology require dedicated hardware resources to detonate and analyze unknown objects in sandbox environemtn to mitigate zero day attacks. NGFW vendors hosting multiple security layers having partial functionalities using common signatures and common hardware and Firmware platform can work as a single point of failure and not recommended considering Data Center cyber security best practices. Also as per "Web Application Firewall" component functional scope you have himself asked for a dedicated WAF solution which should not be hosted on NGFW (RFP clause :"The proposed appliance should be a dedicated appliance with dual power supply, it should not be part of any Firewall or UTM"). Hence it's a humble request to adhere NCIIPC, Cert-In, NIST and DSCI layered security guidelines by removing Anti - APT functional scope from internal	As per RFP
95	24/30		3.The appliance hardware should be a multi-core CPU architecture with a hardened 64-bit operating system to support 64 GB RAM from day1.	With the required virtualisation each instance only gets 6Gig's ram which is not enough to run industry grade services like IPS, Malware Detection. Hence requesting change Revised Clause:The appliance hardware should be a multi-core CPU architecture with a hardened 64-bit operating system to support 128 GB RAM from day1.	As per RFP
96	24/30		Proposed Firewall solution must have 16 Physical Core and 32 virtual Core CPU from day 1	The change doesn't do any functional change as the requested change is on virtual core which is highly dependence on the application architecture in some case virtual core is split into 1:4 ratio as well. Hence requesting change Revised Clause:Proposed Firewall solution must have 16 Physical Core from day 1	Not applicable for ASIC architecture

97	24/30		Proposed solution should support at least 16 million concurrent sessions/connections	As the ask is for NGFW hence the performance parameters should include the NGFW performance parameters thus requesting change Revised Clause:Proposed solution should support at least 6 million concurrent layer 7 (enabled with Firewall, AppID as minimum) sessions/connections measured on HTTP/HTTPS traffic	As per RFP
98	24/30		The platform /appliance shall have Next Generation Firewall throughput of at least 22 Gbps with Application Control, FW and IPS with logging enabled in Enterprise Mix / Application Mix traffic on day 1 and scalable upto 30 Gbps to meet future requirements without replacing the existing hardware.	Only a specific vendor allows throughput based scaling for equal participation requesting to include the overall capacity as day 1 requirement. Revised Clause:The platform /appliance shall have Next Generation Firewall throughput of at least 35 Gbps with Application Control, FW and IPS with logging enabled in Enterprise Mix / Application Mix traffic on day 1	As per RFP
99	24/30		The Solution/appliance shall have Threat Prevention throughput of at least 9 Gbps with Application Control, FW, IPS , Anti-malware/Anti Virus, Antibot & URL/web protection/Filtering with logging enabled in Enterprise Mix / Application Mix traffic on day 1 and scalable upto 14 Gbps to meet future requirements without replacing the existing hardware.	Only a specific vendor allows throughput based scaling for equal participation requesting to include the overall capacity as day 1 requirement. Revised Clause:The Solution/appliance shall have Threat Prevention throughput of at least 15 Gbps with Application Control, FW, IPS , Anti-malware/Anti Virus, Antibot & URL/web protection/Filtering with logging enabled in Enterprise Mix / Application Mix traffic on day 1	As per RFP
100	24/31		9. Proposed solution should support at least 300K connections per second. The requested connections per seconds must be available on OEM datasheet or public website independent of operating system/firmware	As the ask is for NGFW hence the performance parameters should include the NGFW performance parameters thus requesting change. Revised Clause:Proposed solution should support at least 240K layer 7 connections per second. The requested connections per seconds must be with firewall, app id enabled and measured on HTTP/HTTPS traffic available on OEM datasheet or public website independent of operating system/firmware	As per RFP
101	25/31		Firewall should have integrated hot-swappable power supplies.	Field replaceability allows a better ROI as in case of RMA the device do not need to be brought down or replaced. Thus ensuring higher uptime, hence requesting change. Revised Clause:Firewall should have field replaceable hot-swappable power supplies.	As per RFP

102	25/31		Firewall should have integrated redundant/hotswappable fan trays/ Modules / fans	Field replaceability allows a better ROI as in case of RMA the device do not need to be brought down or replaced. Thus ensuring higher uptime, hence requesting change. Revised Clause:Firewall should have filed replaceable hot swappable fan trays/ Modules / fans	As per RFP
103	25/31		The requested Performance numbers and details must be available on OEM public Websites/datasheets independent to software/firmware's. Declaration on letter heads are not acceptable	The change doesn't change any functional aspect of the solution. But allows our participation as different vendor have different data sheet structure.Kindly remove this clause	The requested Performance numbers and details must be available on OEM public Websites/datasheets independent to software/firmware's. Declaration on letter heads are acceptable on the requirement which are not mentioned in public datasheet.
104	27/34		Proposed solution/OEM should have recommended rating from NSS Latest report of NGFW / ICSA	Kindly remove this clause as NSS labs are no longer operationsl and testing is no longer available.	Deleted
105	Additional Query		Internal and External NGFW & Anti-APT appliances must be managed from a single centralized dedicated management system separate from the NGFW appliance. The proposed Management must be hardware based appliance.	Since Internal and external firewall would be from different OEM hence management can't be done from single dashboard.Kindly delete this clause from internal, external firewall and APT.	NGFW & Anti-APT appliances must be managed from a single centralized dedicated management system separate from the NGFW appliance. The proposed Management must be hardware based appliance. The solution must be able to store logs of atleast 180 days.
106	Additional Query		Internal/External Firewall	As per industry standard practise internal and external firewall should be from different OEM.	As per RFP
107	Page 24	Specification External Firewall with Anti-APT device -> Specifications	External Firewall with Anti APT	External Firewall and Anti APT Device are 2 separate product categories. It is best practice to have Firewall and Anti APT solution as separate line items in BoQ. Also, this will ensure more wider OEM participation. We would kindly request to separe External Firewall and Anti APT specifications.	As per RFP
108	Page 28	Specification External Firewall with Anti-APT device -> 62	Deployment modes - Inline with NGFW, ICAP, Inline w/o NGFW, API & MTA	MTA deployment is not a part of Anti-APT features. Hence kindly requesting to remove this point	As per RFP
109	Page 28	Specification External Firewall with Anti-APT device -> 59	Following Specifications are must :- Unique files per hour: 1000 Form Factor: 1U Virtual Machines: 8 Storage: 1x960 GB SSD Memory: 64 GB	Since, this is large turnkey project, we would recommend to revise the specification as per the recommended statement given below. These recommendations are similar to other projects of similar scale and size. We would kindly request to amend the clause as per below. Unique files per hour: 2,000+ Form Factor: 2U Virtual Machines: 182+ Storage: (2) 10 TB HDD, RAID 1	As per RFP
110	Page 28	Specification External Firewall with Anti-APT device -> 57	Ports requirement 10x 10/100/1000 RJ45 from day-1	This is hard coded specification favouring to single OEM. Kinldy requesting to remove this point.	As per RFP

111	Page 28	Specification External Firewall with Anti-APT device -> 61	Protocol support - HTTP, HTTPS, SMTP, SMTPS, IMAP, CIFS, SMBv3, SMBv3 multi-channel, FTP.	These protocols support is vendor specific. We would kindly request to remove this clause.	As per RFP
112	Page 28	Specification External Firewall with Anti-APT device -> 56	Solution must be purpose built Anti-APT Appliance should be inline solution (not out-of-line) and integrate with network perimeter security component devices like firewall/UTM.	This statement suggests that, proposed solution should be dedicated anti-APT solution appliance to scan network traffic to bring network anti-APT visibility and protection. Please suggest if our understanding is correct or not.	Yes. Anti APT device is dedicated device and should be inline with NGFW appliance. Bidder shall provide single APT device with external Firewall solution.
113	Page 28	Specification External Firewall with Anti-APT device -> 64	The solution must not require separate appliances for sandboxing of email protection & web. Proposed solution must integrate with existing email & Web solution.	Anti-APT does not require an integration with web and email solutions. Moreover exising clause, is giving undue advantage to single OEM only. Hence, kindly remove this point.	The solution must not require separate appliances for sandboxing of email protection & web.
114			43. Proposed firewall OEM must be in Gartner leaders/challengers for more then last 5 consecutives years	Changes Require: Proposed firewall OEM must be in Gartner leaders for more then last 5 consecutives years. Justification: Gartner inistitute carry out multiple test scans and evaluate vendor on the basis of threat intel, capabilties, performance and market footprint and feedback therefore, NGFW firewall must be consider only from Leader quadrant only. Therefore, request to amend the changes as suggsested.	As per RFP
115	329-340 and 353-355		Internal and External Firewall + Specification-SDWAN Device for Field Devices	We have observed that as per RFP functional scope you have asked for a dedicated NIPS appliance but still as per Internal/External Firewall and SDWAN you have again asked for NIPS functionalities which is duplicating the functionalities and this will going to inflate commercial bid. Please help us in sharing your undersatnding for this feature duplicacy.	As per RFP
116	39		Section – 3: 6 Financial Bid/ Proposal Format and Content Clause No: 16.8 All prices in the Financial Bid shall be quoted in Indian Rupees. The Bidder shall bear the risk related to foreign exchange variations during the Contract Period. The variation in the statutory taxes will be in accordance with the SI Contract.	Query: Any variation in the tax or imposition of new tax by GoI, GoR during the contract period may be considered for variation in the contract price.	As per RFP
117	53		Section – 3: E. Bid Data Sheet 12.3(a) Banks by whom Bank Guarantee is required to be issued: Indian nationalize bank.	Query: We Kindly request to amend this clause as per the below. 12.3(a) Banks by whom Bank Guarantee is required to be issued: Indian nationalize bank/Scheduled commercial bank located in India.	Section – 3: E. Bid Data Sheet 12.3(a) Banks by whom Bank Guarantee is required to be issued: Indian nationalize bank /Scheduled commercial bank located in India.

118	246		Any breach in SLA will attract penalty on the total Monthly Invoicing Value (FMS Cost) subject to a maximum penalty of 20% of the Monthly Invoicing Value, both as a penalty in single service breach or as an aggregate penalty on multiple service breach, beyond which it will result in no payments for that month of service.	Changes Require: Request you to change clause as Any breach in SLA will attract penalty on the total Monthly Invoicing Value (FMS Cost) subject to a maximum penalty of 10% of the Monthly Invoicing Value, both as a penalty in single service breach or as an aggregate penalty on multiple service breach, beyond which it will result in no payments for that month of service.	Any breach in SLA will attract penalty on the total Monthly Invoicing Value (FMS Cost) subject to a maximum penalty of 15% of the Monthly Invoicing Value, both as a penalty in single service breach or as an aggregate penalty on multiple service breach, beyond which it will result in no payments for that month of service.
119	255		SLAs will be as below: SLA Parameters for Response and resolution Time >99 % -N/A <99 and >=97% -2% of Monthly FMS cost <97 and >=95% - 5% of Monthly FMS cost <95 and >=90% -10% of Monthly FMS cost < 90% - 20% of Monthly FMS cost	Change Require: Request you to change penalty parameter as >98 % -N/A <98 and >=95% -2% of Monthly FMS cost <85 and >=90% -8% of Monthly FMS cost < 85% - 10% of Monthly FMS cost	SLAs will be as below: SLA Parameters for Response and resolution Time >99 % -N/A <99 and >=97% -2% of Monthly FMS cost <97 and >=95% - 5% of Monthly FMS cost <95 and >=90% -10% of Monthly FMS cost < 90% - 15% of Monthly FMS cost
120			Remarks: Although SLA penalties shall be calculated as per above table, however total penalty to be deducted is to be capped at 20% of the Monthly Invoicing Value (FMS Cost).	Chnages Require:- Request you to change clause as Remarks: Although SLA penalties shall be calculated as per above table, however total penalty to be deducted is to be capped at 10% of the Monthly Invoicing Value (FMS Cost).	Remarks: Although SLA penalties shall be calculated as per above table, however total penalty to be deducted is to be capped at 15% of the Monthly Invoicing Value (FMS Cost).
121	134		i) Identify & visualize poor performing assets such as feeder/DT on multiple criteria such as energy losses, outage duration etc. through appropriate colour coding depending on severity thresholds.	What are the visualization tools required ?	As per RFP
122	151		Enterprise GIS system must be highly scalable. It must have architecture deployment flexibility such as single machine, multiple machines, cluster-based environment Active-Active, Active-Passive, multiple sites deployment. System must be horizontally and vertically scalable. GIS platform capability should be offered by a single/ seamless integration of software based on same technology.	We understand that the offered GIS server software licenses should be core-independent to avoid costs associated with additional licenses in the event of scalability. Kindly confirm whether our understanding is correct. It is to submit that UPCL may ask for GIS server software licensing that should not depend on the cores of a physical server or hardware. It should be able to take advantage of the multi-core architecture of the server, i.e., core independent licensing. UPCL does not need to procure additional licenses whenever hardware augmentation happens. It saves a huge amount of money in terms of GIS server licensing. Considering the cost advantage, the core independent GIS server licenses may kindly be requested.	Yes, GIS server software licenses should be core-independent
123	151		GIS System software should support VMware vSphere, Microsoft Hyper-V & Huawei Fusion Sphere virtualization environments. GIS System should support Cloud Environments like Amazon Web Services (AWS) or Microsoft Azure. GIS System should be capable of deployment on-premises on physical hardware, in a private cloud using VMware or other virtualization technologies, or in the cloud using an Infrastructure as a Service provider (IaaS) such as e.g. Amazon Web Services, Microsoft Azure, IBM SoftLayer, etc.	The GIS system support may kindly be asked for VMware vSphere / Microsoft Hyper-V / Huawei Fusion Sphere virtualization environments.	GIS System software should support VMware vSphere/Microsoft Hyper-V /Huawei Fusion Sphere virtualization environments. GIS System should support Cloud Environments like Amazon Web Services (AWS) or Microsoft Azure. GIS System should be capable of deployment on-premises on physical hardware, in a private cloud using VMware or other virtualization technologies, or in the cloud using an Infrastructure as a Service provider (IaaS) such as e.g. Amazon Web Services, Microsoft Azure, IBM SoftLayer, etc.

124	153		4) INTEGRATION WITH OTHER MODULES For ensuring high level of interoperability of GIS software with the various business process software, open GIS standards and OGC Compliant/implemented software shall be adhered by the bidder. Software should have a ready provision / facility so that the proposed system can be easily integrated to the following systems:- • Energy Management System • Customer Call Centre • All Commercial Application including Billing and New Service Connection Modules • ERP • SCADA	Hope the department will share all the APIs for integration.	UPCL shall provide the required APIs
125	153		Section 7. Contract Form and Conditions of Contract 5) MIGRATION OF CONSUMER DATABASE & LT NETWORK	Query: - What will be the database size.	30 GB Approx.
126	154		5) MIGRATION OF CONSUMER DATABASE & LT NETWORK The bidder shall require to migrate the LT network (11/0.4 KV DTR to LT Poles/Pillars/ Distribution boxes) and the consumer indexed to the LT network. The survey of the said LT Network and consumer indexing shall be done by a third party on behalf of UPCL. The third party shall provide the data in .shp format, which shall be used by the bidder for migration into its system. Furthermore, UPCL has completed survey , mapping and digitization of 67 nos towns under R APDRP and IPDS schemes. The GIS database thus created and currently in use by the Utility shall also be required to be migrated to the system proposed by the bidder.	a) How much data is there for migration ? B) Will there be data cleansing required ? C) Will there be reverse migration required ?	a) Approx. 30 GB b) Yes c) No
127			Additional Query Asset Management	We understand UPCL requires an Asset Management module with functionality that includes access to GIS-generated maps, completing work requests, entering resources, creating assets, editing assets, including location and attributes, and creating a work request, etc. Can a ready GIS-EAM integrated system be offered under the current scope? Such a ready-integrated GIS and EAM solution will provide asset records, maintenance, structure, and standardization of asset information, capture the identity, configuration, and structure of physical assets, their complete technical and commercial configurations, and current position (either by location, functional position, or tag), as well as prior locations and maintenance histories. Please confirm.	As per Solution proposed by SI

128			Additional Query Outage Management	We understand UPCL requires a GIS-based OMS system. Can an integrated GIS-OMS module be offered under this scope? Such a ready-integrated GIS-based OMS system can facilitate integration with real-time control systems like SCADA and capacitor controls; integration with resource information systems like ERP, GIS, fleet management, AVL/GPS; and integration with IVR, CIS, AMI, work management, etc. Please confirm.	As per Solution proposed by SI
129			General Query	Query: - Kindly Provide Detail Software Scope for the GIS Survey.	As per RFP
130	138		All Annexure Document - Specification- Help Desk Solution (Minimum 25 nos. concurrent users) Sr no -1	Existing Clasue: ITIL v3 Compliant Solution aligned for rapid deployment Query/Suggestion: ITILv4 represents a significant advancement over ITILv3, offering enhanced features and methodologies that better align with the dynamic and evolving landscape of IT service management. The latest version incorporates modern practices, emphasizes a more holistic approach to service delivery, and provides a more flexible framework to adapt to the changing needs of organizations. With its emphasis on collaboration, agility, and continuous improvement, ITILv4 stands as a superior choice for organizations aiming to optimize their IT service management practices in today's rapidly changing business environment. Hence we request authority to ammend clause as mentioned below: " ITIL v4 Certified Solution aligned for rapid deployment with minimum 7 practices"	ITIL v3 or higher Compliant Solution aligned for rapid deployment
131	138		All Annexure Document - Specification- Help Desk Solution (Minimum 25 nos. concurrent users) Sr no -11	Specification- Help Desk Solution (Minimum 25 nos. concurrent users) Sr No:11 Existing Clause: The service desk should be from the Same Product family as the EMS Integration and should be compliant with ITIL standards. It should be integrated feature with The Datastore should to external storage on-demand in encrypted format and maximum compression using gzip, lzmo or xz compression. Query: As here the datastore asked is with compression functionality with gzip, lzmo or xz compression, we request clarity on comression weather customer will do compression on storage side or comression required in application side?	Compression is required on application side.

132		Help Desk Solution (Minimum 25 nos. concurrent users)- >>General Requiremen	To ensure high level of data exchange between different modules of Desktop Management and provide seamless integration between Helpdesk and Desktop Management tools – the Asset Management, Software Delivery and Control modules should essentially share the same database.	Request you to remove this OEM Specific clause as per following: To ensure high level of data exchange between different modules of Desktop Management and provide seamless integration between Helpdesk and Desktop Management tools – the Asset Management, Software Delivery and Control modules should essentially share the same database.	As per RFP
133	85		solution must be able to detect/prevention communications to Global C&C's and Allow administrators to create user defined list of allowed/blocked URL's and should give the flexibility of deploying features either as agent based and agentless for different modules depending on organization's data center environment also should have seamless integration with Anti-APT solution as per RFP specifications bi-directionally to detect and mitigate zero day threats having common threat sharing platform for holistic visibility and control	Remove point	As per RFP
134	413-417	L3 Switch	Should support minimum 11K IPv4 routes or more	Should support minimum 2K IPv4 routes or more	Should support minimum 2K IPv4 routes or more
135	413-417	L3 Switch	Switch should support 128 or more STP Instances.	Switch should support 32 or more STP Instances.	Switch should support 32 or more STP Instances.
136	413-417	L3 Switch	Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment and MACSec-128 on hardware for all ports.	Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment and MACSec or GRE encapsulation	As per RFP
137	413-417	L3 Switch	Switch should support IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard.	Switch should support IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard/IP lockdown.	Switch should support IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard/ IP Lockdown.
138	413-417	L3 Switch	Switch should support network segmentation that overcomes the limitation of VLANs using VXLAN and VRFs.	Switch should support network segmentation that overcomes the limitation of VLANs using VXLAN/ VRFs.	As per RFP
139	L3 Switch/17	L3 Switch/17	Switch should support IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard.	Switch should RFC 2460 Internet Protocol Version 6 (IPv6) Specification, RFC 4861 Neighbor Discovery for IP Version 6 (IPv6), RFC 4862 IPv6 Stateless Address Autoconfiguration, IPv6 DCHP snooping	As per RFP
140	L3 Switch/18	L3 Switch/18	Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment and MACSec- 128 on hardware for all ports.	Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment and MACSec-128 on hardware for all ports.	As per RFP
141	L3 Switch/19	L3 Switch/19	Switch must have the capabilities to enable automatic configuration of switch ports as devices connect to the switch for the device type.	Kindly remove this clause.	Deleted
142	L3 Switch/20	L3 Switch/20	During system boots, the system’s software signatures should be checked for integrity. System should capable to understand that system OS are authentic and unmodified, it should have cryptographically signed images to provide assurance that the firmware & BIOS are authentic.	During system boots or OS upgrades, the system’s software should be checked for integrity.	As per RFP

143	L3 Switch/21	L3 Switch/21	Switch shall have 24 nos. 10/100/1000 Base-T ports 4 nos. SFP+ uplinks ports. 2 nos. uplink SFP should be provided in switch	Switch shall have 24 nos. 10/100/1000 Base-T ports 4 nos. SFP28 uplinks ports. 2 nos. uplink SFP should be provided in switch	As per RFP
144	L3 Switch/24	L3 Switch/24	Switches,Router, Transreceivers,Access Points and Wireless Controller should be from the same OEM.	Switches,Router, Transreceivers,Acc ess Points and Wireless Controller should be from the same OEM.	Deleted
145	L3 Switch/4	L3 Switch/4	Switch should have dedicated slot for modular stacking, in addition to asked uplink ports. Should support for minimum 80 Gbps of stacking thoughput with 8 switch in single stack.	Switch should have dedicated slot for modular stacking/MLAG, in addition to asked uplink ports. Should support for minimum 80 Gbps of stacking thoughput with 5 switch in single stack/MLAG PoD.	Switch should have dedicated slot for modular stacking/MLAG, in addition to asked uplink ports. Should support for minimum 40 Gbps of stacking thoughput with 5 switch in single stack/MLAG.
146	L3 Switch/9	L3 Switch/9	Switch should support atleast 16K flow entries	Switch should support atleast 16K flow entries or should support sflow.	Switch should support atleast 16K sflow/Netflow/Jflow or equivalent entries
147	413-417	L3 Switch with all Fiber Ports	Should have advance Layer 3 protocol like BGPv4, BGPv6 , MPLS, VRF, VXLAN, IS-ISv4, OSPFv3, MP-BGP	Should have advance Layer 3 protocol like BGPv4, BGPv6 , MPLS, VRF, VXLAN/ IS-ISv4/ OSPFv3, MP-BGP	Should have advance Layer 3 protocol like BGPv4, BGPv6 , MPLS, VRF, VXLAN/ IS-ISv4/ OSPFv3, MP-BGP
148	413-417	L3 Switch with all Fiber Ports	Switch shall have 8K or more multicast routes.	Switch shall have 7K or more multicast routes.	Switch shall have 7K or more multicast routes.
149	413-417	L3 Switch with all Fiber Ports	Switch shall have modular OS to support application 3rd party application hosting	Remove tha clause	Deleted
150	413-417	L3 Switch with all Fiber Ports	Switch should have dedicated slot for modular stacking, in addition to asked uplink ports. Should support for minimum 1 Tbps of stacking thoughput with 8 switch in single stack.	Switch should have dedicated slot for modular stacking or uplink ports. Should support for minimum 200Gbps of stacking thoughput.	Switch should have dedicated slot for modular stacking or uplink ports. Should support for minimum 200Gbps of stacking thoughput.
151	413-417	L3 Switch with all Fiber Ports	Switch should support 128 or more STP Instances.	Switch should support 32 or more STP Instances.	Switch should support 32 or more STP Instances.
152	413-417	L3 Switch with all Fiber Ports	Switch should support atleast 64K flow entries	Switch should support atleast 64K flow entries/sflow	Switch should support atleast 64K flow entries/sflow/Netflow/Jfow.
153	L3 Switch with all Fiber Ports/18	L3 Switch with all Fiber Ports/18	Switch should support IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard.	Switch should RFC 2460 Internet Protocol Version 6 (IPv6) Specification, RFC 4861 Neighbor Discovery for IP Version 6 (IPv6), RFC 4862 IPv6 Stateless Address Autoconfiguration, IPv6 DCHP snooping	As per RFP
154	L3 Switch with all Fiber Ports/20	L3 Switch with all Fiber Ports/20	Switch must have the capabilities to enable automatic configuration of switch ports as devices connect to the switch for the device type.	Kindly remove this clause.	Deleted
155	L3 Switch with all Fiber Ports/28	L3 Switch with all Fiber Ports/28	OEM should be listed in Gartner Leader Quadrant for Wired and Wireless LAN Infrastructure from last 3 years before releasing this RFP.	OEM should be listed in Gartner Leader Quadrant for Wired and Wireless LAN Infrastructure from last 3 years before releasing this RFP.	As per RFP
156	44		Hardware Technical specifications Annexure-VI Specification- Load Balancer New Clause Request	The proposed hardware should be stable and reliable to address current requirement for such critical infra, EAL2 certification ensure the same. Major OEM along with some Make In India OEM as well have this certification. There are other components as well in this RFP where EAL certification is asked. Suggested Clause: The proposed hardware/software should be EAL2 certified.	As per RFP

157	348 of 479		Specification- Load Balancer 5. Traffic Ports support: 4 x 10 GE SFP+, 4 x 1GE SFP and 4 x 1G Copper from day-1 Device L4 Throughput: 20 Gbps and scalable upto 40 Gbps Layer 4 connections per second: 500,000 Layer 7 requests per second: 900,000 RSA CPS(2K Key): 20,000 ECC CPS (EC-P256): 12,000 with TLS1.3 Support Processor: Intel 12-core CPU Concurrent Connections: 40 Million The appliance should have dedicated 2 x 10/100/1000 Copper Ethernet Out-of-band Management Port and RJ45 Console Port * Data should be publically available	Please change the port count as SFP+ can support both 1gig or 10gig fiber. Please change the concurrent connecttion as it will limit other reputed OEM's to participate. Please change to 1 x 10/100/1000 Copper Ethernet Out-of-band Management Port as its specific to one OEM. Kindly modify clause as" 5. Traffic Ports support: 4 x 10 GE SFP+ and 4 x 1G Copper from day-1 Device L4 Throughput: 20 Gbps and scalable upto 40 Gbps Layer 4 connections per second: 500,000 Layer 7 requests per second: 900,000 RSA CPS(2K Key): 20,000 ECC CPS (EC-P256): 12,000 with TLS1.3 Support Processor: Intel 12-core CPU Concurrent Connections: 38 Million The appliance should have dedicated 1 x 10/100/1000 Copper Ethernet Out-of-band Management Port and RJ45 Console Port * Data should be publically available"	As per RFP
158	348 of 479		Specification- Load Balancer 9. "The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. It should NOT use Open Source/3rd party Network Functions. The proposed appliance should have capability to run in Virtualized as well as Standalone mode (Bidder may be asked to demonstrate this feature during Technical Evaluation). Each Virtual Instance contains a complete and separated environment of the Following: a) Resources, b) Configurations, c) Management, d) Operating System The proposed device should support 5 Virtual Instance from Day 1 and scalable upto 10 Virtual Instances. "	Please change virtual instance from 5 to 2 as it's a small appliance which can support up to 4 virtual stance from day one. Kindly modify clause as" 9. "The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. It should NOT use Open Source/3rd party Network Functions. The proposed appliance should have capability to run in Virtualized as well as Standalone mode (Bidder may be asked to demonstrate this feature during Technical Evaluation). Each Virtual Instance contains a complete and separated environment of the Following: a) Resources, b) Configurations, c) Management, d) Operating System The proposed device should support 2 Virtual Instance from Day 1 and scalable upto 4 Virtual Instances."	As per RFP

159	Page 44	Suggestive clause	Page 44 / Specification- Load Balancer / point no 10	Behavior analysis and SYN Flood Protection for TCP SYN floods, as well as network behavior analysis, should be included. We recommend adding the following clause to LLB. Additional Clause The proposed solution should include built-in DDoS connection protection with LLB, TCP SYN flood protection using (Malformed IP Header, Incomplete , 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), as well as network behavior analysis for anomaly detection and packet scoring technology. - Denial of Service (DoS) - Distributed Denial of Service (DDoS) - Reflection/amplification attacks - Ping of Death - TCP/UDP/ICMP/IGMP/NTP/DNS/SIP/SNMP Flood - TCP SYN Flood - TCP ACK flood - TCP-Out-of-Order - DNS based attacks - Slow application layer attacks - HTTP/HTTPS Flood - SSL renegotiation attack	As per RFP
160		Load Balancer/ Point 11	DNSSEC based Global Load Balancing should be supported in the proposed device from Day 1	DNS (GSLB) is the important Functionality of ADC, GSLB must be capable of handling complete Full DNS bind records including A, MX, AAAA, CNAME, PTR, and SOA. It suggested to amend the clause as "The solution should support advance functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSEC, DNS DDOS, application load balancing from day one. It should be capable of handling complete Full DNS bind records including A,MX, AAAA, CNAME, PTR, SOA etc"	As per RFP
161		Load Balancer/ Point 12	The solution should support IPv6 as well as IPv4 and have the ability to turn IPv4 traffic to IPv6 traffic on the backend	The IPv6 Ready Logo will indicate that a product has successfully satisfied strong requirements stated by the IPv6 Logo Committee. The IPv6 Ready Core Logo expands the "core IPv6 protocols" test coverage to approximately 450 tests and adds new extended test categories. It is suggested to amend the clause as "The solution should support IPv6 as well as IPv4 and have the ability to turn IPv4/IPv6 traffic to IPv6/IPv4 traffic on the backend and the solution should be IPv6 ready logo certified from the day 1 and OEM should be listed vendor for ipv6 phase-2 certification".	As per RFP

162		Load Balancer/ Point 5	Traffic Ports support: 4 x 10 GE SFP+, 4 x 1GE SFP and 4 x 1G Copper from day-1 Device L4 Throughput: 20 Gbps and scalable up to 40 Gbps Layer 4 connections per second: 500,000 Layer 7 requests per second: 9,00,000 RSA CPS(2K Key): 20,000 ECC CPS (EC-P256): 12,000 with TLS1.3 Support Processor: Intel 12-core CPU Concurrent Connections: 40 Million The appliance should have dedicated 2 x 10/100/1000 Copper Ethernet Out-of- band Management Port and RJ45 Console Port * Data should be publically available	Traffic Ports support: As per the present datacentre/It infra requirement standard, 10G ports are recommended over 1G, As 10G is backward-compatible with 1G where as vies-versa is not possible. And for load balancer deployment 8 x 10G is more than sufficient because asked throughput is 40G.please amend this clause. Layer 4 connections per second: Considering the asked Concurrent Connections and Layer 4 connections per second requirement is lower side. please amend this clause. Layer 7 requests per second: Considering the asked Concurrent Connections and Layer 7 requests per second requirement is lower side. please amend this clause. RSA CPS(2K Key) and ECC CPS (EC-P256) : SSL parameters are very low and not as per industry standard, as now days 100 % internet traffic is SSL based. please amend this clause. Processor : Request to please amend this clause because asked CPU capacity as this is specific to an OEM. Every vendor customise its own hardware for running multiple VMs. Addition Point :- In the appliance will be running multiple functions,we recommended to add of 4	As per RFP
163	343-347	Leaf switch	Switch should re-converge all dynamic routing protocols at the time of routing update changes i.e. Graceful restart for fast re-convergence of routing protocols like OSPF, IS-IS, BGP.	Switch should re-converge all dynamic routing protocols at the time of routing update changes i.e. Graceful restart for fast re-convergence of routing protocols like OSPF, BGP.	Switch should re-converge all dynamic routing protocols at the time of routing update changes i.e. Graceful restart for fast re-convergence of routing protocols like OSPF, BGP.
164	343-347	Leaf switch	Switch should support IP Source Guard	Switch should support IP Source Guard/IP lockdown	Switch should support IP Source Guard/IP lockdown
165	343-347	Leaf switch	Switch should support minimum 500 VRF instances with route leaking functionality	Switch should support minimum 250 VRF instances with route leaking functionality	As per RFP
166	343-347	Leaf switch	Switch should support minimum 64 ECMP paths	Switch should support minimum 32 ECMP paths	As per RFP
167	343-347	Leaf switch	Switch should support VRF, VRF Edge, Virtual Router to achieve multi	Switch should support VRF/VRF Edge/ Virtual Router to achieve multi	Switch should support VRF/VRF Edge/ Virtual Router to achieve multi instance routing
168	343-347	Leaf switch	The proposed solution and switches should be part of Gartner Leader Quadrant for DC Networking for last 3 years	Request you to remove the clause	As per RFP
169	343-347	Leaf switch	The switch should have MAC Address table size of min 200k	The switch should have MAC Address table size of min 90k	As per RFP
170	343-347	Leaf switch	The switch should support BGP EVPN Route Type 2, Type 4 and Route Type 5 for the overlay control plane	The switch should support BGP EVPN Route Type 2, Type 3/4 and Route Type 5 for the overlay control plane	The switch should support BGP EVPN Route Type 2, Type 3/4 and Route Type 5 for the overlay control plane
171	343-347	Leaf switch	The switch should support min 400k IPv4 LPM routes	The switch should support minimum 130K IPv4 Longest Prefix Match routes	As per RFP
172	343-347	Leaf switch	The switch should support minimum 80K multicast routes	The switch should support minimum 4K multicast routes	The switch should support minimum 40K multicast routes
173	Leaf Switch/13	Leaf Switch/13	Switch should support dedicated process for each routing protocol	Switch should support dedicated process for each routing different protocol	Switch should support dedicated process for each routing different protocol
174	Leaf Switch/16	Leaf Switch/16	The switch should support min 400k IPv4 LPM routes	The switch should support min 350k IPv4 LPM routes	As per RFP

175	Leaf Switch/27	Leaf Switch/27	Switch must provide the capability to be integrated with different Hypervisor Managers viz. Vmware vCenter, Microsoft Hyper-V with System Center, Kubernetes, Redhat Openshift and manage virtualise networking from the single pane of glass	Switch fabric must integrate with different virtual machine environment for centralised provisioning/mana gement.	Switch must provide the capability to be integrated with different Hypervisor Managers viz. Vmware vCenter/ Microsoft Hyper-V with System Center/ Kubernetes/ Redhat Openshift/ manage virtualise networking from the single pane of glass.
176	Leaf Switch/42	Leaf Switch/42	Switch should support segment routing and VRF route leaking functionality from day 1	Switch should support segment routing and VRF route leaking functionality from day 2	Switch should support VRF route leaking functionality from day 1
177	Leaf Switch/55	Leaf Switch/55	Switch must provide the capability of micro- segmentation rules and policies for the Virtualized and Non - Virtualized environment (Bare metal and Container) workloads connected to DC fabric for east-west traffic. It must also support micro-segmentation based on VM attributes like hostname, OS, VM Tags, FQDN, Microsoft AD based classification	Fabric must support Segmentation for the Virtualize and Non - Virtualize environment via integration to orchestration layer	As per RFP
178	Leaf Switch/56	Leaf Switch/56	Switch platform should support encryption of traffic i.e. MAC Sec Encryption (802.1AE) in hardware	Please remove	As per RFP
179	Leaf Switch/61	Leaf Switch/61	Switch should support Dynamic ARP Inspection	Switch should support Dynamic ARP Inspection or equivalent feature	Switch should support Dynamic ARP Inspection or equivalent feature
180	Leaf Switch/81	Leaf Switch/81	•Per Flow Hop by Hop packet drop with reason of drop	Per Flow Hop by Hop packet drop with reason of drop	Per Flow Hop by Hop packet drop
181	54		5.Security Features Vendor must have an integrated Anti-Bot and Anti-Virus application on the next generation firewall	Antivirus is a end host software - request to consider Antivirus or Anti malware Revised Clause:Vendor must have an integrated Anti-Bot and Anti-Virus/Anti malware application on the next generation firewall	Vendor must have an integrated Anti-Bot and Anti-Virus/Anti malware application on the next generation firewall
182	86		Should introduce latency <40 microseconds and information should be publically available and documented also should have inbuilt SSL decryption capability.	Latency on appliance varies dynamically because of factors like load on appliance, memory consumption, policy, level of inspection. Hence it can never be same thus requesting change. Revised Clause:Should introduce ultra low latency and also should have inbuilt SSL decryption capability.	As per RFP
183	89		Proposed solution should get integrate natively with Anti APT solution as per RFP specifiations having common threat sharing platform as per RFP specifications to share threat intelligence to mitigate zero day attacks and proposed OEM should be contributing at least 30 zero-day/Undisclosed vulnerabilities to Microsoft continuously from past 5 years and data should be publicly available	Only specific vendor publishes this data, hence requesting change Revised Clause:Proposed solution should get integrate natively with Anti APT solution as per RFP specifications having common threat sharing platform as per RFP specifications to share threat intelligence to mitigate zero day attacks.	Proposed solution should get integrate natively with Anti APT solution as per RFP specifiations having common threat sharing platform as per RFP specifications to share threat intelligence to mitigate zero day attacks and proposed OEM should be contributing zero-day/Undisclosed vulnerabilities to common sharing platform continuously from past 5 years and data should be publicly available

184	89		The management server must support the archiving and backup of events and export to NFS, SMB, SCP and sFTP and must allow the report to be exported into other format such as PDF, HTML, CSV, XML and should be able to manage locally independently without any centralized management server also should serve as a central point for security policies management including versioning, rollback, import and export (backup) tasks supporting 'threat insights' dashboard that show correlated data such as how many breached host, how many IOC data, 3rd party VA scan integration data and how many pre-disclosed vulnerability discovered	Only specific OEM does this hence requesting change to allow more OEM participation. Revised Clause:The management server must support the archiving and backup of events and export to NFS, SMB, SCP and sFTP and must allow the report to be exported into other format such as PDF, HTML, CSV, XML and should be managed centralized management server also should serve as a central point for security policies management including versioning, rollback, import and export (backup) tasks supporting 'threat insights' dashboard that show correlated data such as how many breached host, how many IOC data, 3rd party VA scan integration data and how many pre-disclosed vulnerability discovered	The management server must support the archiving and backup of events and export to NFS, SMB, SCP and sFTP and must allow the report to be exported into other format such as PDF, HTML, CSV, XML and should be able to manage locally independently / centralized management server also should serve as a central point for security policies management including versioning, rollback, import and export (backup) tasks supporting 'threat insights' dashboard that show correlated data such as how many breached host, how many IOC data, 3rd party VA scan integration data and how many pre-disclosed vulnerability discovered
185	90		The Proposed OEM should be leader in advance Global Vulnerability Research and Discovery market share as per Frost & Sullivan Reports and should be in Leaders Quadrant of Gartner Magic Quadrant report for Intrusion Prevention Systems in each of the latest last two reports having at least security effectiveness rate 99 % as per 2017/2018 NSS Labs NGIPS report.	Only specific vendor publishes this data, hence requesting change. Revised Clause:The proposed solution should be a dedicated solution and not a subset of firewall, router, vulnerability management, ddos, waf, etc.	The Proposed OEM should be leader in advance Global Vulnerability Research and Discovery market share as per Frost & Sullivan Reports and should be in Leaders Quadrant of Gartner Magic Quadrant report for Intrusion Prevention Systems in each of the latest last two reports having at least security effectiveness rate of 99 % .
186	Page 86	Specification-NIPS -> 1	Solution should have 10 Gbps of real world throughput with scalability up to 40 Gbps on same appliance supporting scalable architecture delivering 80 million legitimate concurrent Sessions/Concurrent connections scalable up to 120 million and 400,000 new Connections per second from day one which should scalable up to 650000 new Connections per second.	The said statement is favouring specific OEM and will give dis-advantage to other strong technology vendors to participate in the RFP. Requesting to nuetralize the statement. Recommended Statement- Solution should have 10 Gbps of real world throughput with scalability up to 40 Gbps on same appliance supporting scalable architecture delivering 10 million legitimate concurrent Sessions/Concurrent connections scalable up to 60 million and 4,00000 new Connections per second from day one which should scalable up to 2,000000 new Connections per second.	As per RFP
187	Page 86	Specification-NIPS -> 1	Solution should have 10 Gbps of real world throughput with scalability up to 40 Gbps on same appliance supporting scalable architecture delivering 80 million legitimate concurrent Sessions/Concurrent connections scalable up to 120 million and 400,000 new Connections per second from day one which should scalable up to 650000 new Connections per second.	The said statement is favouring specific OEM and will give dis-advantage to other strong technology vendors to participate in the RFP. Requesting to nuetralize the statement. Recommended Statement- Solution should have 10 Gbps of real world throughput with scalability up to 40 Gbps on same appliance supporting scalable architecture delivering 10 million legitimate concurrent Sessions/Concurrent connections scalable up to 60 million and 4,00000 new Connections per second from day one which should scalable up to 2,000000 new Connections per second.	As per RFP

188	Page 87	Specification-NIPS -> 18	Proposed solution should have customized sandbox capability including Domain Check, Software Check, User Settings check, Requisite file check Office version check, Windows License check Browser Check (Sandbox Customized with OS and Applications in the Environment) supporting operating systems (Windows XP, Win7, Win8/8.1, Win 10, Windows Server 2003,2008, 2012, 2016, 2019 and Linux platforms having >99% breach detection rate and Security Effectiveness as per NSS BDS report.	Requesting to consider the suggestion and make the changes to exisitng technical statement for maximum participation in the RFP. Suggested Statement- Proposed solution should have customized/in-built sandbox capability including Domain Check, Software Check, User Settings check, Requisite file check Office version check, Windows License check Browser Check (Sandbox Customized with OS and Applications in the Environment) supporting operating systems (Windows XP, Win7, Win8/8.1/ Win 10, Windows Server 2003/2008/ 2012/ 2016, 2019, Linux & Mac platforms.	As per RFP
189	2		Also one of the project out of the above must be implemented in India and shall have a minimum consumer base of 7 lakhs	Also one of the project out of the above must be implemented in India /globally and shall have a minimum consumer base of 7 lakhs or Also one of the project out of the above must be implemented in India and shall have a minimum consumer base of 2 lakhs	As per RFP
190	7		Bidder shall have a Minimum Annual Average Turnover of 120 crores from IT/software business in India for the last three audited financial years	Bidder or the Consortium partners (combinedly) shall have a Minimum Annual Average Turnover of 120 crores from IT/software business in India for the last three audited financial years	As per RFP
191	16		2. Qualification Requirements 2.1.1 Sole/ Lead Bidder should have successfully implemented Eligible Projects in any Indian/Global Utility (power/ water/ natural gas/ telecom/ banking) during the last 10 (ten) financial years: (i) With an aggregate project value not less than Rs 120 Crores (ii) With project value of one such Eligible Project not less than Rs 85 Crores (OR) Two such Eligible Projects with each having a project value not less than Rs 68 Crores Note: For calculation of project value of eligible projects, only project value of the portion of the project executed by the Sole/ Lead Bidder shall be considered.		As per RFP

192	17		2. Qualification Requirements 2.1 (4) sole/Lead Bidder /Should have experience of implementation of 1 number Enterprise level data centre (On-Premise) along with 1 number of DR Centre (On-Premise) in any Central of Sate Government/Central of state Government/Central of state Public Sector Undertaking/Utility (Power/Water/Natural/gas/Telecom/Banking), in India covering networking equipments' application servers, database servers, Storage system, firewall and backup system such as tape library etc. during the last 10 (ten) financial years which have completed at least 1 (one) year of operational period. In case, bidder have implemented the DC and Dr before 10 financial years and same bidder is presently managing its operations , the same shall also be considered.The Data Centre and DR Centre should have minimum 50 nos. physical server or server with minimum 100 physical CPU and 70 TB (raw) Storage at each location	The current criterion might discourage the participation of high-quality bidders. To encourage a wide range of high quality bidders, we request your esteemed consideration in revising the criteria provided below.Sole/ Lead Bidders should have experience of implementation of 1 number enterprise level Data Centre (On-Premise/cloud) along with 1 number of DR Centre (on-Premise/ Cloud) in any central or State Government/Central or State Public Sector Undertaking/utility (Power)/water/Natural Gas/Telecom/Banking), In India/Global covering networking equipment's applications severs, database servers, storage system, firewall and backup system such as tape library etc. during the last 10 (ten) financial years which have completed at least 1 (one) year of operational period . In case, bidder have implemented the DC and DR before 10 financial years and same bidders is Presently managing its operations, the same shall also be considered. The Data Centre and DR Centre should have minimum 25 nos. physical sever of server with minimum 50 physical CPU and 35 TB (raw) storage at each location We trust that UPCL will make a prudent decision in addressing this matter by revising this clause	2. Qualification Requirements 2.1 (4) sole/Lead Bidder /Should have experience of implementation of 1 number Enterprise level data centre (On-Premise) along with 1 number of DR Centre (On-Premise) in any Central of Sate Government/Central of state Government/Central of state Public Sector Undertaking/Utility (Power/Water/Natural/gas/Telecom/Banking), in India /Global covering networking equipments' application servers, database servers, Storage system, firewall and backup system such as tape library etc. during the last 10 (ten) financial years which have completed at least 1 (one) year of operational period. In case, bidder have implemented the DC and Dr before 10 financial years and same bidder is presently managing its operations , the same shall also be considered.The Data Centre and DR Centre should have minimum 25 nos. physical server or server with minimum 50 physical CPU and 35 TB (raw) Storage at each location
194	20		B1. Geographical Information System Technical Requirement	1. Regarding the Memorandum and Articles of Association, are there any specific clauses or information that should be highlighted? 2. How recent should the legal documentation confirming acquisition/merger be?	As per RFP
195	20		Section – 2: Eligibility and Qualification requirements B. Geographical Information System Technical Requirement B2. The Lead bidder or the GIS Partner should have executed atleast one GIS projects (software development & customization & mapping and digitization of assets and consumers for an aggregate consumer base for atleast 5 Lakhs Consumers) in Central or State Government/ Central or State Public Sector Undertaking/Indian Utility services like Power/Gas/Telecom/Water in last ten (10) financial years. The bidder should have worked with atleast one Utility Power/Gas/Telecom/Water sector) in implementing DGPS Field Survey, digitization and mapping of asset network , consumers including GIS software development / customisation using any licensed enterprise GIS Platform. The total worth of projects should be at least INR 10 Crores.	<u>Query:</u> We Kindly request to amend this clause as per the below. B. Geographical Information System Technical Requirement B2. The Lead bidder or the GIS Partner should have executed atleast one GIS projects (software development & customization & mapping and digitization of assets and consumers for an aggregate consumer base for atleast 5 Lakhs Consumers) in Central or State Government/ Central or State Public Sector Undertaking/Indian Utility services like Power/Gas/Telecom/Water in last ten (10) financial years. The bidder should have worked with atleast one Utility Power/Gas/Telecom/Water sector) in implementing DGPS Field Survey/GIS Tagging, digitization and mapping of asset network, consumers including GIS software development / customisation using any licensed enterprise GIS Platform. The total worth of projects should be at least INR 10 Crores.	The Lead bidder or the GIS Partner should have executed atleast one GIS projects (software development & customization & mapping and digitization of assets and consumers for an aggregate consumer base for atleast 5 Lakhs Consumers) in Central or State Government/ Central or State Public Sector Undertaking/Indian Utility services like Power/Gas/Telecom/Water in last ten (10) financial years. The bidder should have worked with atleast one Utility Power/Gas/Telecom/Water sector) in implementing DGPS / GPS /Drone Field Survey, digitization and mapping of asset network , consumers including GIS software development / customisation using any licensed enterprise GIS Platform. The total worth of projects should be at least INR 10 Crores.

196	20		Section – 2: Eligibility and Qualification requirements B. Geographical Information System Technical Requirement Clause as per RFP. B1. The Lead bidder or the GIS Partner must be established, reliable and reputed organization in the field of DGPS Survey and GIS Mapping & Indexing including GIS software development and customization in Central or State Government/ Central or State Public Sector Undertaking/Indian Utility services like Power/Gas/Telecom/Water in last ten (10) financial years.	Query: We Kindly request to amend this clause as per the below. B. Geographical Information System Technical Requirement Clause as per RFP. B1. The Lead bidder or the GIS Partner must be established, reliable and reputed organization in the field of DGPS Survey/GIS Tagging and GIS Mapping & Indexing including GIS software development and customization in Central or State Government/ Central or State Public Sector Undertaking/Indian Utility services like Power/Gas/Telecom/Water in last ten (10) financial years.	The Lead bidder or the GIS Partner must be established, reliable and reputed organization in the field of DGPS / GPS / Drone Survey and GIS Mapping & Indexing including GIS software development and customization in Central or State Government/ Central or State Public Sector Undertaking/Indian Utility services like Power/Gas/Telecom/Water in last ten(10) financial years.
197	21		Section – 2.3: Eligibility and Qualification Requirements	1. Regarding the completion of projects worth at least INR 10 Crores, is this a cumulative requirement, or can it be achieved through individual projects? 2. What documentation is acceptable as proof of Go-live status for a project, and is there a specific definition of Go-Live/UAT provided? 3. Can the bidder provide a combination of different proofs for project completion, or is a specific type of documentation preferred?	1. Its individual project worth. 2. Client certificate accepted. 3. Client confirmations for complete go-live or milestone achievement.
198	57		Section – 3: Annexure-II Technical Evaluation Criteria: 4. Sole/ Lead Bidder should have experience of implementation of 1 number Enterprise level Data Center (On-Premise) along with 1 number of DR Center (On-premise) in any Central or State Government/ Central or State Public Sector Undertaking/ Utility (Power/Water/Natural Gas/Telecom/Banking), in India covering networking equipment's, application servers, database servers, storage system, firewall and backup system such as tape library etc. during the last 10(ten) financial years which have completed at least 1 (one) year of operational period. In case, bidder have implemented the DC and DR before 10 financial years and same bidder is presently managing its operations, the same shall also be considered. The Data Center and DR Center should have minimum 50 nos. physical server or server with minimum 100 physical CPU and 70 TB (raw) storage at each location. Marks to be allotted for the above projects shall be as below: DC & DR (On-premise) Implementation (15 Marks) • For Implementation of 1 No DC & DR (Onpremise) – 9 marks • For every additional DC / DR (On- premise) Implementation – 3 mark each subject to a maximum of 6 marks	Query: We Kindly request to amend this clause as per the below. 4. Sole Bidder/ Any Consortium Member/Proposed OEM should have experience of implementation of 1 number Enterprise level Data Center (On-Premise) along with 1 number of DR Center (On- premise) in any Central or State Government/ Central or State Public Sector Undertaking/ Utility (Power/Water/Natural Gas/Telecom/Banking), in India covering networking equipment's, application servers, database servers, storage system, firewall and backup system such as tape library etc. during the last 10(ten) financial years which have completed at least 1 (one) year of operational period. In case, bidder have implemented the DC and DR before 10 financial years and same bidder is presently managing its operations, the same shall also be considered. The Data Center and DR Center should have minimum 50 nos. physical server or server with minimum 100 physical CPU and 70 TB (raw) storage at each location. Marks to be allotted for the above projects shall be as below: DC & DR (On-premises) Implementation (15 Marks) • For Implementation of 1 No DC & DR (Onpremise) – 9 marks • For every additional DC / DR (On-premises) Implementation – 3 mark each subject to a maximum of 6 marks.	Sole/ Lead Bidder should have experience of implementation of 1 number Enterprise level Data Center (On-Premise) along with 1 number of DR Center (On-premise) in any Central or State Government/ Central or State Public Sector Undertaking/ Utility (Power/Water/Natural Gas/Telecom/Banking), in India / Global covering networking equipment's, application servers, database servers, storage system, firewall and backup system such as tape library etc. during the last 10 (ten) financial years which have completed at least 1 (one) year of operational period. In case, bidder have implemented the DC and DR before 10 financial years and same bidder is presently managing its operations , the same shall also be considered. The Data Center and DR Center should have minimum 25 nos. physical server or server with minimum 50 physical CPU and 35 TB (raw) storage at each location. Marks to be allotted for the above projects shall be as below: DC & DR (On-premise) Implementation (15 Marks) •For Implementation of 1 No DC & DR (On-premise) – 9 marks •For every additional DC / DR (On-premise) Implementation – 3 mark each subject to a maximum of 6 marks

199	16 – 17		2. Qualification Requirements 2.1.2 Sole/ Lead Bidder must have successfully implemented billing systems in any Indian/ Global Utility (power/ water/ natural gas/ telecom) during the last 10 (ten) financial years for an aggregate consumer base of at least 17 Lakhs consumers. Also, one of the projects out of the above, must be implemented in India and shall have a minimum consumer base of 7 Lakhs. Each of the projects shall be in operation for at least 1 (one) year as on date of bid submission OR Each of the projects should have completed at least 3 (three) years of operational period. The implementation should have covered at least 5 (five) modules (Modules i to iv are mandatory) out of the below mentioned list: i. Metering, Billing & Collection (MBC) ii. Disconnection & Reconnection iii. Management Information System & Dashboarding v. Energy Accounting & Audit vi. Web Portal and Mobile Applications vii. Workforce Management viii. Prepaid Module ix. Identity Access Management x. Document Management System xi. Accounting, Ledger, & Banking Reconciliation Statement (BRS) Process		As per RFP
200	20,21		B2. GIS Project Execution Requirement	1. What is the expected duration for the execution of a GIS project, from initiation to completion? 2. Can the Lead Bidder or GIS Partner propose a project that involves GIS software development and customization without DGPS Field Survey, digitization, and mapping of asset networks? 3. What is the minimum required value for the references (contract/PO/WO) to be considered relevant for the GIS project execution requirement?	As per RFP
201		18	2. Qualification Requirements 2.1.5 Sole/ Lead Bidder should have the following certificates which should be valid as on the date of bid submission: (a) ISO 9001:2015 (b) ISO/IEC 27001:2013/2017 or latest. (c) CMMi Level 5		As per RFP
202		18	2. Qualification Requirements 2.1.7 Bidder shall have a Minimum Average Annual Turnover (MAAT) of Rs 120 Crores from IT/ Software business in India for the last 3 (three) audited financial years.		As per RFP

203			a. MAAT requirement should be made independent from technical requirements: Such financial capability should be made independent from technical requirements such as specific from IT/software business. Large developers like us have mulϴple streams of revenue which are difficult to be isolated. Hence, such specific requirement should be deleted.		As per RFP
204			b. Appropriate payment security mechanism (PSM) shall ensure efficient price discovery: Payment security provides a better surety towards payment to the Bidders, ensuring competitive rates. Realizing this, REC in its letter dt. 9th November 2023, REC has advised the utilities to specify in their RFP, a requisite Payment Security Mechanism in the form of Escrow, Letter of Credit, etc. In line with the REC Letter (attached as Annexure B), we kindly request the utility to establish a requisite Payment Security Mechanism.		As per RFP
205			c. Failure of Utility to establish Escrow Facility/ Letter of Credit through online Consumer payments or pay the Monthly amount dues to be included under Utility Event of Default: Termination by either party on other party's event of default should be mandated for balancing of contractual risks & rewards. Similar provision has been provided in AMISP SBD notified by Ministry of Power. This will also ensure reduction of financial risks and hence lowering of quoted rate.		As per RFP
206			Section – 1: Request for Proposal Notice Amounts for Bidding B. Bid Security (Refundable)	Clause as per RFP Earnest Money Deposit/Bid Security Rs. 3.5 Crore Query Tender Estimated Cost is 173.25 Crore Please reduce the Bid Security Amount to 1% of the Estimated Tender value i.e., for INR. 1.73 Crore. This will enable more bidders to participate. thereby allowing the DISCOM to create more competition. Also request you to consider relaxation for MSME.	As per RFP

207	57		4. Sole/ Lead Bidder should have experience of implementation of 1 number Enterprise level Data Center (On-Premise) along with 1 number of DR Center (On-Premise) in any Central or State Government/ Central or State Public Sector Undertaking/ Utility (Power/Water/Natural Gas/Telecom/Banking), in India covering networking equipment's, application servers, database servers, storage system, firewall and backup system such as tape library etc. during the last 10 (ten) financial years which have completed at least 1 (one) year of operational period. In case, bidder have implemented the DC and DR before 10 financial years and same bidder is presently managing its operations , the same shall also be considered. The Data Center and DR Center should have minimum 50 nos. physical server or server with minimum 100 physical CPU and 70 TB (raw) storage at each location. Marks to be allotted for the above projects shall be as below: DC & DR (On-premise) Implementation (15 Marks) •For Implementation of 1 No DC & DR (On-premise) – 9 marks •For every additional DC / DR (On-premise) Implementation – 3 mark each subject to a maximum of 6 marks	Sole/ Lead Bidder should have experience of implementation of 1 number Enterprise level Data Center (On-Premise /Cloud) along with 1 number of DR Center (On-premise /Cloud)) in any Central or State Government/ Central or State Public Sector Undertaking/ Utility (Power/Water/Natural Gas/Telecom/Banking), in India / Global covering networking equipment's, application servers, database servers, storage system, firewall and backup system such as tape library etc. during the last 10 (ten) financial years which have completed at least 1 (one) year of operational period. In case, bidder have implemented the DC and DR before 10 financial years and same bidder is presently managing its operations , the same shall also be considered. The Data Center and DR Center should have minimum 25 nos. physical server or server with minimum 50 physical CPU and 35 TB (raw) storage at each location. Marks to be allotted for the above projects shall be as below: DC & DR (On-premise/Cloud) Implementation (15 Marks) •For Implementation of 1 No DC & DR (On-premise/Cloud) – 9 marks •For every additional DC / DR (On-premise/Cloud) Implementation – 3 mark each subject to a maximum of 6 marks	Sole/ Lead Bidder should have experience of implementation of 1 number Enterprise level Data Center (On-Premise) along with 1 number of DR Center (On-premise) in any Central or State Government/ Central or State Public Sector Undertaking/ Utility (Power/Water/Natural Gas/Telecom/Banking), in India / Global covering networking equipment's, application servers, database servers, storage system, firewall and backup system such as tape library etc. during the last 10 (ten) financial years which have completed at least 1 (one) year of operational period. In case, bidder have implemented the DC and DR before 10 financial years and same bidder is presently managing its operations , the same shall also be considered. The Data Center and DR Center should have minimum 25 nos. physical server or server with minimum 50 physical CPU and 35 TB (raw) storage at each location. Marks to be allotted for the above projects shall be as below: DC & DR (On-premise) Implementation (15 Marks) •For Implementation of 1 No DC & DR (On-premise) – 9 marks •For every additional DC / DR (On-premise) Implementation – 3 mark each subject to a maximum of 6 marks
208	123		Should be configured with minimum 1280 GB DRAM based cache and should be scalable up to 6 TB DRAM or higher with or without having to add controllers.	Requesting the technical committee to kindly amend and seek at least 2048GB of DRAM Cache to safeguard future investment and to provide better storage IO. Hence requesting you to kindly change the same to : Should be configured with minimum 2048GB DRAM based cache and should be scalable up to 6 TB DRAM or higher with or without having to add controllers.	Should be configured with minimum 1024 GB DRAM based cache and should be scalable up to 4 TB DRAM or higher with or without having to add controllers.
209	123		The proposed architecture should be supplied minimum two controllers, and should be scalable up to 8 controllers non- disruptively. Offered storage must have minimum 2 x 100Gbps or higher speed interconnect ports per controller	Dear Technical Committee, Requesting you to kindly remove 100GB Ports from the Existing Clause as the ports are OEM Specific and Most of the Gartner Leaders for Primary Storage does not have the subjected Ports hence kindly change the same to : The proposed architecture should be supplied minimum two controllers, and should be scalable up to 8 controllers non-disruptively.	The proposed architecture should be supplied minimum two controllers, and should be scalable up to 4 controllers non- disruptively with minimum offered controller interconnect bandwidth of 200 Gbps or dual redundent backplane.

210	123		The proposed storage should be scalable to atleast 384 drives in future with or without adding a controller	Requesting the technical committee to kindly seek 200 Drives expansion as 384 drives with subjected set of specifications makes the Primary storage OEM Specific and most of the Gartner leaders will not be able to comply on the same. Hence requesting you to kindly amend and change the same to : The proposed storage should be scalable to at least 200 drives or more in future with or without adding a controller	Deleted
211	123		The storage operating system must provide FC, NVMe-oF, NVMe over TCP, iSCSI, NFS (NFSv3, NFSv4, NFSv4.1), CIFS/SMB, S3 protocols natively or by using additional appliance (supported & developed by same OEM) to support heterogeneous application environment.	Dear Technical Committee, Requesting you to kindly remove NVMe over TCP as it has Higher latency with lower throughput and might lead to network congestion. Hence, requesting you to kindly change the same to : The storage operating system must provide FC, NVMe-oF,iSCSI,NFS (NFSv3, NFSv4, NFSv4.1), CIFS/SMB, S3 protocols natively or by using additional appliance (supported & developed by same OEM) to support heterogeneous application environment.	The storage operating system must provide FC, NVMe-oF / NVMe over TCP, iSCSI, NFS (NFSv3, NFSv4, NFSv4.1), CIFS/SMB, S3 protocols natively or by using additional appliance (supported & developed by same OEM) to support heterogeneous application environment.
212	123		The system should be configured with an addressable usable capacity of 250 TB using NVMe drives with dual parity or equivalent protection without considering efficiency features like de-duplication & compression.	Requesting the technical committee to kindly seek NVMe TLC / MLC drives as TLC and MLC drives have higher endurance over standard NVMe Drives hence requesting you to kindly seek NVMe (TLC/MLC) drives to safeguard future investment. The system should be configured with an addressable usable capacity of 250 TB using NVMe drives with dual parity or equivalent protection without considering efficiency features like de-duplication & compression.	As per RFP
213	427-430	Specification-Storage Primary	1) Synchronous and Asynchronous Replication between 2 DCs for both Block and File Protocols. 2) 3DC Replication with Zero RPO across 3 DCs where 2 Sites are within Metro Distance and 3rd Site can be >1000km away for both block and file Protocols. 3) Replication of 1 volume to upto 4 distinct storage systems spread across geographical locations. 4) If separate FCIP routers are required for asynchronous replication, then the same should be included in the BOM Required software as well as hardware as required must be offered from day one for all the features needed above.	1) Synchronous and Asynchronous Replication between 2 DCs 2) 3DC Replication with Zero RPO across 3 DCs where 2 Sites are within Metro Distance and 3rd Site can be >1000km away. 3) Replication of 1 volume to upto 4 distinct storage systems spread across geographical locations. 4) If separate FCIP routers are required for asynchronous replication, then the same should be included in the BOM Required software as well as hardware as required must be offered from day one for all the features needed above.	1) Synchronous and Asynchronous Replication between 2 DCs for both Block and File Protocols. 2) 3DC Replication with Zero RPO across 3 DCs where 2 Sites are within Metro Distance and 3rd Site can be >1000km away for both block and file Protocols. 3) Deleted 4) If separate FCIP routers are required for asynchronous replication, then the same should be included in the BOM Required software as well as hardware as required must be offered from day one for all the features needed above.

214	427-430	Specification-Storage Primary	Offered Storage must be configured with required Licenses to configure: 1) Replication solution must support bi-directional replication to minimum 3 meity compliant public clouds, replication traffic must be encrypted during replication to public cloud. 2) Storage must support tiering of inactive data to minimum 3 meity compliant public clouds or on premise object storage. 3) Offered Storage replication should be secured by end-to-end encryption and bandwidth optmization over a WAN link. All the necessary hardware & licenses should be quoted from day 1 in Highly available configuration. Required software as well as hardware as required must be offered from day one for all the features needed above.	Please delete this clause for wider Participation.	Offered Storage must be configured with required Licenses to configure: 1) Replication solution must support bi-directional replication between DC to DR (on premise and cloud) & vice-versa with encryption through natively or using third party software / hardware. 2) Storage must support tiering of inactive data to public clouds or on premise object storage. 3) Offered Storage replication should be secured by end-to-end encryption and bandwidth optmization over a WAN link. All the necessary hardware & licenses should be quoted from day 1 in Highly available configuration. Required software as well as hardware as required must be offered from day one for all the features needed above.
215	427-430	Specification-Storage Primary	Offered Storage must have capability to implement Quality of Service which must allow administrators to limit IOPS and throughput for certain Block Luns and File shares. Required HW and SW must be offered.	Offered Storage must have capability to implement Quality of Service which must allow administrators to limit IOPS,Latency and throughput for certain Block Luns. Required HW and SW must be offered.	As per RFP
216	427-430	Specification-Storage Primary	Offered Storage must provide Inline as well as Post-Process deduplication, compression for both Block and File data. Data reduction must be maintained while Tiering and replicating the data.	Offered Storage must provide Inline deduplication, compression.	Offered Storage must provide Inline or Post-Process deduplication, compression for both Block and File data. Data reduction must be maintained while Tiering and replicating the data.
217	427-430	Specification-Storage Primary	Offered Storage replication should be secured by end-to-end encryption and bandwidth optmization over a WAN link. All the necessary hardware & licenses should be quoted from day 1 in Highly available configuration.	Please delete this clause for wider Participation.	Offered Storage replication should be secured by end-to-end encryption or equivalent secure mechanism like hashing etc. and bandwidth optmization over a WAN link. All the necessary hardware & licenses should be quoted from day 1.
218	427-430	Specification-Storage Primary	Should have the capability of 32 Gbps Fiber channel ports as well as 25 GbE, 100 GbE optical ports. The storage should be supplied with minimum 16 ports of 32 Gbps FC & 8 x 25GbE .	Should have the capability of 32 Gbps Fiber channel ports as well as 25 GbE, 100 GbE optical ports. The storage should be supplied with minimum 8 ports of 32 Gbps FC & 8 x 25GbE .	Should have the capability of 32 Gbps Fibre channel ports as well as 10/25/100 GbE optical ports. The storage should be supplied with minimum 16 ports of 32 Gbps FC & 8 x 25GbE or 16x10 GbE.
219	427-430	Specification-Storage Primary	Should have the capability to reverse relationships instantly to enable rapid data recovery	Please delete this clause for wider Participation.	As per RFP
220	427-430	Specification-Storage Primary	Solution should have the capability to tier inactive data at a sub volume level between offered NVME solid state drives to low cost object storage in order to optimize TCO. Any license applicable for the same should be included in the Bill of Material	This is OEM Specific clause, Please delete this clause for wider Participation.	Solution should have the capability to tier inactive data between offered NVME storage to low cost object storage in order to optimize TCO natively or using third party software/ hardware. Any license applicable for the same should be included in the Bill of Material
221	427-430	Specification-Storage Primary	Storage OEM should be from the leader's quadrant from the Gartner's Quadrant for primary storage in last 3 years	Storage OEM should be from the leader's quadrant from the Gartner's Quadrant for primary storage in last 3 years. The proposed storage should provide 100% Data Availability Guarantee.	As per RFP

222	427-430	Specification-Storage Primary	The proposed should be All Flash NVME based storage and should support at least 190 NVME or higher drives with offered controllers in scale up and scale out architecture. Offered storage must have at least 96 cores or higher across offered controllers.	The proposed should be All Flash NVME based storage and should support at least 190 NVME or higher drives in scale up and scale out architecture. Offered storage must have at least 32 cores or higher across offered controllers.	As per RFP
223	427-430	Specification-Storage Primary	The proposed system with flash drives should deliver a performance of atleast 500000 IOPS considering a 8KB average IO size, with a read/ write ratio of 70/30.	The proposed system with flash drives should deliver a performance of atleast 500000 IOPS considering a 8KB average IO size, with a read/ write ratio of 70/30 and sub-milisecond latency.	The proposed system with flash drives should deliver a performance of atleast 500000 IOPS considering a 8KB average IO size, with a read/ write ratio of 70/30 and latency <=4 ms.
224	427-430	Specification-Storage Primary	The storage system should offer capability to identify and remediate ransomware attacks using autonomous ransomware protection & restore within the controllers or using additional appliance. The offered system should offer ransomware and insider threat detection to protect data with early detection and actionable intelligence on ransomware and other malware incursions. Required software as well as hardware as required must be offered from day one.	Please delete this clause for wider Participation.	The storage system should have the capacity to recognise and neutralise ransomware assaults through the use of extra appliances or autonomous ransomware protection and restoration within the controllers. Required software / hardware must be offered from day one.
225	427-430	Specification-Storage Primary	The system should be configured with an addressable usable capacity of 250 TB using NVMe drives with dual parity or equivalent protection without considering efficiency features like de-duplication & compression.	The system should be configured with an addressable usable capacity of 250 TB using NVMe TLC/MLC drives with dual parity or equivalent protection without considering efficiency features like de-duplication & compression.	As per RFP
226	115		1.1.2 Payment Collection w. Acceptance of part/advance payment - The system should have the flexibility to accept full, partial or advance payments. The system should also have the facility to centrally change these settings from time to time	a) How should the part payment be accepted ? i) Should be in different payment forms ? Ii) Will there be interest collected on Part payments ?	Part payment is allowed to consumers as per regulatory Provisions.
227	118		1.2 Customer Relation Management Module u. CRM should include Call Center software for call center agents to perform inbound and outbound calling and it should be integrated with the billing system to fetch the customer information automatically when customer call has been received in the call center.	a) How many agents are expected to use the software for which license is required ? B) What are the essential features required for this application ?	a. 70 no. user licenses are required (Pls refer BoQ) b. CRM is the part of Billing software. Calling software features to be mentioned
228	130		Section 7. E. Other application required to be loaded on ANDROID and iOS Based Mobile Devices	Request to change point as below. E. Other application required to be loaded on ANDROID Mobile Devices	Other application required to be loaded on ANDROID Mobile Devices
229	139		Section 7 1.6 Prepaid Engine 3. The system should send low-credit notifications to the consumer when their balance approaches a pre- configured threshold. Alerts shall initiate on every recharge, low credit and load connection/disconnection. The alerts shall be posted on the consumer web Portal/ App in real time and sent through email. Consumer should also be alerted through other mechanisms such as onetime alarm / beep from the meter, LED blinking, message, etc.	Query: Message of low balance will be sent through MDM why it is Required in Billing System.	As per RFP

230	157		Section 7. 3. Brief Scope of work 16. To design and develop the logic to consume the meter reads data from the legacy MDAS Systems and MRIs. This is applicable for the HT and LT High Value Consumers and DT and Feeder meter modems, for the purpose of facilitating Feeder and DT level Energy Auditing.	Query: - The meter reads data from the legacy MDAS should be in MIOS format, the data in MRIs is proprietary protocol, consuming data directly from MRI's is not possible unless the MRI transfers data in MIOS format. This is evident from the fact that DISCOM also uses BCS tools for downloading data from MRI's. Therefore, the scope of consuming data from MRI's may be deleted.	As per RFP
231	172		Section 7 5 Data Migration	Clarification: - Please mention the current size of the database DISCOM wise. Please clarify: 1. How many years data is to be migrated? 2. Will the data be arranged in the required format or the bidder should migrate in whatever form the data is made available to the bidder? Who will verify the authenticity of the data given for migration?	1) Complete data 2) Data shall be required to be arranged in finalised format with Utility. 3) Data verification is not required but data matching at different levels is to be done by the bidder.
232	213		12.4Minimum Resource Requirement from SI Team Leader/ Project Management Expert Shall possess an B. Tech/B.E./MCA/MSc or higher qualification and MBA or its equivalent with at least 15 years of relevant experience in implementation of least 2 end-to-end UBS projects	Change Require :- Request you to change as Minimum Resource Requirement from SI Team Leader/ Project Management Expert Shall possess an B. Tech/B.E./MCA/MSc or higher qualification and MBA or its equivalent with at least 10 years of relevant experience in implementation of least 1 end-to-end UBS projects	As per RFP
233			General Query	Query: - Please provide the Quantity in Nos. of (Billable consumers)	As per RFP
234	126		General Query | Secondary Storage	Dear Technical Committee, Requesting you to kindly share the types of Drives required to configure Secondary Storage. Please clarity if NLSAS or SSD or SAS drives are to be configured for Secondary Storage of 250TB	Bidder shall propose based on the offered solution.
235	126		Proposed storage must have minimum 250 TB usable capacity configured with dual parity and the proposed configuration should use drives with capacity 8TB or less.	Dear Technical Committee, Requesting you to kindly ammend and change the same to 18TB drives as it takes less amount of Rack space and yields better PER TB Usable on RAW drives. hence requesting you to kindly ammend the same to : Proposed storage must have minimum 250 TB usable capacity configured with dual parity and the proposed configuration should use drives with capacity 18TB or less.	Proposed storage must have minimum 250 TB usable capacity configured with dual parity and the proposed configuration should use drives with capacity 18TB or less.

236	126		Storage should have atleast 32GB system cache memory and scalable to 64GB	Dear Technical Committee, Requesting you to kindly ammend and change the same to 256GB Cache per controller to provide better IOPS and to safeguard future investment. Hence reuqesting you to kindly change the same to : Storage should have atleast 384GB DRAM system cache memory on DAY 1	Storage should have at least 128 GB system cache memory (DRAM) per controller or higher from day 1.
237	430-431	Specification-Storage Secondary	Storage should be scalable with atleast 350 drives within expansions	Storage should be scalable with atleast 240 drives within expansions	Storage should be scalable with atleast 240 drives within expansions
238	430-431	Specification-Storage Secondary	Storage should have capabilites like compression and data reduction for efficient use of storage space.	Please delete this clause as it is not applicable on NL-SAS and SAS Disk.	As per RFP (The mentioned capability is asked for storage not for specific drive type)
239	162	4.2 On-Premises IT Infrastructure & Network Solution	The provided solution shall be designed to fulfill the compute and resource requirement based on the growth in user load and transactions in the billing system (peak and non-peak periods; year-on-year increase) for the entire period of contract to meet out the performance requirement and SLAs.	Software should be able to use workload- linked capacity models to generate predictive scenarios on capacity throttle points, based on simulated growth in business transactions & highlight underutilized parts of distributed business applications using such workload-linked capacity models	As per RFP
240	164	4.2.4.3 Resource Management	b) For any major expected increase in the workloads, the SI shall carry out the capacity planning in advance to identify & provision, where necessary, the additional capacity to meet the user growth and / or the peak load requirements to support the scalability and performance requirements of the solution.	Software should be able to use workload- linked capacity models to generate predictive scenarios on capacity throttle points, based on simulated growth in business transactions & highlight underutilized parts of distributed business applications using such workload-linked capacity models	As per RFP
241	172		4.2.4.18 Other General Requirements 3. Si need to optimize the existing mail solution for 2000 users approximately or shall provide the licenses for new email-solution as per the requirement. They shall migirate existing into new hardware including.	The existing email solution that including Operating System & Active Directory has become obsolete. In case optimization / upgradation is not possible with the existing environment. Then, shall the bidder to propose a complete e-mail solution for 2000 users with mailboxes configured on it?	The Bidder shall migrate existing mail solution to the new hardware.

242	186		2. Training Needs Analysis Conduct a Training Needs Analysis to determine the training and development needs for all the job roles that will be affected by the Billing System technology initiative at Utility. The OEM and the SI consultants will collect the appropriate data on user groups, functional and process requirements per user group, required skills and knowledge, existing training culture and training resources through workshops and interviews with Utility business owners and key business users. This will result in a Training and Development Plan including: a. The training requirements per user group. b. Recommendations on the most appropriate training delivery methods and channels. c. Identification of the criteria for training success along with any challenges and risks. d. Plan and responsibilities for the development of the training materials, such as instructor guides, participant guides, media-based training, and quick-reference guides. e. Knowledge sharing strategy to enable to perform future customizations internally.	a) How many resources are to be trained ? B) Will there be retraining involved ? C) Will there be end user training involved ?	All UPCL users involved in billing process are to be trained by successful bidder by physical training at 10-15 locations of Uttarakhand along with virtual trainings. Retraining will also be required if necessary.
243	210		2 Business Blueprinting 13. Requirement gathering workshops with findings for updated requirement specification. 14. Provisioning of testing and development environment 15. Detailed To-Be report including: To + [6] Month	Will there be a requirement to provide prototypes ?	The testing environment has to be developed within To+6 months by the successful bidder.
244	254	16.2.2.4Problem Resolution and Notification Times a) Threshold Definitions	Critical: Show-stopper application breakdown/crash.	Application performance and availability is the most critical factor in this RFP and to do that performance monitoring it should have an APM (Application Performnace Monitoring) software to meet SLAs and avoid unwanted down times.	As per RFP
245			Reporting: SLA Dashboards for Servers, Routers, Switches etc. All Servers Availability / Outage Report, Health Report for Servers, Routers, Switches etc. TopN Servers by CPU, Memory and Disk, Top N Servers by Interface traffic report, Server access report through firewall logs. TopN report for routers by CPU and Memory Utilization, Interface Traffic/Utilization/Error Reports, Peak time reports (Eg. 8:00am to 8:00pm), WAN Link availability/ RTT report, Forensic reports, Bandwidth capacity planning reports, Traffic reports, User audit reports, Schedule Reports, Custom Reports, Export Reports (PDF,XLS, CSV formats), Email/Print report directly to printer..	Request to give more clairity on Forensic reports under Reporting feature	Any report as required by the auditor or any investigation agency.
246			To ensure high level of data exchange between different modules of Desktop Management and provide seamless integration between Helpdesk and Desktop Management tools – the Asset Management, Software Delivery and Control modules should essentially share the same database.	Request you to remove this OEM Specific clause as per following: To ensure high level of data exchange between different modules of Desktop Management and provide seamless integration between Helpdesk and Desktop Management tools – the Asset Management, Software Delivery and Control modules should essentially share the same database.	To ensure high level of data exchange between different modules of Desktop Management and provide seamless integration between Helpdesk and Desktop Management tools – the Asset Management, Software Delivery and Control modules should essentially share the same database.
247	1		At least 8 x 10/100/1000Base-T RJ-45 ports, Minimum 4x 1/10 GbE fiber port with module	At least 8 x 10/100/1000Base-T RJ-45 ports, Minimum 8x 1GbE fiber port, 8x 10 Gbps SFP+ with module	As per RFP

248	4		The proposed solution should provide web-based management of SD-WAN	The proposed solution should provide web-based management of SD-WAN. The proposed SDWAN solution OEM should be a Leader in latest Gartner SDWAN report.	As per RFP
249	4		The SD-WAN solution should support more than 10,000 application signatures allowiing granular traffic steering	The SD-WAN solution should support more than 5000 application signatures allowiing granular traffic steering	The SD-WAN solution should support more than 5,000 application signatures allowiing granular traffic steering
250	24		Proposed solution should support at least 16 million concurrent sessions/connections	Proposed solution should support at least 8 million concurrent sessions/connections or higher	As per RFP
251	43	43	The SD-WAN solution should support more than 10,000 application signatures allowing granular traffic steering		The SD-WAN solution should support more than 5000 application signatures allowing granular traffic steering
252	48		2. Performace Requirement: Solution must support minimum 25 Gbps of Firewall throughput under enterprise test conditions	Kindly remove this clause. As there is a separate firewall ask in the DC, the same functionality is not required on the DC SDWAN hardware device	As per RFP
253	48		Solution must support minimum 25 Gbps of Firewall throughput under enterprise test conditions	Solution must support minimum 25 Gbps of Firewall throughput	Solution must support minimum 25 Gbps of Firewall throughput under Enterprise mix / Real world traffic
254	49		2. Performace Requirement: Solution must support minimum 5 Gbps of Threat Prevention throughput and 13 Gbps of NGFW throughput.	Please remove this clause As there is a separate firewall ask in the DC, the same functionality is not required on the DC SDWAN hardware device	As per RFP
255	49		3.Solution General Requirement: Application control database must contain more than 5000 known applications. The proposed solution must allow free custom application signatures for Homegrown and custom applications.	Please change the clause to allow for 1000 application signatures - Most applications signatures are well wthin 1000 and hence request you to reduce it to 1000 Revised Clause:Application control database must contain more than 1000 known applications. The proposed solution must allow free custom application signatures for Homegrown and custom applications.	As per RFP
256	49		3.Solution General Requirement: Proposed solution should support IPsec and SSL VPN functionality	Please remove this clause As there is a separate firewall ask in the DC, the same functionality is not required on the DC SDWAN hardware device	As per RFP
257	49		3.Solution General Requirement: Solution must not have Application specific chips like ASICs that doesn't allow future firmware and feature expansions on the same hardware. Solution must not use proprietary ASIC chips.	Please remove this clause As there is a separate firewall ask in the DC, the same functionality is not required on the DC SDWAN hardware device	Deleted
258	49		3.Solution General Requirement: The solution should have security controls such as Firewall, VPN, Application Control, URL Filtering, IPS, QOS, Anti- Bot, Antivirus. All required licenses must be included from day 1.	Please remove this clause As there is a separate firewall ask in the DC, the same functionality is not required on the DC SDWAN hardware device	As per RFP

259	49		4.SDWAN Features: The SD-WAN solution should support more than 10,000 application signatures allowiing granular traffic steering	Please change the clause to allow for 1000 application signatures - Most applications signatures are well wthin 1000 and hence request you to reduce it to 1000 Revised Clause:The SD-WAN solution should support more than 1000 application signatures allowiing granular traffic steering	4.SDWAN Features: The SD-WAN solution should support more than 5,000 application signatures allowiing granular traffic steering
260	49		Solution must not have Application specific chips like ASICs that doesn't allow future firmware and feature expansions on the same hardware. Solution must not use proprietary ASIC chips.	Remove the Point	Deleted
261	49		Solution must support minimum 5 Gbps of Threat Prevention throughput and 13 Gbps of NGFW throughput.	Solution must support minimum 10 Gbps of Threat Prevention throughput	As per RFP
262	49		The proposed solution should provide web-based management of SD-WAN	The proposed solution should provide web-based management of SD-WAN. The proposed SDWAN solution OEM should be a Leader in latest Gartner SDWAN report.	As per RFP
263	49		The proposed solution should provide web-based management of SD-WAN	The proposed solution should provide web-based management of SD-WAN. The proposed SDWAN solution OEM should be a Leader in latest Gartner SDWAN report.	As per RFP
264	49	49	The solution should support Link Health SLA state based on Excellent, Good, Poor or Down State.		The solution should support Link Health SLA state based on Excellent, Good, Poor or Down State or equivalent health SLA
265	50		4. SDWAN Features: The solution should provide granular support for application (or service) based traffic steering - support for User / Machine based Access Role objects, network and host objects.	Kindly remove user/machine as it is no SDWAN specification. Revised Clause:The solution should provide granular support for application (or service) based traffic steering	As per RFP
266	50		5.Security Features: Vendor must have an integrated Anti-Bot and Anti-Virus application on the next generation firewall	Please remove this clause - As there is a separate firewall ask in the DC, the same functionality is not required on the DC SDWAN hardware device	As per RFP
267	50	50	Device Management system should provide the real time health status of all the modules on the dashboard for CPU & memory utilization, state table, total no. of concurrent connections and the connections per second counter. It must provide a security rule hit counter in the security policy.		As per RFP
268	50	50	Device Management system should provide the real time health status of all the modules on the dashboard for CPU & memory utilization, state table, total no. of concurrent connections and the connections per second counter. It must provide a security rule hit counter in the security policy.		As per RFP
269	51		5.Security Features: For future reference, the proposed solution should be capbale of On-prem Sandboxing functionality to avoid zero day attack, Sandbox appliance should be provided from Firewall OEM only without any 3rd party. OEM to submit the public website/datasheet of availablity of sandbox appliance during bid submission.	Please remove this clause - As there is a separate firewall ask in the DC, the same functionality is not required on the DC SDWAN hardware device	As per RFP

270	51		6.Administration, Management and Logging: Device Management system should provide the real time health status of all the modules on the dashboard for CPU & memory utilization, state table, total no. of concurrent connections and the connections per second counter. It must provide a security rule hit counter in the security policy.	Total no. of concurrent connections and the connections per second counter. It must provide a security rule hit counter in the security policy Kindly remove this as this is firewall feature and not SDWAN feature.	As per RFP
271	51	51	Solution must be able to segment the rule base in a layered structure. Solution must be able to segment the rule base to allow structure flexibility to align with dynamic networks.		Yes
272	51	51	Solution must be able to segment the rules base in favor of delegation of duties in which changes in one segment will not affect other segments on the same autonomous system.		Yes
273	51	51	The proposed solution must support the ability to lock configuration while modifying it, avoiding administrator collision when there are multiple people configuring the appliance		Yes
274	52		2.Performance Requirement: Solution must support minimum 2.5Gbps of Firewall throughput underenterprise test conditions	Since this device is for branch location , 100 Mbps throughput would be sufficient Revised Clause:Solution must support minimum 100Mbps of Firewall throughput underenterprise test conditions	As per RFP
275	52		2.Performance Requirement: Solution must support minimum 500Mbps of Threat Prevention throughput and 900 Mbps of NGFW throughput.	Since this device is for branch location , 100 Mbps throughput would be sufficient Revised Clause:Performance Requirement:Solution must support minimum 100Mbps of Threat Prevention throughput and 100 Mbps of NGFW throughput.	As per RFP
276	52		3.Solution General Requirment The solution should have security controls such as Firewall, VPN, Application Control, URL Filtering, IPS, QOS, Anti-Bot, Antivirus, Email Security/Anti-Spam. All required licenses must be included from day 1.	Please remove Email security and Antibot as these are not SDWAN features and are not required at the branch - they will be applied at the email security appliance at the DC. Revised Clause:The solution should have security controls such as Firewall, VPN, Application Control, URL Filtering, IPS, QOS, Antivirus. All required licenses must be included from day 1.	As per RFP
277	52		3.Solution General Requirment: Proposed solution should support IPsec and SSL VPN functionality.	Please remove this clause SSL VPN functionality as it is not required for SDWAN	As per RFP
278	52		At least 8x 10/100/1000Base-T RJ-45 ports, 1x 1GbE copper/fiber WAN port and 1x 1GbE copper/fiber DMZ port	At least 5x 10/100/1000Base-T RJ-45 ports,	As per RFP
279	52		Security Management App: The solution must have flexibility to have intuitive mobile app to provides real-time monitoring of network events, alerts when your network is at risk, enables admin to quickly monitor and alert of security events.	Security Management App/Email Alert: The solution must have flexibility to have intuitive mobile app/Email alert to provides real-time monitoring of network events, alerts when your network is at risk, enables admin to quickly monitor and alert of security events.	Security Management App/Email Alert: The solution must have flexibility to have intuitive mobile app/Email alert to provides real-time monitoring of network events, alerts when your network is at risk, enables admin to quickly monitor and alert of security events.
280	52		Solution must support minimum 2.5Gbps of Firewall throughput underenterprise test conditions	Solution must support minimum 2.5Gbps of Firewall and IPSec throughput	Solution must support minimum 2.5Gbps of Firewall and IPSec throughput under Enterprise mix / Real world traffic
281	52		Solution must support minimum 500Mbps of Threat Prevention throughput and 900 Mbps of NGFW throughput.	Solution must support minimum 500Mbps of Threat Prevention throughput and 800 Mbps of NGFW throughput.	As per RFP

282	52		The SD-WAN solution should support more than 10,000 application signatures allowiing granular traffic steering	The SD-WAN solution should support more than 5000 application signatures allowiing granular traffic steering	The SD-WAN solution should support more than 5000 application signatures allowiing granular traffic steering
283	52	52	The solution should have security controls such as Firewall, VPN, Application Control, URL Filtering, IPS, QOS, Anti-Bot, Antivirus, Email Security/Anti-Spam. All required licenses must be included from day 1.		As per RFP
284	52	52	The solution should have security controls such as Firewall, VPN, Application Control, URL Filtering, IPS, QOS, Anti-Bot, Antivirus, Email Security/Anti-Spam. All required licenses must be included from day 1.		As per RFP
285	53		3.Solution General Requirment Application control database must contain more than 5000 known applications. The proposed solution must allow free custom application signatures for Homegrown and custom applications.	Please change the clause to allow for 1000 application signatures - Most applications signatures are well wthin 1000 and hence request you to reduce it to 1000 Revised Clause:Application control database must contain more than 1000 known applications. The proposed solution must allow free custom application signatures for Homegrown and custom applications.	As per RFP
286	53	53	The solution should be able to capture historic events of link swap events, specific sd-wan traffic steering logs and monitoring administrative events such as policy install or steering object changes.		Yes
287	53	53	The solution should support Link Health SLA state based on Excellent, Good, Poor or Down State.		The solution should support Link Health SLA state based on Excellent, Good, Poor or Down State or equivalent health SLA
288	54		5.Security Features For future reference, the proposed solution should be capbale of On-prem Sandboxing functionality to avoid zero day attack, Sandbox appliance should be provided from Firewall OEM only without any 3rd party. OEM to submit the public website/datasheet of availablity of sandbox appliance during bid submission.	Please allow cloud based sandboxing as it will help reduce hardware footprint at the branch. Revised Clause:For future reference, the proposed solution should be capbale of On-prem/cloud based Sandboxing functionality to avoid zero day attack, Sandbox appliance should be provided from Firewall OEM only without any 3rd party. OEM to submit the public website/datasheet of availablity of sandbox appliance during bid submission.	As per RFP
289	54		5.Security Features The proposed solution shall include all additional licenses required for the antivirus & Anti-Bot features from Day1	Antivirus is a end host software - request to consider Antivirus or Anti malware. Revised Clause:The proposed solution shall include all additional licenses required for the antivirus/anti malware & Anti-Bot features from Day1	The proposed solution shall include all additional licenses required for the antivirus/anti malware & Anti-Bot features from Day1
290	54	54	Device Management system should provide the real time health status of all the firewall modules on the dashboard for CPU & memory utilization		As per RFP
291	353-359	SD WAN Field device	Anti-bot application must be able to detect and stop suspicious abnormal network behavior	End point function not required on the SDWAN gateway.	As per RFP

292	353-359	SD-WAN DC Equipment	Anti-bot application must be able to detect and stop suspicious abnormal network behavior	Remove the clause	As per RFP
293	353-359	SD WAN Field device	Anti-Bot protections should be able to scan for bot actions	End point function not required on the SDWAN gateway.	As per RFP
294	353-359	SD-WAN DC Equipment	Anti-Bot protections should be able to scan for bot actions	Remove the clause	As per RFP
295	353-359	SD WAN Field device	Anti-Virus and Anti-Bot policies must be centrally/Locally managed with granular policy configuration and enforcement	End point function not required on the SDWAN gateway.	As per RFP
296	353-359	SD-WAN DC Equipment	Anti-Virus and Anti-Bot policies must be centrally/Locally managed with granular policy configuration and enforcement	Remove the clause	As per RFP
297	353-359	SD-WAN DC Equipment	At least 8 x 10/100/1000Base-T RJ-45 ports, Minimum 4x 1/10 GbE fiber port with module	Minimum 6x 1/10 GbE fiber port.	As per RFP
298	353-359	SD-WAN DC Equipment	Device Management system should provide the real time health status of all the modules on the dashboard for CPU & memory utilization, state table, total no. of concurrent connections and the connections per second counter. It must provide a security rule hit counter in the security policy.	Device Management system should provide the real time health status of all the modules on the dashboard for CPU & memory utilization/state table, total no. of concurrent connections and the connections per second counter or It must provide a security rule hit counter in the security policy.	As per RFP
299	353-359	SD-WAN DC Equipment	Firewall should have Pre-defined security policy for easy deployment.	Firewall should have Pre-defined or manual customised security policy for easy deployment.	Firewall should have Pre-defined or manual customised security policy for easy deployment.
300	353-359	SD WAN Field device	Firewall should have Pre-defined security policy for easy deployment.	Firewall should have Pre-defined or manual customised security policy for easy deployment.	Firewall should have Pre-defined or manual customised security policy for easy deployment.
301	353-359	SD WAN Field device	For future reference, the proposed solution should be capbale of On-prem Sandboxing functionality to avoid zero day attack, Sandbox appliance should be provided from Firewall OEM only without any 3rd party. OEM to submit the public website/datasheet of availablity of sandbox appliance during bid submission.	Firewall OEM specific clause, restricting point.	As per RFP
302	353-359	SD-WAN DC Equipment	For future reference, the proposed solution should be capbale of On-prem Sandboxing functionality to avoid zero day attack, Sandbox appliance should be provided from Firewall OEM only without any 3rd party. OEM to submit the public website/datasheet of availablity of sandbox appliance during bid submission.	Remove the clause	As per RFP
303	353-359	SD-WAN DC Equipment	IPS must be able to detect and block network and application layer attacks, protecting at least the following services: email services, DNS, FTP.	IPS must be able to detect and block network.	As per RFP
304	353-359	SD WAN Field device	IPS must be able to detect and block network and application layer attacks, protecting at least the following services: email services, DNS, FTP.	IPS must be able to detect and block network.	As per RFP
305	353-359	SD-WAN DC Equipment	NG-Firewall should support Identity based AD queries	Remove the clause AD integration not possib;e	As per RFP
306	353-359	SD WAN Field device	NG-Firewall should support Identity based AD queries	Remove the clause AD integration not possib;e	As per RFP
307	353-359	SD-WAN DC Equipment	Proposed solution should support IPsec and SSL VPN functionality	Proposed solution should support IPsec /SSL VPN functionality	As per RFP
308	353-359	SD WAN Field device	Proposed solution should support IPsec and SSL VPN functionality	Proposed solution should support IPsec /SSL VPN functionality	As per RFP

309	353-359	SD WAN Field device	Security Management App: The solution must have flexibility to have intuitive mobile app to provides real-time monitoring of network events, alerts when your network is at risk, enables admin to quickly monitor and alert of security events.	Remove the clause	As per RFP
310	353-359	SD-WAN DC Equipment	Solution must be able to segment the rule base in a layered structure. Solution must be able to segment the rule base to allow structure flexibility to align with dynamic networks.	Solution must be able to segment the rule base in a layered structure.	Yes
311	353-359	SD-WAN DC Equipment	Solution must be able to segment the rule base in a sub-policy structure in which only relevant traffic is being forwarded to relevant policy segment for an autonomous system	Solution must be able to segment the rule base in a sub-policy structure.	Yes
312	353-359	SD-WAN DC Equipment	Solution must be able to segment the rules base in favor of delegation of duties in which changes in one segment will not affect other segments on the same autonomous system.	Solution must be able to segment the rules base in favor of delegation of duties.	Solution must be able to segment the rules base in favor of delegation of duties.
313	353-359	SD WAN Field device	Solution must support minimum 2.5Gbps of Firewall throughput underenterprise test conditions	Solution must support minimum 1Gbps of Firewall throughput underenterprise test conditions	As per RFP
314	353-359	SD-WAN DC Equipment	Solution must support minimum 25 Gbps of Firewall throughput under enterprise test conditions	Solution must support minimum 5 Gbps of Firewall throughput under enterprise test conditions	As per RFP
315	353-359	SD-WAN DC Equipment	Solution must support minimum 5 Gbps of Threat Prevention throughput and 13 Gbps of NGFW throughput.	Solution must support minimum 5 Gbps of Threat Prevention throughput and NGFW throughput.	As per RFP
316	353-359	SD WAN Field device	Solution must support minimum 500Mbps of Threat Prevention throughput and 900 Mbps of NGFW throughput.	Solution must support minimum 500Mbps of Threat Prevention throughput and 500 Mbps of NGFW throughput.	As per RFP
317	353-359	SD-WAN DC Equipment	The proposed solution must allow policy creation for IP Address,, Services, application control etc.. The proposed solution should support MAC filtering as well.	The proposed solution must allow policy creation for IP Address,, Services, application control etc.	The proposed solution must allow policy creation for IP Address,, Services, application control etc.
318	353-359	SD WAN Field device	The proposed solution must allow policy creation for IP Address,, Services, application control etc.. The proposed solution should support MAC filtering as well.	The proposed solution must allow policy creation for IP Address,, Services, application control etc.	The proposed solution must allow policy creation for IP Address,, Services, application control etc.
319	353-359	SD-WAN DC Equipment	The proposed solution must support different actions in the policy such as deny, drop, Allow, accept	The proposed solution must support different actions in the policy such as deny/ drop, Allow/ accept and inspect.	The proposed solution must support different actions in the policy such as deny/ drop, Allow/ accept
320	353-359	SD WAN Field device	The proposed solution must support different actions in the policy such as deny, drop, Allow, accept	The proposed solution must support different actions in the policy such as deny/ drop, Allow/ accept and inspect.	The proposed solution must support different actions in the policy such as deny/ drop, Allow/ accept
321	353-359	SD-WAN DC Equipment	The proposed solution must support the ability to lock configuration while modifying it, avoiding administrator collision when there are multiple people configuring the appliance	while doing the config change by multiple users, it will alert through messagin status.	Yes
322	353-359	SD-WAN DC Equipment	The proposed solution of appliances should support the dynamic routing protocols with readiness for OSPFv2, BGPv4 and 4++, RIP, PIM (SM, DM, SSM), IGMP	The proposed solution of appliances should support the dynamic routing protocols with readiness for OSPFv2, BGPv4 or 4++, RIP, PIM (SM/DM/ SSM)/ IGMP	The proposed solution of appliances should support the dynamic routing protocols with readiness for OSPFv2, BGPv4 or 4++, RIP, PIM (SM/DM/ SSM)/ IGMP

323	353-359	SD WAN Field device	The proposed solution of appliances should support the dynamic routing protocols with readiness for OSPFv2, BGPv4 and 4++, RIP, PIM (SM, DM, SSM), IGMP	The proposed solution of appliances should support the dynamic routing protocols with readiness for OSPFv2, BGPv4 or 4++, RIP, PIM (SM/DM/ SSM)/ IGMP	The proposed solution of appliances should support the dynamic routing protocols with readiness for OSPFv2, BGPv4 or 4++, RIP, PIM (SM/DM/ SSM)/ IGMP
324	353-359	SD WAN Field device	The proposed solution shall include all additional licenses required for the antivirus & Anti-Bot features from Day1	End point function not required on the SDWAN gateway.	As per RFP
325	353-359	SD-WAN DC Equipment	The proposed solution shall include all additional licenses required for the antivirus & Anti-Bot features from Day1	Remove the clause	As per RFP
326	353-359	SD-WAN DC Equipment	The solution must support IPv6. Local network and internet connections, dual stack tunneling IPv4 over IPv6 networks and prefix delegation	The solution must support IPv6. Local network and internet connections, dual stack tunneling IPv4 over IPv6 networks/ prefix delegation	The solution must support IPv6. Local network and internet connections, dual stack tunneling IPv4 over IPv6 networks/ prefix delegation
327	353-359	SD WAN Field device	The solution must support IPv6. Local network and internet connections, dual stack tunneling IPv4 over IPv6 networks and prefix delegation	The solution must support IPv6. Local network and internet connections, dual stack tunneling IPv4 over IPv6 networks/ prefix delegation	The solution must support IPv6. Local network and internet connections, dual stack tunneling IPv4 over IPv6 networks/ prefix delegation
328	353-359	SD WAN Field device	The solution should have security controls such as Firewall, VPN, Application Control, URL Filtering, IPS, QOS, Anti-Bot, Antivirus, Email Security/Anti-Spam. All required licenses must be included from day 1.	The solution should have security controls such as Firewall, VPN, Application Control, domain/URL Filtering, IPS, QOS. All required licenses must be included from day 1.	As per RFP
329	353-359	SD-WAN DC Equipment	The solution should support Domain Based VPNs, VPN Gateways behind NAT Devices, Hub-Spoke Topology	OEM specific clause for Domain Based VPN	The solution should support Domain Based VPNs/ VPN Gateways behind NAT Devices, Hub-Spoke Topology
330	353-359	SD WAN Field device	The solution should support Domain Based VPNs, VPN Gateways behind NAT Devices, Hub-Spoke Topology	OEM specific clause for Domain Based VPN	The solution should support Domain Based VPNs/ VPN Gateways behind NAT Devices, Hub-Spoke Topology
331	353-359	SD WAN Field device	Vendor must have an integrated Anti-Bot and Anti-Virus application on the next generation firewall	End point function not required on the SDWAN gateway.	As per RFP
332	353-359	SD-WAN DC Equipment	Vendor must have an integrated Anti-Bot and Anti-Virus application on the next generation firewall	Remove the clause	As per RFP
333	353-359	SD-WAN DC Equipment	VPN, Application Control, URL Filtering, IPS, QOS, AntiBot, Antivirus. All required licenses must be included from day 1.	VPN, Application Control, domain/URL Filtering, IPS, QOS. All required licenses must be included from day 1.	As per RFP
334	1		Ability to have physical or logical separation of the collection module, logging module and analysis / correlation module with the ability for adding more devices, locations, applications, etc.	Ability to have physical or logical separation of the collection module, logging module /analysis / correlation module with the ability for adding more devices, locations, applications, etc.	Ability to have physical or logical separation of the collection module, logging module / analysis / correlation module with the ability for adding more devices, locations, applications, etc.
335	2		Addresses various scenarios including but not limited to the following: Activity monitoring and attack detection on critical systems, Breach detection, Tracking and trace-back events across disparate devices end to end, Comprehensive monitoring of firewalls and other security devices and Malware detection and supports log collection, correlation and alerts for a minimum of 2000 events per second and it should be scalable to more events when required without having to make architectural changes.	Addresses various scenarios including but not limited to the following: Activity monitoring and attack detection on critical systems, Breach detection, Tracking and trace-back events across disparate devices end to end, Comprehensive monitoring of firewalls and other security devices and Malware detection and supports log collection, correlation and alerts for a minimum of 2000 events per second and it should be scalable to more events when required without having to make architectural changes. SIEM must support 500 devices from dayone.	Addresses various scenarios including but not limited to the following: Activity monitoring and attack detection on critical systems, Breach detection, Tracking and trace-back events across disparate devices end to end, Comprehensive monitoring of firewalls and other security devices and Malware detection and supports log collection, correlation and alerts for a minimum of 10,000 events per second and it should be scalable to more events when required without having to make architectural changes.

336	5		Administrator can define role-based access to the system by device, device group, functional group or network range also ability to modify communications ports between SIEM components in case there is a conflict with the port configuration in the user environment supportting for Multi Factor Authentication with solutions like Google Authenticator, Microsoft Authenticator also Central management of all components and administrative functions from a single web based/console user interface also provide knowledge base and best practices for various security vulnerabilities of the detected incidents and versions.	Administrator can define role-based access to the system by device, device group, functional group or network range also ability to modify communications ports between SIEM components in case there is a conflict with the port configuration in the user environment supportting for Multi Factor Authentication with solutions like Google Authenticator/ Microsoft Authenticator/ Cisco Duo/Okta also Central management of all components and administrative functions from a single web based/console user interface also provide knowledge base and best practices for various security vulnerabilities of the detected incidents and versions.	Administrator can define role-based access to the system by device, device group, functional group or network range also ability to modify communications ports between SIEM components in case there is a conflict with the port configuration in the user environment supportting for Multi Factor Authentication with solutions like Google Authenticator/ Microsoft Authenticator/ Cisco Duo/Okta also Central management of all components and administrative functions from a single web based/console user interface also provide knowledge base and best practices for various security vulnerabilities of the detected incidents and versions.
337	6		User interface that allows security analysts to manually analyse the data collected and ability to handle one month of online and 11 months of offline data with flexibility to increase the capability by adding additional hardware resources. The proposed solution should have capability to archive logs in cold storage such as tape. The proposed solution should have capability to store raw logs if required.	User interface that allows security analysts to manually analyse the data collected and ability to handle one month of online and 11 months of offline data with flexibility to increase the capability by adding additional hardware resources. The proposed solution should have capability to archive logs in cold storage such as tape or NFS storage . The proposed solution should have capability to store raw logs if required.	User interface that allows security analysts to manually analyse the data collected and ability to handle one month of online and 11 months of offline data with flexibility to increase the capability by adding additional hardware resources. The proposed solution should have capability to archive logs in cold storage such as tape or NFS storage . The proposed solution should have capability to store raw logs if required.
338	7		No logs should be lost due to any kind of disruption for both real time collection as well as long-term storage and Log security in terms of integrity and availability also run in active / passive mode in a DC-DR environment in future and should be able to failover automatically to DR in case of a primary failure also proposed Solution must offer all of the below built-in Compliance Modules at no additional cost: ISO 27001 Compliance, PCI Compliance and ISO 27017	No logs should be lost due to any kind of disruption for both real time collection as well as long-term storage and Log security in terms of integrity and availability also run in active / passive mode in a DC-DR environment in future and should be able to failover manually or automatically to DR in case of a primary failure also proposed Solution must offer all of the below built-in Compliance Modules at no additional cost: ISO 27001 Compliance, PCI Compliance or ISO 27017	No logs should be lost due to any kind of disruption for both real time collection as well as long-term storage and Log security in terms of integrity and availability also run in active / passive mode in a DC-DR environment in future and should be able to failover manually or automatically to DR in case of a primary failure also proposed Solution must offer all of the below built-in Compliance Modules at no additional cost: ISO 27001 Compliance, PCI Compliance or ISO 27017
339	10		Perform offline data dump analysis by the analyst. Including the ability to create data stores, upload files to a data store, create analytical queries, and map the results to a dashboard. The data file formats should include csv, json, xml. also solution must not be constrained by EPS having unified single dashboard to view the resources usage like CPU, RAM, Storage, Interface bandwidth, for every single server node sub-system, with support for historic view.	Perform offline data dump analysis by the analyst. Including the ability to create data stores, upload files to a data store, create analytical queries, and map the results to a dashboard. The data file formats should include csv, json, xml. also solution must not be constrained by EPS having unified single dashboard to view the resources usage like CPU, RAM, Storage, Interface bandwidth, for every single server node sub-system, with support for historic view.	As per RFP
340	12		The system should support, not restricted to, the following log and event collection methods:Syslog – UDP (as detailed in RFC 3164) TCP (as detailed in RFC 3195), Flat file logs such as from DNS, DHCP, Mail servers, web servers, Windows events logs – Agent- based or agentless, FTP, S/FTP, SNMP, ODBC, CP-LEA, SDEE, WMI, JDBC, NetFlow, JFlow, Sflow , AIX,Single-line Flat Files and Multi-line Flat Files, Compressed Flat Files (single and multi- line), NetApp CIFS, eStreamer, Metasploit, Nexpose, Nessus, eEye Retina, Tripwire and API.	The system should support, not restricted to, the following log and event collection methods:Syslog – UDP (as detailed in RFC 3164) TCP (as detailed in RFC 3195), Flat file logs such as from DNS, DHCP, Mail servers, web servers, Windows events logs – Agent-based or agentless, FTP, S/FTP, SNMP, CP-LEA, SDEE, WMI, JDBC, NetFlow, JFlow, Sflow , AIX,Flat file, NetApp CIFS, eStreamer, Metasploit, Nexpose, Nessus, and API.	As per RFP

341	13		Ability to collect and analyse logs from different log sources which include operational Events / Logs of Security devices including IDS / IPS, Firewalls, Anti-virus and other such devices, Logs / Events from the servers such as Web server, Mail server, DNS Server, Application Servers, Operating systems (Windows, Unix, Linux, AIX, Solaris etc), Virtualization platforms, Databases (Postgres, Oracle, SQL, DB2, MySql, Sqlite, MS-Access etc.), Storage systems, etc. as deemed to be important for the purpose of Security.	Ability to collect and analyse logs from different log sources which include operational Events / Logs of Security devices including IDS / IPS, Firewalls, Anti-virus and other such devices, Logs / Events from the servers such as Web server, Mail server, DNS Server, Application Servers, Operating systems (Windows, Unix, Linux, AIX, Solaris etc), Virtualization platforms, Databases (Postgres, Oracle, SQL, DB2, MySql, Sqlite etc.), Storage systems, etc. as deemed to be important for the purpose of Security.	Ability to collect and analyse logs from different log sources which include operational Events / Logs of Security devices including IDS / IPS, Firewalls, Anti-virus and other such devices, Logs / Events from the servers such as Web server, Mail server, DNS Server, Application Servers, Operating systems (Windows, Unix, Linux, AIX, Solaris etc), Virtualization platforms, Databases (Postgres, Oracle, SQL, DB2, MySql, Sqlite/ MS-Access etc.), Storage systems, etc. as deemed to be important for the purpose of Security.
342	14		Solution should support distributed deplyment with log collectors in multiple branches to aggregate and forward logs to centralized SIEM and ensures optimum usage of bandwidth from remote locations to Central location with minimum overall load on bandwidth also provide time based, criticality-based store and forward feature at each log collection point.	Solution should support distributed deplyment with log collectors in multiple branches to aggregate and forward logs to centralized SIEM and ensures optimum usage of bandwidth from remote locations to Central location with minimum overall load on bandwidth.	As per RFP
343	47		Ability to perform free text searches for events, incidents, rules and other parameters.	Ability to perform text searches for events, incidents, rules and other parameters.	As per RFP
344	59		No logs should be lost due to any kind of disruption for both real time collection as well as long-term storage and Log security in terms of integrity and availability also run in active / passive mode in a DC-DR environment in future and should be able to failover automatically to DR in case of a primary failure also proposed Solution must offer all of the below built-in Compliance Modules at no additional cost: ISO 27001 Compliance, PCI Compliance and ISO 27017	Kindly requesting to provide the details if the required SIEM solution in DC and DR is at High availibility	UPCL DC and DR shall work in Active Passive mode.SIEM application shall also work in active passive mode.
345	61		Provide a real-time event view of monitored information having native integration with Anti - APT, NIPS, EPP, HIPS, SOAR solution as per RFP specifications for centralized visibility and control	Remove point	As per RFP
346	17		Solution should provide for dissolvable agents for machines that are under investigation to unobtrusively perform forensic tasks on those machines for Windows, Linux and Mac platform.	Remove point	As per RFP
347	28		Solution should support Zero Coding Playbook Creation Mechanism	Solution should support ZeroCoding /low code Playbook Creation Mechanism	UPCL is not restricting bidder to write any codes for SOAR integration. OEM/bidders are granted the flexibility to write code during initial phase of integration. However, after integration, we aim to implement a zero-code playbook creation mechanism to mitigate any dependencies on resources for playbook creation.
348	71		Should be able to parse all the fields from SIEM, UEBA, NTA alerts including but not limited to: creation time, update time, source / destination IP, source country, category, system, rule-name, severity, etc.	Kindly requesting you to provide the number of Users the UEBA is monitoring	3000
349	71		Should be able to parse all the fields from SIEM, UEBA, NTA alerts including but not limited to: creation time, update time, source / destination IP, source country, category, system, rule-name, severity, etc.	Kindly requesting you to provide the details regarding the minimum and the maximum Gpbs of throughput performance of NTA solution.	As per RFP

350	340-343	Annexure-VI/Specification-Spine Switch	Switch must provide the capablity of inserting physical and virtual L4 - L7 (FW, LB,IPS) services dynamically between multiple segment using policy-based traffic redirect.	Remove the clause	Deleted
351	340-343	Annexure-VI/Specification-Spine Switch	Switch should support minimum 500 VRF instances with route leaking functionality	Switch should support minimum 250 VRF instances with route leaking functionality	As per RFP
352	340-343	Annexure-VI/Specification-Spine Switch	The proposed solution and switches should be part of Gartner Leader Quadrant for DC Networking for last 3 years	Request you to remove the clause	As per RFP
353	340-343	Annexure-VI/Specification-Spine Switch	The switch proposed should have minimum 50 MB Packet Buffer	The switch proposed should have minimum 32 MB Packet Buffer	As per RFP
354	340-343	Annexure-VI/Specification-Spine Switch	The switch should have capability to support 400G without any additional software or module from day 1	Remove the clause	As per RFP
355	340-343	Annexure-VI/Specification-Spine Switch	The switch should support BGP EVPN Route Type 2, Type 4 and Route Type 5 for the overlay control plane	The switch should support BGP EVPN Route Type 2, Type 3/4 and Route Type 5 for the overlay control plane	The switch should support BGP EVPN Route Type 2, Type 3/4 and Route Type 5 for the overlay control plane
356	340-343	Annexure-VI/Specification-Spine Switch	The switch should support minimum 20k multicast routes	The switch should support minimum 7k multicast routes	The switch should support minimum 7k multicast routes
357	340-343	Annexure-VI/Specification-Spine Switch	The switch should support minimum 400K IPv4 Longest Prefix Match routes	The switch should support minimum 130K IPv4 Longest Prefix Match routes	As per RFP
358	Spine Switch/13	Spine Switch/13	Switch should support a minimum of 12 Tbps Bandwidth	Switch should support a minimum of 6.4 Tbps Bandwidth	As per RFP
359	Spine Switch/14	Spine Switch/14	Device should be based on simple and intelligent shared-memory buffered architecture that simplifies the system buffer management and queuing implementation.	Please remove	Device should be based on simple and intelligent shared-memory buffered architecture or equivalent that simplifies the system buffer management and queuing implementation.
360	Spine Switch/19	Spine Switch/19	Switch must provide the capability to be integrated with different Hypervisor Managers viz. Vmware vCenter, Microsoft Hyper-V with System Center, Kubernetes, Redhat Openshift and manage virtualise networking from the single pane of glass	Switch fabric must integrate with different virtual machine environment for centralised provisioning/mana gement.	Switch must provide the capability to be integrated with different Hypervisor Managers viz. Vmware vCenter/ Microsoft Hyper-V with System Center/ Kubernetes/ Redhat Openshift/ manage virtualise networking from the single pane of glass.
361	Spine Switch/38	Spine Switch/38	Switch in Spine-Leaf network fabric set up must provide the capability of micro-segmentation rules and policies for the Virtualized and Non - Virtualized environment (Bare metal and Container) workloads connected to DC fabric for east-west traffic. It must also support micro-segmentation based on VM attributes like hostname, OS, VM Tags, FQDN, Microsoft AD based classification	Fabric must support Segmentation for the Virtualize and Non - Virtualize environment via integration to orchestration layer	As per RFP
362	Spine Switch/44	Spine Switch/44	Per Flow Hop by Hop packet drop with reason of drop	Per Flow Hop by Hop packet drop with reason of drop	Per Flow Hop by Hop packet drop
363	432-433	Specification-Tape Library	2x16 Gb FC port per drive with transceivers required if any Should support backup server FC HBA	2x8 Gb FC port per drive with transceivers required if any Should support backup server FC HBA	As per RFP
364	432-433	Specification-Tape Library	Should be capable of supporting both FH and HH drives	Should be capable of supporting FH/ HH drives	Should be capable of supporting both FH / HH drives

365		UPS specification	The bidder shall provide 04 Nos. online UPS with isolation transformer to UPCL as per tender specification. Two online UPS shall be provided without battery bank and two online UPS with battery bank. The successful bidder shall commission online UPS with battery bank in UPCL Data Center, Dehradun and dismantle 2 nos. existing battery bank of 160 KVA UPS (240nos. X 2Volt X 300 AH), transport and commission these batteries in Disaster Recovery Center, Haldwani with two new UPS supplied without batteries. The battery bank capacity of independent new UPS for Data Center Dehradun should not be less than the existing battery sizing i.e. (240nos. X 2Volt X 300 AH). The new battery bank should be built with 2 Volt battery cells. The cost of dismantling and safe transportation of battery bank with necessary insurance shall be borne by the bidder.	161	As per RFP
366	48		Hardware Technical specifications Annexure-VI Specification- Web Application Firewall New Clause Request	The proposed hardware should be stable and reliable to address current requirement for such critical infra, EAL2 certification ensure the same. Major OEM along with some Make In India OEM as well have this certification. There are other components as well in this RFP where EAL certification is asked. Suggested Clause: The proposed hardware/software should be EAL2 certified.	New clause added: The proposed hardware/software should be EAL2 certified.
367	350 of 479		Specification- Web Application Firewall 5. Traffic Ports support: 4 x 10 GE SFP+, 4 x 1GE SFP and 4 x 1G Copper from day-1 Device L4 Throughput: 20 Gbps and scalable upto 40 Gbps Layer 4 connections per second: 500,000 Layer 7 requests per second: 900,000 RSA CPS(2K Key): 20,000 ECC CPS (EC-P256): 12,000 with TLS1.3 Support Processor: Intel 12-core CPU Concurrent Connections: 40 Million The appliance should have dedicated 2 x 10/100/1000 Copper Ethernet Out-of-band Management Port and RJ45 Console Port * Data should be publically available	Please change the port count as SFP+ can support both 1gig or 10gig fiber. Please change the concurrent connecttion as it will limit other reputed OEM's to participate. Please change to 1 x 10/100/1000 Copper Ethernet Out-of-band Management Port as its specific to one OEM. Kindly modify clause as" 5. Traffic Ports support: 4 x 10 GE SFP+ and 4 x 1G Copper from day-1 Device L4 Throughput: 20 Gbps and scalable upto 40 Gbps Layer 4 connections per second: 500,000 Layer 7 requests per second: 900,000 RSA CPS(2K Key): 20,000 ECC CPS (EC-P256): 12,000 with TLS1.3 Support Processor: Intel 12-core CPU Concurrent Connections: 38 Million The appliance should have dedicated 1 x 10/100/1000 Copper Ethernet Out-of-band Management Port and RJ45 Console Port * Data should be publically available"	As per RFP

368	351 of 479		Specification- Web Application Firewall 15. The proposed Solution should have NSS Lab recommended, ICSA Certified and PCI Compliant WAF on the same Hardware from the same OEM. It must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification.	NSS Lab already close, kindly asked EAL2/NdcPP certification. https://nsslabs.com/ NSS Labs ceased operations on October 15, 2020. CyberRatings.org has since reached an agreement with the custodians of NSS Labs to acquire the assets of their library. Kindly modify clause as" 15. The proposed Solution should have NSS Lab recommended or NDcPP certified, ICSA Certified and PCI Compliant WAF on the same Hardware from the same OEM. It must be able to handle OWASP Top 10 attacks or WASC Web Security Attack Classification. "	"The proposed Solution should have NSS Lab recommended or EAL2 or NDCPP, ICSA Certified and PCI Compliant WAF on the same Hardware from the same OEM. It must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification"
369	351 of 479		Specification- Web Application Firewall 9. "The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. It should NOT use Open Source/3rd party Network Functions. The proposed appliance should have capability to run in Virtualized as well as Standalone mode (Bidder may be asked to demonstrate this feature during Technical Evaluation). Each Virtual Instance contains a complete and separated environment of the Following: a) Resources, b) Configurations, c) Management, d) Operating System The proposed device should support 5 Virtual Instance from Day 1 and scalable upto 10 Virtual Instances. "	Please change virtual instance from 5 to 2 as it's a small appliance which can support up to 4 virtual stance from day one. Kindly modify clause as" 9. "The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. It should NOT use Open Source/3rd party Network Functions. The proposed appliance should have capability to run in Virtualized as well as Standalone mode (Bidder may be asked to demonstrate this feature during Technical Evaluation). Each Virtual Instance contains a complete and separated environment of the Following: a) Resources, b) Configurations, c) Management, d) Operating System The proposed device should support 2 Virtual Instance from Day 1 and scalable upto 4 Virtual Instances."	As per RFP
370	352 of 479		Specification- Web Application Firewall 22. Auto Policy Optimization a • Known Types of Attack Protection - Rapid Mode b • Security Filter Auto Policy Generation a) Full Auto b) Auto Enabled c) Auto Refinements c • Working in Learn Mode d • Auto Discovery e • Web Crawler	Please change Equivalent feature as mentioned Mode is specific to one OEM. Kindly modify clause as" 22. Auto Policy Optimization a • Known Types of Attack Protection - Rapid Mode or Equivalent b • Security Filter Auto Policy Generation a) Full Auto b) Auto Enabled c) Auto Refinements or Equivalent c • Working in Learn Mode d • Auto Discovery e • Web Crawler	Specification- Web Application Firewall 22. Auto Policy Optimization a • Known Types of Attack Protection - Rapid Mode or equivalent b • Security Filter Auto Policy Generation a) Full Auto b) Auto Enabled c) Auto Refinements or equivalent c • Working in Learn Mode d • Auto Discovery e • Web Crawler

371	Page 44	OEM should have TAC & R&D facility in INDIA. OEM should be present in India from last 10 Years.	Page 44 / Specification- Web Application Firewall / point no 1	We Haltdos were established eight years back , hence we cant have R&D and TAC of 10 years longivity. Please reduce it to make us participate on this.	As per RFP
372	Page 45	Suggestive clause	Page 45 / Web Application Firewall (WAF)	As the solution is going to integrate with service mesh environment, we assume that some of the applications are going to be API first applications. In order to adequately protect APIs from Layer 7 DDoS attacks without impacting API queries from legitimate users, we recommend to add the following clause in WAF. Suggestive Clause The solution should support Built-in API gateway for authentication, rate limiting, transformation, documentation and discovery from same OEM for additional layer of security against attacks targeting API infrastructure.	As per RFP
373	Page 45	Suggestive clause	Page 45 / Web Application Firewall (WAF)	Bot attacks are one of the fastest growing attacks on web applications. Advanced bots are capable in solving captcha and can result in creating disruption to web applications. We recommend the addition of the following clause to provide protection against Bot attacks: Suggestive Clause The solution should have advanced Anti-Bot capabilities to detect and block advanced AI bots including deception capability to implant decoys (fake links and forms) in any application without any changes to application or client.	As per RFP
374	Page 45	Suggestive clause	Page 45 / Web Application Firewall (WAF)	Company want to integrate the threat feed from other resources to protect the organsation and infra as well. We recommend to add the following clause in WAF. Suggestive Clause The proposed solution should have 3rd party threat feed integration to allow bulk IP blacklisting using API, FTP and schedule task etc.	As per RFP

375	Page 45	Suggestive clause	Page 45 / Web Application Firewall (WAF)	Web applications that support file upload are left vulnerable if these files are not inspected against Sandboxing or AV scan. We recommend the addition of the following clause: Suggestive Clause The solution should enforce file upload restrictions based on file extension, file size and support scanning file against built-in AV scanning engine as well as have option to support external Sandboxing / AV engine.	As per RFP
376		Web Application firewall/Point 15	The proposed Solution should have NSS Lab recommended, ICSA Certified and PCI Compliant WAF on the same Hardware from the same OEM. It must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification.	For OEM wider participation, it suggested to amend the clause "The proposed Solution should have NSS Lab recommended/ICSA Certified/PCI Compliant WAF on the same Hardware from the same OEM. It must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification"]	"The proposed Solution should have NSS Lab recommended or EAL2 or NDCPP, ICSA Certified and PCI Compliant WAF on the same Hardware from the same OEM. It must be able to handle OWASP Top 10 attacks and WASC Web Security Attack Classification"
377		Web Application firewall/ Point 11	The solution should support IPv6 as well as IPv4 and have the ability to turn IPv4 traffic to IPv6 traffic on the backend	The IPv6 Ready Logo will indicate that a product has successfully satisfied strong requirements stated by the IPv6 Logo Committee. The IPv6 Ready Core Logo expands the "core IPv6 protocols" test coverage to approximately 450 tests and adds new extended test categories. It is suggested to amend the clause as "The solution should support IPv6 as well as IPv4 and have the ability to turn IPv4/IPv6 traffic to IPv6/IPv4 traffic on the backend and the solution should be IPv6 ready logo certified from the day 1 and OEM should be listed vendor for ipv6 phase-2 certification".	As per RFP

378		Web Application firewall/ Point 5	Traffic Ports support: 4 x 10 GE SFP+, 4 x 1GE SFP and 4 x 1G Copper from day-1 Device L4 Throughput: 20 Gbps and scalable up to 40 Gbps Layer 4 connections per second: 500,000 Layer 7 requests per second: 9,00,000 RSA CPS(2K Key): 20,000 ECC CPS (EC- P256): 12,000 with TLS1.3 Support Processor: Intel 12-core CPU or equivalent or better Concurrent Connections: 40 Million The appliance should have dedicated 2 x 10/100/1000 Copper Ethernet Out-of-band Management Port and RJ45 Console Port * Data should be publically available	Traffic Ports support: As per the present datacentre/It infra requirement standard, 10G ports are recommended over 1G, As 10G is backward-compatible with 1G where as vies-versa is not possible. And for load balancer deployment 8 x 10G is more than sufficient because asked throughput is 40G.please amend this clause. Layer 4 connections per second: Considering the asked Concurrent Connections and Layer 4 connections per second requirement is lower side. please amend this clause. Layer 7 requests per second: Considering the asked Concurrent Connections and Layer 7 requests per second requirement is lower side. please amend this clause. RSA CPS(2K Key) and ECC CPS (EC-P256) : SSL parameters are very low and not as per industry standard, as now days 100 % internet traffic is SSL based. please amend this clause. Addition Point :- In the appliance will be running multiple functions,we recommended to add of 4 TB Storage on the appliance to cater to logging and reporting functions for multiple modules It is suggested to amend the clause as :- The proposed appliance	As per RFP
379		Web Application firewall/ Point 21	WAF should support for IPv4 and IPv6 traffic along with DNS functionality from day-1	DNS must be capable of handling complete Full DNS bind records including A, MX, AAAA, CNAME, PTR, and SOA. It suggested to amend the clause as "WAF should support for IPv4 and IPv6 traffic along and advance functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSEC, DNS DDOS, application load balancing from day one. It should be capable of handling complete Full DNS bind records including A,MX, AAAA, CNAME, PTR, SOA etc"	As per RFP

380				should be a dedicated appliance with dual power supply, it should not be part of any Firewall or UTM Traffic Ports support: 8 x 10 GE SFP+ from day-1 Device L4 Throughput: 20 Gbps and scalable up to 40 Gbps Layer 4 connections per second: 4 Million Layer 7 requests per second: 8 Million RSA CPS(2K Key): 40 K ECC CPS (EC-P256): 35 K with TLS1.3 Support Processor: Intel 12-core CPU or equivalent or better Concurrent Connections: 40 Million HDD - 4 TB The appliance should have dedicated 2 x 10/100/1000 Copper Ethernet Out-of-band Management Port and RJ45/DB9 Console Port * Data should be publically available	As per RFP
381				TB Storage on the appliance to cater to logging and reporting functions for multiple modules It is suggested to amend the clause as :- The proposed appliance should be a dedicated appliance with dual power supply, it should not be part of any Firewall or UTM Traffic Ports support: 8 x 10 GE SFP+ from day-1 Device L4 Throughput: 20 Gbps and scalable up to 40 Gbps Layer 4 connections per second: 4 Million Layer 7 requests per second: 8 Million RSA CPS(2K Key): 40 K ECC CPS (EC-P256): 35 K with TLS1.3 Support Processor: Multi-core CPU Concurrent Connections: 40 Million HDD - 4 TB The appliance should have dedicated 2 x 10/100/1000 Copper Ethernet Out-of-band Management Port and RJ45/DB9 Console Port * Data should be publically available	As per RFP
382	96	96	Specification-Web Security	We would like UPCL to confirm whether they are looking for an on-premise proxy or cloud based proxy. It seems to favor a specific OEM and a mix of both cloud based as well as cloud based proxy have provided.	As per RFP
383	97	97	Solution on-premises shall not be a hardware appliance offering		Accepted Bidders can propose either Hardware or Software based solution meeting the overall functional scope.

384	97	97	Solution shall be capable to block malicious website by "web category". Minimum requirement of category must include: Ransomware, Phishing, Scam, Spam, C&C, Disease Vector (known malware website) and Insecure IOT connections (IoT botnet detection).		As per RFP
385	97	97	Solution shall be capable to block malicious website by "web category". Minimum requirement of category must include: Ransomware, Phishing, Scam, Spam, C&C, Disease Vector (known malware website) and Insecure IOT connections (IoT botnet detection).		Deleted
386	97	97	Solution shall be capable to block malicious website by "web category". Minimum requirement of category must include: Ransomware, Phishing, Scam, Spam, C&C, Disease Vector (known malware website) and Insecure IOT connections (IoT botnet detection).		Deleted
387	97	97	Solution shall be capable to detect and block unknown (not pattern based) malware in real time according to its machine- learning security service. Detection period per file (<10MBytes) shall be detected within 2 seconds. Must support Windows PE file. The suspicious file can be blocked according to the result in 1st connection.		As per RFP
388	97		Solution shall be capable to detect and block unknown (not pattern based) malware in real time according to its machine-learning security service. 1. Detection period per file (<10MBytes) shall be detected within 2 seconds. 2. Must support Windows PE file. 3. The suspicious file can be blocked according to the result in 1st connection.	Only a specific vendor does this hence requesting change to allow more vendors Revised Clause:Solution shall be capable to detect and block unknown (not pattern based) malware in real time according to its machine-learning security service	Solution shall be capable to detect and block unknown (not pattern based) malware in real time according to its machine-learning security service
389	97		Solution shall be capable to detect known malware. 1. File size shall be supported up to 2GBytes. 2. For anti-malware engine and pattern, Vendor shall provide its backend service in case it provided with 3rd party vendor. Must include one of anti-malware vendors: Trend Micro, [others]. 3. No addtional fees to use above anti-malware engines, services, and patterns. 4. Open-source Anti-malware patterns, services, or engines must not be included.	Requesting change to remove the vendor specific name Revised Clause:Solution shall be capable to detect known malware. 1. File size shall be supported up to 2GBytes. 2. For anti-malware engine and pattern, Vendor shall provide its backend service in case it provided with 3rd party vendor. Must include two anti-malware vendors 3. No additional fees to use above anti-malware engines, services, and patterns. 4. Open-source Anti-malware patterns, services, or engines must not be included.	Solution shall be capable to detect known malware. 1. File size shall be supported up to 2GBytes. 2. For anti-malware engine and pattern, Vendor shall provide its backend service in case it provided with 3rd party vendor. Must include two anti-malware vendors 3. No additional fees to use above anti-malware engines, services, and patterns. 4. Open-source Anti-malware patterns, services, or engines must not be included.

390	97	97	Solution shall be capable to send suspicious files to cloud based sandbox for further analysis. Must support below filetype: Windows PE, Microsoft Office.	We would like to draw your attention to "Specification-External Firewall with Anti APT Device" on page 28 clause 58 . The specifications mentioned under this section asks bidder to provide protection against spam and as well as sandboxing of email and web. This clause is redundant and we would request you to delete the clause.	As per RFP
391	97		Solution shall be capable to send suspicious files to cloud based sandbox for further analysis. Must support below filetype: Windows PE, Microsoft Office.	For all the solutions in RFP sandbox has been asked as on prem thus requesting to change. Revised Clause:Solution shall be capable to integrate with onprem anti apt sandbox for further analysis. Must support below filetype: Windows PE, Microsoft Office.	Solution shall be capable to integrate with onprem anti apt sandbox for further analysis. Must support below filetype: Windows PE, Microsoft Office.
392	98	98	Solution must support "application control". Minimum numbers of application shall be at least supporting 700 applications.		As per Solution proposed by SI
393	98	98	Solution must support "business cloud application access control". Minimum numbers of cloud application shall be at least supporting 25,000 (25K).		As per Solution proposed by SI
394	98		Solution must support "business cloud application access control". Minimum numbers of cloud application shall be at least supporting 25,000 (25K).	The number of application is a dynamic attribute hence requesting change Revised Clause:Solution must support "business cloud application access control".	Solution must support "business cloud application access control".
395	98		Solution shall be capable to detect and block content by true filetype as user/group policy. 1. Must support action by policy. 2. Must support below true filetype: EPS, CHM, GZ, RAR, SIT, TAR, ZIP, AIF, FLV, M4A, MID, MOV, MP4, MP3, RA/RM, SWF, WAV, AVI, ASF, COM, DLL, EXE, LNK, MSI, BMP, GIF, JPG, PNG, PSD, PSP, TIF, DOC/X, ODT, PDF, PPT/X, WPD, XLS/X	Requesting change to remove the vendor specific file types Revised Clause: Solution shall be capable to detect and block content by true filetype as user/group policy. 1. Must support action by policy. 2. Support for filetype like: EPS, CHM, GZ, RAR, SIT, TAR, ZIP, AIF, FLV, M4A, MID, MOV, MP4, MP3, SWF, WAV, AVI, DLL, EXE, LNK, MSI, BMP, GIF, JPG, PNG, PSD, TIF, DOC/X, ODT, PDF, PPT/X, WPD, XLS/X	Solution shall be capable to detect and block content by true filetype as user/group policy. 1. Must support action by policy. 2. Support for filetype like: EPS, CHM, GZ, RAR, SIT, TAR, ZIP, AIF, FLV, M4A, MID, MOV, MP4, MP3, SWF, WAV, AVI, DLL, EXE, LNK, MSI, BMP, GIF, JPG, PNG, PSD, TIF, DOC/X, ODT, PDF, PPT/X, WPD, XLS/X
396	99	99	Solution shall be capable to manage all policy over cloud and on- premises proxy in one console. The management of policy shall be performed via GUI based managemental console must not be performed as command based (e.g. CLI, SSH)		Deleted
397	99	99	Solution shall be capable to manage all policy over cloud and on- premises proxy in one console. The management of policy shall be performed via GUI based managemental console must not be performed as command based (e.g. CLI, SSH)		SI can propose either Hardware or Software based solution meeting the overall functional scope.

398	100		Solution on-premise proxy shall be capable to let customer installed as below platform: 1. Any patform which are compatible Redhat Enterprise 7.x or CentOS 7.x 2. Hardware baremetal, Virtualized platform (VMWare, HyperV, KVM), Microsoft Azure and Amazon AWS.	All components are asked as on on-prem thus this should also be an onprem appliance. Hence requesting change Revised Clause:Solution on-premises shall be a hardware appliance offering deployed as on-prem appliance	The solution either Hardware or Software based solution meeting the overall functional scope and integrate natively with existing running web security solution having common management platform safeguardding investment made by UPCL.
399	100	38	Solution shall be capable to provide cloud (hosted) proxy and on- premises proxy		SI can propose either Hardware or Software based solution meeting the overall functional scope.
400	76		The vendor shall have 30 year's experience in enterprise data security and cybersecurity solutions	Specific to an OEM appliance,kindly remove this clause.	The vendor shall have 10 year's experience in enterprise data security and cybersecurity solutions
401	379		XDR	As per RFP you have asked for XDR capability which is need of the hour to protect UKPCL ecosystem holisticaly from sophisticated cyber threats by providing detection, Mitigation and investigation capability but as per our understanding defined function is lacking few capabilities which should be part of you XDR platform. Hence it is our humble request to incorporate our below suggestion. 1. Proposed and exsiting security layers including Endpoint Security, HIPS, Anti APT and NIPS, Web Security, Email Security , SIEM and SOAR should integrate create a native data lake by ingesting activity & telemetry data from all sensors to achieve comprehensive protection by capabilities including risk score, risk index, Vulnerability and risk prioritization, Suspicious object management, Campaign intelligence, Internal and External Attack Surface Discovery, Observed Attack Techniques, MITRE ATT&CK mapping, Workflow Automation having common threat sharing and management platform. 2. The solution should provide a drill down view of a different set of risk factors contributing to events that are triggered over a period of time which can be quickly utilized by SOC team for mitigation efforts. a. Discovered highly exploitable vulnerabilities, b. Behaviour Events (User, Device, and Network),c. Detected XDR and Threat events (Endpoint, Web, Network, Email and mobile), d. Accessed cloud apps/URLs, d. System misconfigurations 3. The solution should consider the risk score of each internal asset (device) from different parameters combined with leading AI/ML techniques to calculate the most accurate risk score including : User	As per RFP
402	Page 76	Specification-XDR -> 20	Services scope should deliver with skilled resources and expertise to deliver Managed XDR Services	Requesting to consider the suggestion and make the changes to exisitng technical statement for maximum participation in the RFP. Recommended Statement- Services scope should deliver with skilled resources and expertise to deliver Managed XDR Services by service provider or OEM.	As per RFP

403	Page 76	Specification-XDR -> 15	The OEM Data center should be in India region for the provisioned SaaS XDR services and the telemetry should always stay within the data center and the region to meet data sovereignty and data privacy concerns.	Since , OEM and SI are both responsible for data secuirty and sovereignity, we would request to amend this clause to below The OEM/Bidder Data center should be in India region for the provisioned SaaS XDR services and the telemetry should always stay within the data center and the region to meet data sovereignty and data privacy concerns.	As per RFP
404	Page 76	Specification-XDR -> 17	The proposed OEM must be in Leader Quadrant "Gartner Endpoint Protection Platform in a recently published report "	This statement needs to be removed as Indian government does not promote Gartner leader quandrant clause. As per the Indian gov. circular dated 30th Sep. 2022. Reference Link-https://dot.gov.in/sites/default/files/Circulation%20of%20important%20OMs%20and%20amendments%20regarding%20GFRs-2017%20dated%2026-09-2022.pdf?download=1	As per RFP
405	Page 77	Specification-XDR -> 34	The vendor is highly recognized by Gartner, Forrester, AV-TEST, NSS Labs etc.	This statement needs to be removed as Indian government does not promote Gartner clause or any other third-party vendor evaluations. As per the Indian gov. circular dated 30th Sep. 2022. Reference Link-https://dot.gov.in/sites/default/files/Circulation%20of%20important%20OMs%20and%20amendments%20regarding%20GFRs-2017%20dated%2026-09-2022.pdf?download=1	As per RFP
406	54	54	Specification-SSL VPN Zero Trust Network Access (ZTNA)		Requirement shall be as per solution proposed by SI
407	54	54	Specification-SSL VPN Zero Trust Network Access (ZTNA)		Requirement shall be as per solution proposed by SI
408	54	54	Specification-SSL VPN Zero Trust Network Access (ZTNA)		Requirement shall be as per solution proposed by SI
409	55		The proposed ZTNA solution OEM should be a Leader in Gartner Security Service Edge (SSE) Magic Quadrant 2023 or latest.	Requesting change for wider participation. Revised Clause:The proposed ZTNA solution OEM should be a Leader/Challenger in Gartner Security Service Edge (SSE) Magic Quadrant 2023 or latest.	As per RFP
410	55	SSL VPN Zero Trust Network Access (ZTNA) 10	The proposed ZTNA solution OEM should be a Leader in Gartner Security Service Edge (SSE) Magic Quadrant 2023 or latest.	We hereby request to consider removing this point	As per RFP
411	55	55	The proposed ZTNA solution OEM should be a Leader in Gartner Security Service Edge (SSE) Magic Quadrant 2023 or latest.		As per RFP
412	55	SSL VPN Zero Trust Network Access (ZTNA) 11	The proposed ZTNA Solution should have DEM (Digital Experience Management) functionalities active for all users from Day 1	We hereby request to consider removing this point	As per RFP
413	55	55	The proposed ZTNA Solution should have DEM (Digital Experience Management) functionalities active for all users from Day 1		Yes

414	55		The ZTNA solution admin console access must be able to restricted from known customer IP locations only to ensure authorised access.	Specific to an OEM appliance, Kindly remove this clause.	As per RFP
415	55	55	The ZTNA solution must be able to integrate with SAML 2.0		As per RFP (Requirement shall be as per solution proposed by SI)
416	55	55	The ZTNA solution must have 99.999% uptime backed by SLA.		The ZTNA solution must have 99.99% uptime backed by SLA.
417	55		The ZTNA solution must have in-built data retention of atleast 90 days from day 1. The Admin should be able to view all end user activity logs for last 90 Day transactions on the Admin Console. The Solution must be able to integrate with SIEM for future log retention.	Specific to an OEM appliance, hence requesting change for wider participation. Revised Clause:The ZTNA solution must have in-built data retention of at least 30 days from day 1. The Admin should be able to view all end user activity logs for last 30 Day transactions on the Admin Console. The Solution must be able to integrate with SIEM for future log retention.	The ZTNA solution must have in-built data retention of atleast 30 days from day 1. The Admin should be able to view all end user activity logs for last 30 Day transactions on the Admin Console. The Solution must be able to integrate with SIEM for future log retention of at least 90 days log.
418	55	SSL VPN Zero Trust Network Access (ZTNA) 5	The ZTNA solution should have ZTNA and Digital Experience Management (DEM) from Day 1 using the same Endpoint Agent and single management console for both capabilities.	We hereby request to consider removing this point	As per the proposed solution by SI
419	56		Any component installed in DC's (On-premise or IaaS) must not need any inbound ACL rule in customer DC/DR Firewall to provide access to Private Application.	This doesn't change any functional aspect different OEM have different deployment architecture hence requesting change. Revised Clause:Any component installed in DC's (On-premise or IaaS) must provide access to Private Application.	As per RFP
420	56	56	Any component installed in DC's (On-premise or IaaS) must not need any inbound ACL rule in customer DC/DR Firewall to provide access to Private Application.		As per RFP
421	56		The Endpoint agent (less than 50 MB in size) must be tamper proof and users should not be able to disable or uninstall the Client even with System Admin Right. Any application policy change on the Admin UI should reflect near real-time on the users.	This doesn't change any functional aspect different OEM have different deployment architecture hence requesting change. Revised Clause:The Endpoint agent must be tamper proof and users should not be able to disable or uninstall the Client even with System Admin Right. Any application policy change on the Admin UI should reflect near real-time on the users.	The Endpoint agent must be tamper proof and users should not be able to disable or uninstall the Client even with System Admin Right. Any application policy change on the Admin UI should reflect near real-time on the users.
422	56	SSL VPN Zero Trust Network Access (ZTNA) 12	The proposed solution must be certified with CSA STAR, CIS, FedRamp, ISO 27001, ISO 27017, ISO 27018, and TrustARC certification	We hereby request to consider this point " The proposed solution must be certified with any of CSA STAR, CIS, FedRamp, ISO 27001, ISO 27017, ISO 27018, or TrustARC certification"	As per RFP
423	56		The proposed solution must be certified with CSA STAR, CIS, FedRamp, ISO 27001, ISO 27017, ISO 27018, and TrustARC certification	Requesting change for wider participation. Revised Clause:The proposed solution must be certified with certification bodies like CSA STAR, CIS, FedRamp, ISO 27001, ISO 27017, ISO 27018, and TrustARC certification	As per RFP

424	56		The Solution should have the capability to authenticate users and enrol/log in to the service using their Email Address. This capability should not need any SAML/SSO Integration and admin should be able to send invite links to the user's email to enable this functionality.	Specific to an OEM , hence requesting change for wider participation. Revised Clause:The Solution should have the capability to authenticate users and enrol/log in to the service using their Username/Email Address	The Solution should have the capability to authenticate users (internal and external/third party) and enrol/log/register using their Email Address. This capability should not need any SAML/SSO Integration and admin should be able to send invite links to the user's email to enable this functionality.
425	57	57	The End point Agent should support multi-user mode installation (for ex. Installing agent on VDI/Thin Clients)		As per RFP Requirement shall be as per solution proposed by SI
426	57		The End-user should not be able to see the Application Local IP even if they are authorised to access the application (application access based on FQDN but real Application IP is masked)	Specific to an OEM , hence requesting change for wider participation. Revised Clause:The End-user should have a same experience when accessing private app's, SaaS or Internet	As per RFP
427	57	SSL VPN Zero Trust Network Access (ZTNA) 24	The ZTNA solution must be able to provide clientless Browser based access to Internal Web Applications from Day 1. It should also support the capability to enforce DLP policies on the acces to Internal Web Applications	We hereby request to consider removing this point	As per RFP
428		SSL VPN Zero Trust Network Access (ZTNA)		We hereby request to consider the point" The solution should be able to verify the devices using the same agent that it runs necessary compliance policies like 1)Active AV with recent signature updates,firewalls 2) Necessary security policies / services protecting endpoints 3) No vulnerable applications running 4) Disk encryption service is on 5) Recommended OS system version etc.	The new point added : "The ZTNA solution must enforce device posture validation across multiple parameters like Device Encryption, Registry Check, Process Check, AD Domain Check, and Certificates etc to provide specific Application Access based on this. The device posture check should be recurring and check the compliance of the posture every 10 mins or less or configurable to maintain the Device Trust."