REQUEST FOR QUOTATION

MMI:PU:RF:003

BHARAT HEAVY ELECTRICALS LIMITED
Electronics Division
PB No. 2606, Mysore Road Bangalore - 560026
INDIA

RFQ NUMBER: SAKMRCH014

RFQ DATE : [redacted]

Due Date/Day: [redacted]
Time : [redacted]
Tender Box : Reception Area
Opening Venue:
NEW ENGG. BLDG

(address for communication) :

(for all correspondence)
Purchase Executive : Santosh Kumar
Phone : 8004939865
Fax :
E-mail: kumar.santosh@bhel.in

Sl No.	Description	Qty	Unit	Delivery qty	Delivery Date
1	ED7470497013 Network Security Firewall-Type-1 * HSN/SAC : Network Security Firewall-Type-1 (IPS &IDS) as per Clause 2 Sl no.1 of Purchase specification PS4042971	40	ST	40	[redacted]
2	ED7470497021 Network Security Firewall-Type-2 * HSN/SAC : Network Security Firewall-Type-2 (IPS &IDS) as per Clause 2 Sl no.2 of Purchase specification PS4042971	40	ST	40	[redacted]
3	ED7470497030 Network Security Firewall-Type-3\ * HSN/SAC : Network Security Firewall-Type-3 as per Clause 2 Sl no.3 of Purchase specification PS4042971	20	ST	20	[redacted]
4	ED7470497048 Network Management Software * HSN/SAC : Network Management Software as per Clause 2 Sl no.4 of Purchase specification PS4042971	20	ST	20	[redacted]
5	ED7470497056 Security Event Manger * HSN/SAC : Security Event Manger as per Clause 2 Sl no.5 of Purchase specification PS4042971	20	ST	20	[redacted]
	ED7470497064 Syslog server Software	20	ST	20	[redacted]

TWO PART BID - SUBMIT TECHNICAL AND PRICE BID IN SEPARATE SEALED COVERS

NOTES:
1. This RFQ is governed by:
a) INSTRUCTIONS TO BIDDERS/SELLERS and GENERAL CONDITIONS OF CONTRACT FOR PURCHASE available at **http://edn.bhel.com (RFQ-PO Terms & Conditions)**
b) Any other specific Terms and Conditions mentioned.
2. Bidders / Representatives who would like to be present during opening of offers are required to furnish authorization letter for the same.
* The HSN/SAC no mentioned against the line items in the RFQ are indicative only.

For and On behalf of BHEL.

Santosh Kumar
Control Equipment

REQUEST FOR QUOTATION

MMI:PU:RF:003

BHARAT HEAVY ELECTRICALS LIMITED
Electronics Division
PB No. 2606, Mysore Road Bangalore - 560026
INDIA

RFQ NUMBER: SAKMRCH014

RFQ DATE : [redacted]

Due Date/Day: [redacted]
Time : [redacted]
Tender Box : Reception Area
Opening Venue:
NEW ENGG. BLDG

(address for communication) :

(for all correspondence)
Purchase Executive : Santosh Kumar
Phone : 8004939865
Fax :
E-mail: kumar.santosh@bhel.in

Sl No.	Description	Qty	Unit	Delivery qty	Delivery Date
6	* HSN/SAC : Syslog server Software as per Clause 2 Sl no.6 of Purchase specification PS4042971				
7	ED7470497072 Network attached Storage * HSN/SAC : Network attached Storage as per Clause 2 Sl no.7 of Purchase specification PS4042971	10	ST	10	[redacted]
8	ED7470497080 Cybersecurity Accessories * HSN/SAC : Cybersecurity Accessories as per Clause 2 Sl no.8 of Purchase specification PS4042971	20	ST	20	[redacted]

Total Number of Items - 8

1.
2.

TWO PART BID - SUBMIT TECHNICAL AND PRICE BID IN SEPARATE SEALED COVERS

NOTES:
1. This RFQ is governed by:
a) INSTRUCTIONS TO BIDDERS/SELLERS and GENERAL CONDITIONS OF CONTRACT FOR PURCHASE available at **http://edn.bhel.com (RFQ-PO Terms & Conditions)**
b) Any other specific Terms and Conditions mentioned.
2. Bidders / Representatives who would like to be present during opening of offers are required to furnish authorization letter for the same.
* The HSN/SAC no mentioned against the line items in the RFQ are indicative only.

For and On behalf of BHEL.

Santosh Kumar
Control Equipment

PURCHASE SPECIFICATION
for
DCS Cybersecurity Suite
Project: Multiple

REVISON HISTORY SHEET

REV NO.	DATE	NATURE OF CHANGE	REASON
00	10.10.2025	FIRST ISSUE	----

1. General

This purchase specification has been prepared to define the technical, functional, and security requirements for network components and solutions used for securing OT layered network. The objective of this document is to ensure that all proposed solutions comply with regulatory standards, and industry best practices for securing OT & IT environments. Suppliers are required to adhere to the specifications outlined herein to ensure compatibility, scalability, reliability, and long-term support for the deployed solutions.

2. Material codes & Description

Table 1 - Bill of Materials

Sl	MATERIAL CODE	Description	Qty.
1	**ED7470497013**	*Network Security Firewall Type-1: Shall conform to the technical specifications detailed under Clauses 3A, 3AB1, and 3AB2.*	**As per Indent**
2	**ED7470497021**	*Network Security Firewall Type-2: Shall conform to the technical specifications detailed under Clauses 3A, 3AB1, and 3AB2.*	
3	**ED7470497030**	*Network Security Firewall Type-3: Shall conform to the technical specifications detailed under Clauses 3B& 3AB1.*	
4	**ED7470497048**	*Network Management Software: Shall conform to the technical specifications detailed under Clauses 3C*	
5	**ED7470497056**	*Security Event Manger Shall conform to the technical specifications detailed under Clauses 3D*	
6	**ED7470497064**	*Syslog server : Shall conform to the technical specifications detailed under Clauses 3E*	
7	**ED7470497072**	*Network attached Storage : Shall conform to the technical specifications detailed under Clauses 3F*	
8	**ED7470497080**	*Cyber Security Accessories: Shall conform to the technical specifications detailed under Clause 3G* *i. RJ45 Locking Plugs -100 Nos with 5 keys* *ii. USB Port Lock-30 Nos with 3 keys* *iii. BHEL ASTR Secured Hologram sticker-30 Nos*	

Note: Firewalls Type-1 and Type-2 should be from different makes.

Table 2 - Technical services

A	Technical Services to be provided at BHEL/EDN (refer clause 4.A)	

3. Technical Specifications

Sl. No.	Specifications	Compliances Yes/No
3A	**Network Security Firewall (Type-1 & Type-2) – IPS & IDS:** The Type-1 and Type-2 Firewalls shall be identical in technical specification but of different make, to ensure cybersecurity compliance requiring multiple vendor implementations. These firewalls will function as both Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).	
	- Next Generation Firewall (NGFW) with packet filtering, stateful and deep packet inspection.	
	- Support for High Availability & Load Balancing.	
	- Data encryption: 3DES, AES 128/192/256-bit.	
	- Support for NAT, PAT, and Policy-based NAT/PAT.	
	- Minimum 500,000 concurrent sessions.	
	- Minimum 20,000 new sessions per second	
	- Minimum firewall throughput: 4 Gbps.	
	- Minimum 3DES/AES VPN throughput: 400 Mbps.	
	- Capability to forward logs to external log repository servers.	
	- Minimum 8 Ethernet interfaces.	
	- Common Criteria Certification: Product or OS must have EAL4 / NDPP or higher certification (ISO/IEC 15408). Certification document to be submitted with offer.	
	- IPS/IDS must support host-based and network-based intrusion protection, threat protection, malware/botnet protection, and web/URL filtering.	
	- Firewall log repository: minimum one year.	
	- 1-year IDP and Anti-Virus subscription included.	
	- Makes: CISCO / CHECKPOINT / SOPHOS / FORTINET / PALO ALTO	
3B	**Network Security Firewall (Type-3)**	
	- Minimum 4 Ethernet ports.	
	- Minimum 150 Mbps firewall throughput.	
	- Minimum 40 Mbps IPS throughput.	
	- Minimum 50 Mbps VPN throughput.	
	- Minimum 25,000 concurrent sessions.	
	- Should be a Stateful Inspection Firewall.	
	- On-device reporting required.	
	- Support for IPv6.	

	- Support both Transparent and Gateway modes.	
	- Unrestricted user support.	
	- 1-year IDP, Antivirus, and Content Filtering subscription included.	
	- 19-inch rack-mountable design with necessary accessories.	
	- Makes: CISCO / CHECKPOINT / SOPHOS / FORTINET / PALO ALTO	
3AB1	**General Specifications of Network Security Firewall (Type-1,2 & 3)**	
	The firewall appliances shall support multi-vendor, multi-application environments and be compatible with third-party products. Active-Active configuration should be supported (except for Type-3).	
	- Support Stateful Inspection and NAT functionality (dynamic/static).	
	- Support latest SNMP version.	
	- Logs should be sent to a separate log server via encrypted connection without affecting performance.	
	- Remote administration access allowed only through secured administrative interface.	
	- Firewall administration station must push policies/configurations securely to individual or multiple firewalls.	
	- Both GUI and CLI should be provided, accessible through encrypted channels.	
	- All administrative changes and commands should be logged.	
	- No unencrypted access allowed to firewall.	
	- Comprehensive monitoring of all network traffic with detection of known and unknown threats via deep packet inspection, anomaly scanning, and behavior pattern analysis (zero-day protection).	
	- Up-to-date signature and vulnerability database maintenance	
3AB2	**IPS/ IDS FEATURES (Applicable toType-1 & Type-2):**	
	The Intrusion Detection and Prevention System (IDS/IPS) shall be capable of monitoring all inbound and outbound network traffic and identifying suspicious patterns that may indicate potential network or system attacks aimed at compromising the Station LAN Network. The proposed IDS/IPS solution shall incorporate the following combined features, configurable as either IDS or IPS mode as required.	
	- Analyze, detect, and report security-related events.	
	- Inspect and drop malicious traffic based on configured policies.	
	- Content inspection using signature-based detection.	
	- Prevent known attacks (worms, Trojans, hacks, DoS, DDoS).	
	- Monitor network behavior to prevent abnormal activities.	
	- Update regularly with new threats and vulnerabilities.	
	- Provide user-friendly interface for queries and reports.	
	- Maintain detailed logs for audit and analysis.	
	- Detect known threats through deep-packet inspection.	
	- Detect unknown threats via anomaly and behavior-based scanning (zero-day protection).	

Sl. No.	Specifications	Compliances Yes/No
3C	**Network Management Software** **(Free source software not acceptable)** The proposed Network Management Software shall provide centralized network administration, monitoring, and management capabilities for SNMP-enabled devices across the enterprise network. Free or open-source software shall not be acceptable. The offered product such as "WhatsUp Gold Network Management Software" or equivalent shall meet or exceed the following technical specifications.	
	Centralized administration of a network with various SNMP-enabled devices.	
	Real-time monitoring of network status and performance.	
	Support for up to 1000 managed IP nodes and minimum 100 device licenses preloaded from day one.	
	Automatic discovery and generation of network topology maps with periodic device polling.	
	Graphical presentation of real-time device status with automatic color changes to reflect device conditions.	
	Capability to monitor traffic flow through **at least 10** network devices.	
	Display device image showing active ports and installed modules; when a device is down, diagnostic tools such as Ping and Telnet shall be accessible directly from the interface.	
	Provide real-time activity, utilization statistics, and graphical trend analysis.	
	Monitor device status, port status, CPU utilization, memory utilization, and all port utilization including uplink ports.	
	Enable logical graphs of devices such as routers and web servers as per monitoring requirements.	
	Capability for configuration of multiple devices simultaneously.	
	Support client-server architecture allowing multiple concurrent logins from different locations.	
	Provide differentiated user access rights to define visibility and manageability by user domain.	
	Customizable trap messages with user-defined readable and meaningful information.	
	Support pre-defined actions such as email and SMS alerts upon any network event.	
	Include an MIB compiler for integration and compilation of third-party device MIBs.	
	Support for device panel simulation module.	
	Comprehensive reporting functions including collector configuration, collector and data analysis capabilities.	

Sl. No.	Specifications		Compliances Yes/No
3D	**Security Event Manager: Perpetual License** This specification covers the supply, installation, and commissioning of Security Event Manager (SEM) software for centralized log collection, correlation, and security incident management within the Powerplant OT infrastructure. The software shall provide real-time security event monitoring, automated incident response, and compliance reporting. SolarWinds Security Event Manager SEM30 (Perpetual License for up to 30 Nodes) or equivalent shall qualify		
	Product Type	Enterprise-grade Security Event Manager (SIEM) software	
	License Type	Perpetual License for up to 30 Nodes / Devices	
	Deployment Mode	Software or virtual appliance, deployable on Windows or Linux environment	
	Event Source Compatibility	Support syslog, SNMP traps, Windows event logs, firewalls, IDS/IPS, routers, switches, servers, antivirus, and application logs	
	Log Collection	Centralized collection of security and system logs from multiple heterogeneous devices	
	Log Retention	Minimum configurable retention of 365 days with archiving option	
	Correlation Engine	Real-time correlation and analysis of events across all connected nodes	
	Alerting	Automated alerting via email, SMS, or dashboard on detection of security anomalies	
	Incident Response Automation	Predefined and customizable automated actions on event detection (e.g., block IP, disable user, isolate host)	
	Dashboard	Web-based dashboard for live monitoring, trending, and investigation	
	Reporting	Built-in and customizable reports for ISO 27001, NIST, GDPR, HIPAA, PCI-DSS compliance	
	Integration	Integration with existing network and security devices via standard protocols (Syslog, SNMP, WMI, API)	
	Database	Embedded or external database supported ensuring high availability and data integrity	
	Security	TLS/SSL encryption, RBAC, and secure audit trails	
	Scalability	Support for minimum 30 nodes, scalable to higher node count by license upgrade	
	Backup and Restore	Facility to back up configuration and log data with restore functionality	
	Performance	Capable of handling at least 500 Events Per Second (EPS) sustained	
	User Management	Integration with Active Directory / LDAP	
	Updates and Maintenance	Regular signature updates, patches, and version	

	upgrades during warranty/support period	
	Manageability and User Interface • Web-based management interface accessible via standard browsers. • Configurable role-based dashboard and reporting views. • Multi-user concurrent access with administrator control. • Customizable rule-based alerts and correlation templates. • Exportable reports in CSV, PDF, or HTML format.	
	Installation and Configuration Vendor shall perform installation, initial configuration, and policy setup at BHEL premises. Integration with existing network devices and servers shall be demonstrated. All required licenses, activation keys, and documentation shall be handed over to BHEL HMI department.	
	Documentation and Deliverables *Vendor shall provide:* 1. Product datasheet and compliance certificates. 2. User, administrator, and installation manuals. 3. License certificate and key details. 4. Training for administrators on operation and reporting. 5. Backup and restore procedure documentation.	
	Warranty and Support Minimum 1 Years Comprehensive Support from OEM or authorized partner. Includes technical support, updates, and patch management. OEM shall ensure vulnerability patch releases and product updates throughout the support period.	
	Approved Makes / OEMs **SolarWinds / ManageEngine / Splunk / Fortinet / IBM QRadar / Rapid7 / LogRhythm / equivalent.** (Models equivalent or superior to SolarWinds Security Event Manager SEM30, Perpetual License for up to 30 Nodes, shall qualify.)	
	Delivery and Acceptance Supply, installation, and commissioning at BHEL EDN. Acceptance based on successful installation, configuration, and verification of licensed node connections and event logging.	

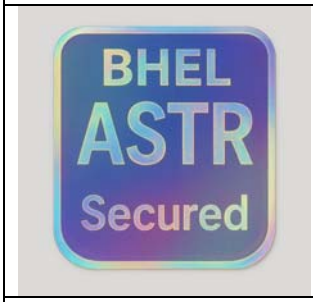
3E	**Syslog Server – Perpetual License**	
	Purpose & Scope: The purpose of this purchase is to acquire a centralized syslog server solution to collect, store, alert, forward and archive logs from network devices (routers, switches, firewalls), servers (Windows) and applications across the Process plant network. The solution will support both security monitoring and operational troubleshooting and meet regulatory/compliance requirements (e.g., audit log retention, archival).	
	• Collection of syslog messages (UDP/TCP, IPv4/IPv6) and SNMP traps.	
	• Collection of Windows Event logs (via forwarding) if required.	
	• Real-time alerting, filtering, log management actions (forwarding, scripts).	
	• Log archival and cleanup per retention policy.	
	• Web-based access for log viewing/searching/monitoring.	
	• Support for current and future log volume growth.	
	• Able to Store and archive logs to assist with regulatory compliance	
	• Should have UI with an intuitive dashboard	

Sl. No.	Specifications		Compliances Yes/No
3F	**Network Attached Storage** The Network Attached Storage (NAS) system shall be a high-performance, rack-mountable, multi-bay storage appliance designed for data backup, centralized file sharing, and secure storage applications. The NAS shall be compatible with standard data-center rack installations and suitable for 24x7 operation in enterprise environments		
	Parameter	Specification Requirements	
	Form Factor	• 2U rackmount chassis with 8 hot-swap 3.5″ drive bays.	
	Power Supply	Redundant hot-swap Power Supply Units (PSUs).	
	Processor	Intel Xeon class CPU, quad-core or higher. (Alternatively, enterprise-grade embedded processors are acceptable, including Intel Atom C5000/C3000 series (e.g., C5125, C5315, C3758 or higher) or AMD Ryzen Embedded V-series (e.g., V1500B, R1600 or	

		higher). These must be quad-core or above, designed for 24×7 NAS operation, and support hardware-accelerated encryption, RAID operations, and sustained 10GbE throughput.)	
	Memory (RAM)	32 GB DDR4 ECC RAM, upgradeable to minimum 64 GB.	
	RAID Support	RAID 1, 5,6 Support	
		Minimum 2 × NVMe M.2 slots for SSD cache/journal	
	Storage Drives -HDD	A. HDDs (Primary Storage) • 8 × 8 TB NAS/enterprise-grade CMR HDDs.(Hot Swappable) • Acceptable makes: Seagate IronWolf Pro / WD Red Pro / Toshiba Enterprise. • Configured in RAID6.	
	Storage Drives -SSDD	B. SSDs (Cache/Journal) • 2 × 1 TB NVMe enterprise-grade SSDs. • Used for cache/journal acceleration.	
	Network Interface	• Minimum 2 × 10 GbE SFP+ uplink ports. • Minimum 2 × 1 GbE management ports. • Support for link aggregation, VLAN tagging and jumbo frames	
	Operating System & Features	• Enterprise-grade NAS operating system. • Support for snapshots, block-level and file-level replication. • Support for SMB, NFS and iSCSI protocols. • Support for user access control, quota management and audit logs. • Online RAID expansion and rebuild management.	
	Reliability, Management & Monitoring	• Support for redundancy across PSU, fans and cooling. • SNMP support for integration with central NOC. • E-mail/SMS alerting for drive failure, temperature and power faults. • Local replication to secondary NAS within the same plant. • Support for offsite backup to remote NAS or cloud target.	
	Additional Requirements	Rackmount kit and all necessary cables. • Minimum 3-year warranty with onsite support. • Vendor must provide documentation,	

	installation and commissioning support.	
	Functional and Software Requirements 1. Manageability - Web-based management software for network, user, and storage administration. - Real-time storage and performance monitoring dashboard. - File Service Capacity Management (quota and usage monitoring). - Remote management and health monitoring tools - Vendor must provide detailed software feature list with the offer.	
	OS and Backup Compatibility - Client OS support: Windows 11, Windows 10 LTSC, Windows Server 2016 / 2019 / 2022. - Compatible with Veritas Backup Exec / Veritas System Recovery software. - Must automatically resume scheduled backup operations post-reboot (after power failure) without manual NAS login.	
	Installation and Commissioning Vendor shall perform on-site installation, configuration, and initial firmware update at BHEL site. All system parameters including RAID configuration and user shares shall be verified in the presence of BHEL HMI representative.	
	Documentation Vendor shall supply product datasheet, compliance certificates, manuals, factory test certificate, and warranty card.	
	Warranty and Support Minimum 3 Years Comprehensive On-Site Warranty covering all hardware and software components. OEM or Authorized Partner Support mandatory. Firmware updates and patches shall be provided free during warranty.	
	Approved Makes / OEMs **DELL / HP / IBM / LENOVO / BUFFALO / QNAP / SYNOLOGY / ASUSTOR or Equivalent**	

Sl. No.	**Specifications**	**Compliances Yes/No**
3G	**Cyber Security Accessories**	

	1. RJ45 Port Locking device:	
	Prevent users from inserting cables, devices or foreign objects without permission	
	Quickly and easily block physical access to RJ-45 Network ports Single key shall be suitable for all locks. And 1 key shall be supplied for each 20 RJ45 Locks	
	2. USB A Port Blockers:	
	Physically prevent access to a USB Type A Port	
	Single key shall be suitable for all locks and 1 key shall be supplied for each 10 USB Locks	
	3. Hologram Sticker "BHEL ASTR Secured", Size 20mm x20mm Tamper-evident holographic security sticker for authentication purpose	
		
	Material: Metallized polyester film (PET) with holographic image layer. Thickness: 25–50 microns	
	Dimensions: Size: 20 mm × 20 mm Shape: Square	
	Printing & Design: Custom design with BHEL ASTR logo and text 2D/3D holographic image with multi-color light diffraction effect include microtext or hidden text (visible under laser or UV)	
	Adhesive: Pressure-sensitive adhesive suitable for metal, plastic, and painted surfaces Tamper-evident type: destroys on removal attempt	
	Features: Scratch- and moisture-resistant Non-reusable and non-transferable Operating temperature: –10°C to +60°C Minimum adhesion strength: ≥ 20 N/25 mm	

4. Technical Services

Sl. No.	Service Requirement	Compliances Yes/No
4A	Technical Services to be provided at BHEL/EDN, Bangalore. Vendor should depute Engineer for test set up configuration at BHEL/EDN Bangalore for as many days required to complete configuration and demonstration. Various technical features have to be demonstrated and the final approved deployment has to be documented.	

Tender General Specifications

I. Authorization from Reseller/System Integrator

An authorization letter shall be provided by the Reseller/System Integrator for the following:

a. Sales and post sales service by the reseller / system integrators
b. Quoted Bill of Material (BOM) should be brand new sourced from OEM.
(Refurbished products either from OEM or from third party are not acceptable.)

II. Documents to be provided with offer

a. Authorization letters from respective OEMs for all firewalls, NAS & Software to be provided stating that all the technical support will be provided by dealer after sales.
b. Proof for the technical compliance for all items in the form of data sheets/manuals with highlighting the relevant compliance. Signed & stamp copy with Technical compliances of full purchase specifications also to be submitted
c. Bill material including technical services in line with Table 1,2 &3.

III. Power supply rating & power cord:

All the equipment quoted for this tender should operate on 230V, 50HZ single phase AC supply. Power cord for all the equipment shall be INDIAN compatible.

IV. 19" Rack mount hardware:

19" rack mounting hardware has to be provided for all the applicable components.

V. Set up /configuration software & user manuals:

BHEL's control system will be running on windows 10 & Windows server 2019. Hence all set-up / configuration software should be compatible to windows 10/ windows server 2019. All the products should be provided with installation, configuration and error logs etc., either by hard copy or by DVD.

VI. Test certificates with serial numbers from OEM along with delivery:

Test certificates with serial numbers shall be provided from the respective OEMs.

VII. Warranty for the system:

Warranty as per technical specification specified in Clause 3

****

Pre-Qualification Criteria (Minimum Eligibility Criteria) to participate in Rate Contract tender for Cyber Security Suite

The bidders intending to participate shall meet the following criteria and such of those bidders shall be pre-qualified for this tender.

Sl.No	Criteria	Documentary Evidence	Vendor compliance/ remarks
1.	**Upload Manufacturer authorization:** Bidder shall submit Manufacturers Authorization Form (MAF)/Certificate with OEM details such as name, designation, address, e-mail Id and Phone No. required to be furnished along with the bid for item 2.1 to 2.7 of PS4042971	Manufacturer Authorization Form (MAF)	
2.	**IMPORTED PRODUCTS:** In case of imported products, OEM or Authorized Seller of OEM should have a registered office in India to provide after sales service support in India. The certificate to this effect should be submitted.	Certificate for authorized after sales service support in India	
3.	**Experience Criteria** The Bidder **should have experience of at least two (2) years** in **supplying and/or implementing the same or similar category of Cyber Security products and solutions** as specified in **Clauses 2.1 to 2.7 of PS4042971**, for **power plant and/or process plant applications**. **Bidders who have supplied and integrated at least two (2) hardware items** (such as IPS Firewall, IDS Firewall, Multifunction Firewall, or Network Attached Storage) **and at least one (1) software item** (such as NMS software, Security Event Manager software, or Syslog Server software) **from the above list during this period shall also qualify**, prior to the bid opening date	Bidder should submit relevant PO copies with detailed BoM clearly indicating makes /models supplied as part of PO as a proof of supply.	
4.	**Malicious Code Certificate:** The seller should upload following certificate in the bid:- (a) This is to certify that the Hardware and the Software being offered, as part of the contract, does not contain Embedded Malicious code that would activate procedures to :- (i) Inhibit the desires and designed function of the equipment. (ii) Cause physical damage to the user or equipment during the exploitation. (iii) Tap information resident or transient in the equipment/network. (b) The firm will be considered to be in breach of the procurement contract, in case physical damage, loss of information or infringements related to copyright and Intellectual Property Right (IPRs) are caused due to activation of any such malicious code in embedded software.	Certificate to be provided.	
5.	Bidders shall quote only those products in the bid which are not obsolete in the market and has at least 3 years residual market life i.e. the offered product shall not be declared end-of-life by the OEM before this period.	OEM declaration for the same	