Request For Proposal (RFP)

for

Cyber Security Operations Centre (Cyber SOC) Services

And

Web Application and API Protection (WAAP) Services

Table of Contents

1 Terms and Definitions:

1.1. **'Owner'** - The Owner shall mean M/s Bharat Heavy Electricals Limited (A Govt. of India Undertaking) incorporated under the Companies Act 1956/2013 with its registered office at BHEL House, Siri Fort, New Delhi-110049. The expression shall include its successors and assigns. It may also be referred to as BHEL.

1.2. **'OEM'** - The OEM of the offered Cyber Security Operations Center (SOC) or WAAP solution / products.

1.3. **'Request for Proposal (RFP)'** - Tender document containing the Specifications, scope, qualification criteria, terms & conditions etc. released by BHEL.

1.4. **'Bid'** - The documents submitted in response to the RFP.

1.5. **'Bidder' -** The Bidder shall mean the OEM / Implementation Partner / System Integrator registered under the Indian Statute governing the respective entity who is quoting against the Tender Enquiry issued by the Owner.

1.6. **'Successful Bidder' –** OEM **/** Implementation Partner / System Integrator bidding for this RFP document, who has qualified successfully in the biding process and is given the award of Work.

1.7. **'Units/Sites'**- Units are BHEL's manufacturing facilities and Sites are BHEL's project sites.

1.8. **'Specification' -** The Specification shall mean the specifications contained in the RFP Documents and Annexure, Schedule, etc. attached thereto, if any, and includes any subsequent modifications thereof.

1.9. **'Approved' -** The Approved means approved in writing.

1.10. **'Month / Week'** - The Month shall mean calendar month & Week shall mean 7 days.

1.11. **'Day / Days'** - The Day / Days shall mean calendar day / days.

1.12. '**Commissioning Date**' - Date mentioned in the commissioning certificate issued by the owner.

2 Introduction:

Established in 1964, Bharat Heavy Electricals Limited (BHEL) is the largest engineering and manufacturing enterprise in India in the energy and infrastructure sector with the capability to manufacture the entire range of power plant equipment.

BHEL manufactures over 180 products under 30 major product groups and caters to core sectors of the Indian Economy viz., Power Generation & Transmission, Industry, Transportation, Telecommunication, Renewable Energy, etc. The wide network of BHEL's 17 manufacturing divisions, four Power Sector regional centers, over 100 project sites, eight service centers and 18 regional offices, enables the Company to promptly serve its customers and provide them with suitable products, Systems and services. The high level of quality & reliability of its products is due to the emphasis on design, engineering and manufacturing to international standards by acquiring and adapting some of the best technologies from leading companies in the world, together with technologies developed in its own R&D centers.

BHEL's vision is to become a world-class engineering enterprise, committed to enhancing stakeholder value. The company is striving to give shape to its aspirations and fulfill the expectations of the country to become a global player.

3 Information Technology in BHEL:

In BHEL, Information Technology has deeply penetrated all the functional areas and it is suitably deployed in various facets of company's operations. The company has substantially introduced IT in its Engineering, Manufacturing, and Materials Management & Production functions. A number of IT initiatives have been taken up so as to meet the emerging demands of the business and challenges of the New Economy.

3.1 IT Infrastructure:

In BHEL, computer devices (endpoints) have been deployed at all Units, Divisions, Offices and project sites. All endpoints at location / Unit / office are connected through a state-of-the-art LAN network Different Units, divisions, offices and project sites are inter-connected through dual-cloud, dual homed MPLS network. The internet connectivity has been provided to all the locations through two centralized internet gateways at CDT Noida and HPEP Hyderabad internet gateways. There is a third internet gateway at Corporate Office, New Delhi for exclusive internet access to Top Management. Perimeter security devices like firewalls, IPS, VPN, etc., have been installed at these three internet gateway locations. The exchange of information across the Units / Divisions is through MPLS network only.

Recently BHEL has consolidated its multiple datacenters to two datacenters, Primary DC at HPEP Hyderabad and DR Centre at HEEP Haridwar. The centralized internet gateways shall be at HPEP Hyderabad and HEEP Haridwar. The Noida Internet Gateway will be phased out in next 6 months' time period.

Internet Bandwidth at HPEP Hyderabad: 1 Gbps, 800 Mbps (two links)

Internet Bandwidth at HEEP Haridwar: 1 Gbps, 800 Mbps (two links)

Internet Bandwidth at Corporate Office, New Delhi: 256 Mbps, 256 Mbps (two links)

3.2 Business Applications & Other software used:

Integrated end to end Business Applications, largely rendered in web, have been developed and used at various manufacturing units within various processes from receipt of work order to dispatch of equipment.

A number of Web based applications are being developed and implemented in various functions across various Units/Regions/Business Sectors for their local operations. Some Corporate wide web applications have also been developed over a period of time, mostly. RDBMS & J2EE is the favored technology for application development.

All engineering centers are well equipped with engineering workstations using advance Engineering Software for Designing, Modeling, Analysis and Drafting etc. Electronic Depositories, with appropriate work flow & change control, have been implemented particularly for Engineering Documents at major units.

There are about 100 internet facing applications across the organizations. These applications have been put behind Web Application Firewall (WAF) installed at HPEP Hyderabad and Noida. All these applications have been made available on internet through centralized Internet Gateways at HPEP Hyderabad, CDT Noida and Corporate Office, New Delhi. Going forward, these applications will be centrally hosted at HPEP Hyderabad and HEEP Haridwar datacenters and made online through internet gateways at these two units.

3.3 Existing Network Infrastructure:

BHEL is using MPLS connectivity from multiple service providers to connect their locations. The BHEL locations are connected through multiple connectivity options with redundancy as required.

4 Cyber Security in BHEL:

BHEL has deployed defense-in-depth multi-layered protection for its IT assets and data against cyber threats. Perimeter security comprising of Next Generation Firewalls, Intrusion Prevention System (IPS), Secure Web Gateways, Virtual Private Network (VPN), Secure Email Gateway etc is in place.

A centralized endpoint protection solution with Endpoint Detection and Response (EDR) has been deployed across the organization.

BHEL had established a state-of-the-art Cyber Security Operations center (Cyber SOC), a facility in which an information security team continuously monitors and improves the organization's security posture while preventing, detecting, analyzing and responding cyber security incidents with the aid of both technology as well as well-defined processes and procedures.

The current SIEM deployed in BHEL is a purpose-built solution with appliances installed at BHEL Hyderabad unit and the Control Centre established at BHEL Noida office. The existing SOC contract is expiring in the year 2025 and is proposed to be replaced with a new state-of-the-art SOC solution through this RFP.

5 Objective:

BHEL is committed to the security of its information and information assets. It takes cybersecurity very seriously. The objective is to maintain the trust and confidence of its customers and stakeholders in its information assets and systems by enhancing and strengthening the IT Security posture of the organization by:

a. Implementing an on prem Cyber Security Operations Center (Cyber SOC) for 24X7 comprehensive monitoring, detecting and analyzing of information / cyber security events and incidents.
b. Implementing a cloud based managed Web Application & API Protection (WAAP) for the security of online applications, websites and APIs.

6 Technical Pre-Qualification Requirements (Technical PQR):

S. No.	Qualification Criteria	Documents to be Provided	Bidder's Compliance (Yes / No)
For bidder			
1	The bidder should have a registered office in India having a valid PAN No. and GST Registration No.	a) Copy of Certificate of registration. b) Copy of PAN Card c) Copy of GST Registration	
2	The bidder shall be OEM / OEM's Subsidiary / OEM's authorized partner or system integrator.	Documentary evidence for OEM / OEM's Subsidiary / OEM's authorized partner or system integrator. (In case bidder is not OEM, an authorization letter from OEM to be submitted by the bidder specifically authorizing the bidder to quote in this tender)	

3	The Bidder should be ISO 27001:2013 / ISO 27001:2022 certified.	Appropriate documentary evidence to be provided. Copy of valid ISO 27001:2013 / ISO 27001:2022 certificate.	
4	The bidder should have executed similar work in the **last 7 years,** preceding the bid submission date as follows: One Order of similar work for minimum **60000 EPS** (events per second). OR Two orders of similar work for minimum **50000 EPS** each. OR Three orders of similar work for minimum **40000 EPS** each. Note: (a) Executed here means the bidder should have implemented and commissioned the solution and should have maintained the same for at least one year from the date of commissioning in the last 7 years, preceding the bid submission date. (b) Similar work here means the bidder should have implemented and maintained/maintaining a SIEM solution in combination with either SOAR or UEBA or both in the last 7 years, preceding the bid submission date.	a) copy of PO / WO / LOI b) copy of commissioning certificate c) Satisfactory services certificate / confirmation from customer d) Bidder shall provide contact details (name, email id, phone no.) of customers for verification.	
5	The bidder should have executed SIEM solution for at least 5 customers in India in the last 7 years, preceding the bid submission date. with a cumulative 120000 EPS Note: (a) Executed here means the bidder should have implemented and commissioned the solution and should have maintained the same for at least one year from the date of commissioning in the last 7 years, preceding the bid submission date.	a) copy of PO / WO / LOI b) copy of commissioning certificate c) Satisfactory services certificate / confirmation from customer d) Bidder shall provide contact details (name, email id, phone no.) of customers for verification.	
6	The bidder should have had a positive networth in the preceding three financial years, i.e., 2023-24, 2022-23, 2021-22.	Copy of Audited Balance Sheets and Profit and Loss Account for the year 2021-22, 2022-23 and 2023-24 or Networth certificate from a CA with UDIN no.	

7	The bidder should have had an average turn-over of Rs 50 crores in the preceding 3 financial years, i.e., 2023-24, 2022-23, 2021-22	Copy of Audited balance sheets and Profit and Loss Account for the year 2021-22, 2022-23 and 2023-24 or Turnover certificate from a CA with UDIN number.	
8	The bidder should not have been banned in the last 3 years, preceding the bid submission date, in any BHEL Units / Divisions, CPSE or Central Govt entities for any unlawful or immoral business dealings.	Self-attested certificate from the bidder on letter head.	
9	The bidder of the proposed solution should have minimum following certified professionals on its own rolls. Certified Information Systems Security Professional (CISSP) / Certified Information Security Manager (CISM) / GIAC Security Leadership Certification (GSLC): 2 nos. Certified Ethical Hacker (CEH from EC-Council): 2 nos.	Copy of certificates. All certificates should be current and valid. Expired certificates will not be considered. Signed Letter on company's letterhead from Company HR Head to be submitted for being on company's rolls.	
For OEMs and Proposed Solutions			
1	The OEMs of the SIEM, SOAR and UEBA solutions should have a registered office in India.	Copy of certificate of registration.	
2	The OEMs of the SIEM and WAAP solutions should have been present in India for at least last 5 years before the date of submission of the bid.	Certificate of incorporation /Audited Balance Sheet /Merger, Amalgamation or Demerger agreement alongwith relevant order /Purchase Agreement, etc.	
3	The OEM of the WAAP solution should have its own datacentre in India (MeitY empanelled) or should have a pre-tie-up with an Indian Data Center Service Provider (MeitY empanelled) from which the solution offered to BHEL shall be rendered.	Valid MeitY empanelment certificate of the OEM data centre in India / service agreement or hosting agreement between the OEM and the MeitY empanelled Data Centre (where the proposed WAAP solution would be hosted), etc.	
4	The proposed SIEM and WAAP solutions must have been deployed in India for at least **10 customers** (each solution, i.e., SIEM, WAAP) in the last 7 years, preceding the bid submission date and it should be currently operational for at least **5 customers** (each solution).	a) copy of PO / WO / LOI b) copy of commissioning certificate c) Satisfactory services certificate / confirmation from customer d) Bidder shall provide contact details (name, email id, phone no.) of customers for verification.	

5	The proposed SIEM solution should have been deployed in India for a minimum cumulative **240000 EPS in the last 7 years**, preceding the bid submission date.	a) copy of PO / WO / LOI b) copy of commissioning certificate c) Satisfactory services certificate / confirmation from customer d) Bidder shall provide contact details (name, email id, phone no.) of customers for verification.	
6	The proposed SIEM solution should have been deployed at a single customer in India for a sustained minimum **60000 EPS** (events per second) in the **last 7 years**, preceding the bid submission date. The solution should have been commissioned and successfully running for a minimum one year in the **last 7 years**, preceding the bid submission date.	a) copy of PO / WO / LOI b) copy of commissioning certificate c) Satisfactory services certificate / confirmation from customer d) Bidder shall provide contact details (name, email id, phone no.) of customers for verification.	
7	The proposed WAAP solution should have been deployed in India for a customer for a minimum **100Mbps** data transfer rate or at least **50 applications** / **websites** in the **last 7 years**, preceding the bid submission date**.**	a) copy of PO / WO / LOI b) copy of commissioning certificate c) Satisfactory services certificate / confirmation from customer d) Bidder shall provide contact details (name, email id, phone no.) of customers for verification.	
8	The OEMs of the SIEM, SOAR, UEBA and WAAP solutions should have their own customer support centre in India.	a) Address of the Customer Support Centre b) Copy of lease agreement / rent agreement / electricity bill / Telephone bill, etc.	

Notes:

1) All criteria of PQR (for bidder and for OEM's of proposed solution) have to be met for the bid to be qualified for next stage of evaluation. The bidder shall submit necessary documentary proof in support of the PQR criteria. All documentary proof submitted by the bidder should be verifiable by BHEL. BHEL's decision on PQR criteria, interpretation and acceptance or rejection of any documentary evidence shall be final and binding on all the bidders.
2) Bidder shall not be under Bankruptcy proceedings (IBC) by NCLT or under liquidation / BIFR, which will render it ineligible for participation in this tender. The bidder shall submit an undertaking towards this effect.
3) For the purpose of evaluating the Pre Qualification Requirements (PQR), only the credentials of the Bidder will be considered. However, if the Bidder is a subsidiary company, the credentials of its Parent Company will be considered, provided that the Bidder submits satisfactory documentary evidence acceptable to BHEL. Acceptable documentary evidence may include any of the following, but is not limited to:
   i. Board Resolution
   ii. Slump Sale Agreement
   iii. Demerger Agreement

Credentials of any other subsidiaries or associates of the Parent Company will not be taken into account. Additionally, an agreement between the Bidder and its Parent Company must be executed in the format provided in **Annexure-XVII** and submitted as part of the bid.

4) The bidder's representative/individual signing the bid documents on behalf of the bidder should have an authorization letter / power of Attorney, etc. from the bidder specifically authorizing the representative/individual to sign in this tender.

7 Delivery Timelines:

S. No.	Activity	Timelines
1.	Supply, installation, configuration and commissioning	120 days from date of PO

8 Contract Period & Start Date:

The contract shall be initially for a period of 5 years. The start date of the contract shall be the Commissioning Date of the solution.

9 Project Implementation:

a) For smooth and timely implementation of the project, the successful bidder shall assign a project team headed by a project manager during the implementation phase. The assigned project manager should have minimum 10 years of experience in security solutions and should have successfully delivered/managed at least 02 SOC related projects.

b) In addition to the Project Manager, the successful bidder's project team shall include two (02) qualified and experienced professionals (having minimum five years of experience in deployment of security solutions.).

c) The project team shall physically be placed at BHEL Corporate Office, CDT, Noida/New Delhi during the implementation. This project team shall interact, coordinate and closely work with BHEL's project team for the implementation of the project. The team may be required to visit DC/DR locations (Haridwar/Hyderabad) for implementation of the solution without any additional cost to BHEL.

d) The successful bidder's Project Manager shall prepare and submit the implementation plan along with timelines to BHEL.

e) The successful bidder's Project Manager shall, in association with OEM of the solution, design the solution architecture for the offered solution. The solution architecture plan shall be vetted by the OEM for performance and security best practices without any additional cost.

f) The successful bidder shall provision the solution maintaining the RTO of 30 minutes and RPO of zero, i.e., zero data loss. The evidence of the same shall be provided to BHEL.

g) The successful bidder shall provide documentation specifying the BCP and DR plan of the solution as per required RPO/RTO.

h) The successful bidder shall provide the escalation mechanism for the support for the entire contract period.

i) For any software provided as part of the solution, the licenses should be in BHEL's name or BHEL shall have the right to use.

j) The successful bidder shall implement the SIEM solution, create report templates, Log Parsing, Log source integration, dashboards & do monitoring of the solution for the complete contract period.

k) The successful bidder shall create an instance / tenant for BHEL in a dedicated or distributed architecture for provisioning of WAAP services on cloud. The WAAP service shall be adequately sized to meet peak data transfer rate and SLA.

l) The successful bidder shall offer cloud-based WAAP solutions from a datacenter within India.

m) The Solution and all its component (including hardware/software to be provisioned at BHEL premises) shall be offered as a service to BHEL. The project deliverables will broadly consist of below constituents:

- **i.** On prem SOC (SIEM, SOAR and UEBA)
- **ii.** Cloud based WAAP
- **iii.** Log storage for 12 months (Last 6 Months log data in online (hot storage), preceding 6 months (after first 6 months) log data on Archive storage)
- **iv.** A common integrated centralized dashboard for all the SOC components (SIEM / SOAR/UEBA & WAAP)
- **v.** Onsite 24x7 helpdesk
- **vi.** Remote Support for WAAP
- **vii.** TAM support from OEM

10 Solution Architecture & Deployment

a) The SOC solution (SIEM, SOAR, UEBA) shall be deployed at BHEL HPEP Hyderabad datacenter in a high availability mode. The DR for the same shall be provisioned and deployed at near DR Centre at HPEP Hyderabad only.

b) The log collectors / forwarders shall be provisioned at **2 datacenters at BHEL HPEP Hyderabad and HEEP Haridwar**.

c) The log collectors at each of the 2 datacenters (Hyderabad and Haridwar) shall be deployed in HA mode with auto failover feature.

d) The dashboard and hardware/software as part of dashboard shall be deployed at BHEL CDT Noida location. The role-based access to dashboard (SIEM, UEBA and WAAP) should be made available to minimum 5 concurrent users.

e) The necessary hardware and software required for log collectors / forwarders shall be provided by the successful bidder. The log collectors shall be sized in such a manner so as to support log ingestion rate of 4TB per day and local log retention for 2 days in each of the log collectors.

f) A detailed tentative deployment architecture is given in **Annexure - II**. This is the minimum level of redundancy and capacity required. If the solution offered by the bidder requires higher level of redundancy and capacity to meet the technical and functional requirements of BHEL, the same shall be provisioned by the bidder.

g) The SOC (SIEM, SOAR, UEBA) solution should be designed and deployed in Active-Active or Active--Passive mode with auto-failover from DC to DR.

h) All the supplied hardware at all BHEL location shall be Rack Mountable. All the supplied hardware shall have redundant (1+1) hot swappable power supply.

11 Scope of Work

11.1 General:

a. The broad scope includes:

   i. Provisioning of on prem Cyber Security Operations Centre (Cyber SOC -- SIEM, SOAR, UEBA)

   ii. Provisioning of Web Application & API Protection (WAAP) on cloud

   iii. Maintaining and managing Cyber SOC and WAAP for entire contract period.

b. The entire scope of work covered in this document and subsequent instructions to the bidder post award shall be deemed to be bidder's obligation. The scope of work / specifications detailed herein are indicative only.

c. Successful bidder shall work in co-ordination with BHEL team and OEMs for completion of project.

d. The solution shall include all the required components as per technical specifications and requirements (**Annexure-III**) for successful implementation of the solution.

e. The successful bidder shall configure and provision the solution as per technical specifications and requirements (As per **Annexure – III**).

f. After installation, the bidder shall demonstrate the operational and functional working of the solution as per technical specification.

g. The successful bidder shall monitor, maintain and manage the entire solution during the complete contract period.

h. The successful bidder shall carry out installation of systems, fixing, termination and inter-cabling, etc. Arrange and provide requisite item, component, cables, tools and software etc. for carrying out the installation and commissioning job. Proper documentation, labeling and tagging shall be done for all the equipment used in the entire solution for easy management and maintenance.

i. Any Server / Workstation / Desktop / Laptop (Physical / Virtual) provided as part of the solution should come with latest licensed version of the OS and should support Check Point EDR (Harmony Endpoint Advanced, client version 88:32 or above).

j. The successful bidder shall provide upgrades / updates of software / firmware supplied as part of solution for the entire contract period.

11.2 Event Log Collection & Management

a. The solution shall collect and forward logs from various data sources to the SIEM solution through log collector /forwarder / connector in a centralized manner.

b. The solution shall also support direct log transfer / ingestion to the SIEM solution.

c. The tentative list of log data sources is given in **Annexure- IV.**

d. Apart from on-prem data sources, the successful bidder shall also integrate the BHEL data sources (EDR solution, WAAP solution, SSE & ZTNA, www.bhel.com, etc.) that are / shall be running on cloud solution (SaaS)

e. In case, out of the box connectors are not available, the bidder shall create custom connectors / parser to integrate the data source. Any custom parser shall be created and implemented within

7 days of request from BHEL. During the period of contract, BHEL may upgrade / change solutions, in such case, bidder is required to integrate the new / upgraded / changed solutions into the SOC solution.

f. The successful bidder shall write customized parsers by understanding data format and ensure that major and important fields present in the same are indexed individually as per their specific field names.

g. The proposed SOC solution shall collect raw data in its native format and make it available for both real time and historical correlations and searches.

h. Log Collectors should compress logs (minimum 1:2 ratio) before forwarding to the SOC solution. The solution shall ensure lossless compression of the logs between log forwarder / collector to on prem storage for optimized network performance during transit.

i. If connectivity between intermediate log repositories/forwarder and on prem Log storage is down, then the proposed solution shall ensure log repositories/forwarder forwards data to the SOC solution once connectivity is re-established without any data loss. In case of network failure, the logs must be retained for at least 2 days in Log collectors.

j. The solution shall support collection and processing of raw logs in real-time from any IP Device including Networking devices (such as router/ switches), Security systems (EDR, Patch Mgmt., Firewall, Active Directory, DNS, IPS, Proxy, etc.), Operating systems (Windows (all Flavors), Unix, LINUX (all Flavors),), Virtualization platforms (Hyper V, Hypervisor, Nutanix, etc.), Databases (Oracle, SQL, DB2, MongoDB, Postgress, etc.) Storage Systems (Windows, Nutanix, etc.), and Application Servers (Oracle WebLogic, Windows IIS, Apache Tomcat, etc.) etc. The solution should capture all the fields of the information in the raw logs.

k. The SOC should be configured to retain both Raw and Normalized logs.

l. All the Logs (raw as well as normalized) stored must be tamperproof.

m. Event Dropping or Caching by SOC should not happen in normal circumstances and same should be reported and corrected immediately.

n. The successful bidder shall provide report of storage utilization (uncompressed storage utilization) of each data source on daily basis.

o. The successful bidder shall provide access to a portal for raising support tickets and ticket management.

p. The solution shall provide the following:

    a) REST API to expose all indexed data, search commands, and functionality to external systems, applications, and dashboards.

    b) A GUI interface for configuration and management to enable granular changes and customization.

    c) Creation of reports and dashboards as per BHEL requirements.

    d) Easy forwarding of data / logs to external systems or logging tools.

    e) Ingesting data from custom applications in secure / encrypted manner.

    f) Installation of agents on end devices, if required. Initial device count will be around 1000, which can increase during the project period.

g) Log collection / forwarding / transferring from agent based and agent less devices (like Syslog etc.)

q. The proposed solution shall have pre-filtering (discarding) option from all log source types based on, but not limited to, event type, event ID, etc. at agent level before collecting / transferring of Logs. The data that is filtered out should not be counted against the licensed capacity.

r. There shall not be any license restrictions on number of endpoints (Desktop / Servers / network devices) / users / agents, etc., to be integrated with the solution.

s. The proposed solution shall ensure ingestion of data in a secure manner via HTTPS/ encrypted manner from various data sources in different format such as RAW text, XML, JSON, etc. The solution should support for API ingestion via single event, batches, or streaming.

t. The proposed solution shall ensure capturing log collection time and event time of the logs. Collection time means when the logs have reached to the SOC solution and event time means when the event has occurred on end device.

u. If required, the successful bidder shall ensure deployment of agent on (including but not limited to) Windows (all flavors currently in support by Microsoft and any new version released in future), MAC and Linux/Unix based OS. The agent shall be light weight and have low resource utilization (Disk, RAM, CPU) at the endpoint level.

v. The successful bidder shall ensure that the deployed agent coexists with other existing endpoint agents of other OEMs (like Checkpoint EDR Agent, Patch Management Solution agent, Netskope SSE, ZTNA, etc.) without any conflicts / issues.

w. The successful bidder shall carry out deployment of solution or agents across multiple end points, if required, by deploying necessary resources with minimum disruption to BHEL operations.

x. The successful bidder shall ensure that the deployment of agent shall not require reboot of end devices / machines for installation / removal / update / upgrade etc.

y. The successful bidder shall ensure that the deployed agent is able to select (enable/disable) different types of logs from endpoint device to be forwarded to log collector/forwarder and SIEM. e.g. Admin should be able to forward PowerShell logs but can stop forwarding of System logs of Windows.

z. The proposed solution shall have provision / feature so that a copy of raw logs can be transferred / shared (through Push/Pull mechanism) to any other location (cloud or on prem) of same or different OEM in log source native / raw format at BHEL discretion, without any additional cost and without any limitation on volume of log to be transferred / copied.

aa. The proposed solution shall have a dedicated monitoring console to monitor day to day operations and solution health.

bb. The solution shall monitor activities and alerts for internal and external threats and ensure alerting / reporting on the same but not limited to the following:

i. Login by dormant user
ii. Failed login attempts on locked out account.
iii. Windows logs cleared using PowerShell.
iv. User added to / removed from a group
v. User account modified to password never expires.
vi. Possible brute force attempts
vii. Any user performing large upload first time in last 30 days.

viii. Any rare process executed on user machine which is not seen in environment since last 30 days.
ix. Password spraying, user enumeration
x. Account takeover or credentialed access.
xi. Unauthorized user activity during non-business hours.
xii. Lateral movement when a compromised account is used.
xiii. Unusual username in the authentication logs (rare Users)
xiv. Suspicious login activity
xv. Rare and unusual errors
xvi. Anomalous network activity
xvii. Command-and-control, persistence mechanism, or data exfiltration activity.
xviii. Unauthorized software & malware
xix. Unusual network Destination: communication with command-and-control (C2)
xx. Denial-of-service attacks or traffic floods
xxi. Credential Harvesting: anomalous access to the metadata service by an unusual user.
xxii. Unusual user context switches due to privilege escalation.
xxiii. Unusual RDP (remote desktop protocol) user logins

cc. The solution shall provide customized correlation rules for conducting intelligent analytics / alerting on real-time and historical log data obtained from multiple log sources on multiple parameters (like Hosts, Geographies, recurring activities) including OS platforms, network & security devices, applications, etc. as well as threat feeds obtained from different sources.

dd. The solution shall ensure anomaly detection, user behavioural profiling, predictive analytics, and real-time/historical analysis of data/logs.

ee. The solution shall provide machine learning algorithms to analyze the behaviour of all endpoints/users and detect anomalies that point to a threat that might be present.

ff. The solution shall detect and alert for threats like Lateral Movement and Data Exfiltration.

gg. The solution shall detect and alert for signature-based attacks and volumetric attacks.

hh. The solution shall provide native user authentication through SAML, OpenID Connect, LDAP, Active Directory, ADFS, PKI, etc. and provide Multi-Factor Authentication from day one.

ii. The solution shall provide flexible fine-grained Roles Based Access Control (RBAC) and Attribute Based Access Control (ABAC) for controlled user and API access. Shall restrict access, but not limited, to specific data sources, data types, time periods, specific views, reports, or dashboards, etc.

jj. The successful bidder shall arrange to perform health check-up by OEM (at least twice a year) and fine tuning of solution, as and when required by BHEL and submit the report.

kk. The successful bidder shall submit the SLA report at the end of every quarter to BHEL.

ll. In case of default on any of the service level metric, the bidder shall submit performance improvement plan along with the root cause analysis and implement the plan after BHEL's approval.

mm. The solution should be able to integrate with third party threat intel (like CERT-In, NCIIPC, etc.) for endpoint protection for blocking of IOCs like hashes, etc.

nn. The SOC solution should have built-in integration with following log sources. The proposed SOC solution should support **MITRE ATT&CK framework** and provide a **navigator** for the same. The solution should support AI/ML models to identify any unusual behaviour. It should

detect alerts and incidents from these log sources and map them with MITRE ATT&CK adversarial tactics, techniques and procedures.

It should help in identifying gaps in log data for mapping alerts / incidents to MITRE ATT&CK Technique & Sub techniques.

i. Endpoint log sources
   - Windows Professional 10 / 11 and above
   - Windows Server 2016/2019/2022 and the latest
   - Linux (RHEL 7 and above, Ubuntu, CentOS, Oracle Linux 8.9 and above, etc.,)
   - Unix (AIX / HP-UX)
   - Vmware Hypervisor (ESXi 7.0)
   - Microsoft Hyper-V
   - Nutanix Acropolis
   - Etc.,

ii. Active Directory log sources
iii. Anti-virus log sources (Check Point (Harmony Advanced) / Sophos, etc.)
iv. Database log sources (Oracle / Mongo / SQL)
v. DNS log sources (Microsoft DNS / Cisco Umbrella / Infoblox, etc.,)
vi. VPN log sources (Fortinet / Netskope Private Access)
vii. Web Application Firewall / Web Applications & API Protection (WAF/WAAP) log sources
   - Array
   - F5
   - Imperva
   - Cloudflare
   - Radware
   - Etc.

viii. Web Proxy log sources (Netskope ZTNA)
ix. IDS/IPS log sources (Fortinet / Cisco / HP)
x. Firewall/router log sources (Fortinet / Cisco)

11.3 Security Orchestration, Automation & Response (SOAR): Automation of Actions

a) The solution should provide min. **3 no**. of named users for management.

b) The solution should collect and aggregate logs to generate events and take automated actions to respond to these events.

c) The solution must provide out- of-box playbooks based on SANS and NIST that provide incident response.

d) The solution must support the ability to take action related to an incident. The action includes blocking of the malicious IOCs, etc.

11.4 User Entity & Behaviour Analytics (UEBA): Analysis of high-risk entities / users

a) Solution should provide user behaviour analytics for minimum 18000 users and entity behaviour analytics for at least 2000 entities.

b) Solution should establish a baseline of typical user behavior and use AI / ML algorithms, and user behaviour to know when there is a deviation from established patterns which could result in a potential threat.

c) The solution should provide the capability to rapidly respond to insider threats by automatically measuring and prioritizing the risk based on measured risk score, associated with suspicious users/ entities.

11.5 Web Application & API Protection (WAAP): Web Application Protection

a) The bidder shall provide web applications and API protection services to BHEL for online business applications and websites.

b) The solution shall be cloud based providing protection to BHEL's on-prem applications and websites (around 120 FQDN)

c) The solution should protect web applications by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevent any unauthorized data from leaving the application.

d) The solution must address and mitigate the OWASP Top 10 web application security vulnerabilities but not limited to this.

e) The solution should support integration with the offered on prem SIEM and other Monitoring and Reporting solution.

11.6 Attack Surface Management

The bidder shall provide a solution for continuous monitoring of BHEL's Attack Surface, covering internet facing applications, APIs, devices, domains, DNS, email gateway, etc., to detect and assess new vulnerabilities, identity and credential breaches, data breaches, exposures, etc. It shall provide a centralized console to monitor the status of attack surface in real time.

11.7 Threat Intelligence

a) The SIEM solution should come integrated with a leading industry Threat Intelligence Database for early detection of Threats.

b) BHEL has been designated as a Strategic Sector organization by GOI, and as such it receives threat intel from NCIIPC on regular basis. The successful bidder shall integrate threat intel from NCIIPC with the offered solution. Additionally, BHEL receives advisories, alerts, scanning reports and malicious communication / incident reports from NCIIPC, CERT-In, NCCC (National Cyber Coordination Centre), Cyber Swachchta Kendra (CSK) on regular basis. The successful bidder shall take necessary action on these advisories and alerts on urgent basis as and when received.

c) Successful bidder shall maintain a knowledge base of alerts, incidents and mitigation steps and this knowledge base should be updated with evolving security events within and outside BHEL.

d) The solution should send notification messages and alerts through email, SMS, etc.

11.8 Digital forensics and incident response (DFIR)

a) In case of a major cybersecurity breach or ransomware attack, the bidder shall provide onsite Digital forensics and incident response (DFIR) services by deploying forensics specialists at BHEL site(s). The travel, lodging and boarding charges for the same shall borne by the bidder.

b) The DFIR team shall help in identification, containment and remediation of the incident. It shall identify, collect and analyze logs and attack artefacts from various affected systems, and do correlation and root cause analysis of the attack. It shall preserve the artefacts and logs for any legal investigation and forensics. It shall prepare report of the investigation and submit to BHEL within one month of such an attack.

c) The bidder shall provision specified hours of onsite DFIR services in its bid. The services will be invoked by BHEL as and when required, and payment will be made in lumpsum on actual consumption basis.

11.9 Service Availability

The successful bidder shall do 24x7 monitoring of all in-scope devices. The following performance parameters are expected from the successful bidder and the solution offered:

a) 99.9% Uptime of on prem SOC (SIEM, SOAR, UEBA, etc.) solution on quarterly basis.

b) 99.9% Uptime of log collectors / forwarders installed at BHEL Internet Gateways on quarterly basis.

c) 99.9% Uptime of On-cloud WAAP on quarterly basis.

d) All components of the solution including Log collectors/Forwarders in HA mode with auto fail over.

e) Categorization of Incidents / Alerts into Critical, High, Medium and Low priority as per below table:

Category	**Incident Type**
Critical	D-DOS Attack
	Ransomware
	Website defacement
	Application Level Attacks
	Data Exfiltration
	Cyber Espionage and Advanced Persistent Threat Attacks
	DNS Attack
	Active Directory attacks
High	Phishing Attack
	Credential based Attacks
	Router / Perimeter Device attack
	VPN attack
	C2C Attacks

	Brute force attack
	Worm/virus outbreak
	Lateral Movement
Medium	Blacklisted IP Communication
	Connection to Known Malicious Actor in Published Host List
Low	Reconnaissance Attacks
	Port & vulnerability Scans

f) All Critical, High and Medium priority security incidents to be logged as cases and responded as per below table:

Incident Type	**Detection & Reporting Time (minutes)**	**Analysis & Containment Time (Hours)**	**RCA Time (hours)**
Critical	15	2	12
High	30	4	24
Medium	60	6	36
Low	120	24	48

11.10 Service Level Agreement (SLA)

The successful bidder shall ensure that **solution uptime is 99.9% or above** during the quarter. The solution uptime will consist of:

a) Availability of on prem solution (SOC)
b) Availability of Cloud based Solution / Instance / tenant (WAAP)
c) Availability of Log collectors / forwarders
d) Availability of onsite helpdesk staff

SLA will be calculated as follows:

S. No.	**SLA Parameter**	**Required Uptime / Availability Per Quarter**
1	Availability of on prem SOC solution (SIEM, SOAR, UEBA)	99.9 % or above
2	Availability of Log collectors / forwarders	99.9 % or above

3	Availability of Cloud based Solution / Instance / tenant (WAAP)	99.9 % or above
4	Availability of onsite helpdesk staff	100%

If uptime of any of the above parameters at S. No. 1 & 2 is less than the required level, the downtime of that parameter will be considered the downtime of the SOC (SIEM, SOAR, UEBA) solution.

If uptime of the parameter at S. No. 3 above is less than the required level, the downtime of that parameter will be considered the downtime of the WAAP solution.

i. Deduction due to solution downtime (D1):

S. No.	Uptime (U)	Penalty % (P)	Multiplication Factor (F)
1	**U > = 99.9**	**0**	**0**
2	**U > = 99.7 < 99.9**	**1**	**1.1**
3	**U > = 99.5 < 99.7**	**3**	**1.3**
4	**U > = 99.3 < 99.5**	**5**	**1.5**
5	**U > = 99.1 < 99.3**	**7**	**1.7**
6	**U < 99.1**	**10**	**2**

D1 = P*F*Q

Where P=Penalty percentage
F=Multiplication Factor
Q=Quarterly charges of SOC / WAAP (excluding DFIR charges).
D1 will be calculated separately for SOC and WAAP.

ii. Deduction due to absence of onsite helpdesk staff (D2):

D2= Rs 5000/ per staff per shift * No. of absences

iii. Deduction due to delay in response and resolution of incidents (D3):

In case timelines required for Analysis & Containment of Critical / High / Medium incident specified in **Clause 11.9 (f)** are not met, a penalty equal to 0.025 % of the quarterly charges (excluding DFIR charges) of the solution will be deducted for every hour above mentioned timeline on cumulative incident basis.

Total deduction per quarter (D) = D1 + D2 +D3

Total deductions per quarter due to D1, D2 and D3 shall be limited to 20% of the quarterly charges (excluding DFIR charges) of the solution.

11.11 Solution Sizing:

The solution shall be sized as per follows:

a) **SIEM solution**: For ingestion of raw data / logs minimum **80,000 sustained EPS (events per second)** at all layers (on-premises components) without dropping events or queuing events due to insufficient computing resources. There shall be no limitation on the number of servers, users or log sources integrated with the solution.

b) **WAAP solution**: The solution must support minimum 500Mbps of data transfer rate.

c) The both SOC (SIEM, SOAR, UEBA) and WAAP solutions shall be able to handle occasional **spike up to +20% over the above sizing requirement** without degradation of performance at any level.

11.12 Solution Scalability:

a) **SOC solution:** The SOC solution should be scalable to +50% in terms of EPS capacity. In case the data ingestion rate of BHEL is consistently coming over 80,000 sustained EPS over a quarter, BHEL reserves the right to place order on the successful bidder for the extra EPS capacity in multiples of 5000 EPS on pro-rata basis at any time during the contract period. The successful bidder shall provide the required additional EPS capacity within one month of placement of order. Payment for the additional EPS would be paid from the date of provisioning of extra capacity after placement of order by BHEL. No payment will be paid retrospectively. The same SLA shall be applicable to the increased capacity.

b) **WAAP solution:** In case the data transfer rate of BHEL applications is consistently coming over 500Mbps over a quarter, BHEL reserves the right to place order on the successful bidder for the extra data transfer rate by up to +50% (i.e., upto 750Mbps) at any time during the contract period. The successful bidder shall provide the required capacity meeting all the deliverables and services as described in the scope of work for this additional data transfer rate. Payment for the increased data transfer rate above 500Mbps would be paid from the date of provisioning of extra capacity after placement of order by BHEL. No payment will be paid retrospectively. The same SLA shall be applicable to the increased capacity.

11.13 Log retention and Storage:

Overall minimum of 12 months log must be available as per follows:

i. Last 6 Months log data in online (hot storage)

ii. Preceding 6 months (after first 6 months) log data on Archive storage.

The successful bidder shall ensure policy-based retention of raw logs, in its original format and for each log source group/type. BHEL may occasionally ask for raw logs (tamperproof) for audit purposes, the successful bidder shall provide such logs as and when required.

11.14 L1/L2 Support (Onsite Helpdesk)

a) The bidder shall provide 24X7 helpdesk at BHEL's Corporate Office, Noida.

b) The helpdesk shall work on 24x7 basis and shall deploy the resources as per the table below:

Timings	No. of Resource	Remarks	Location
24x7	L1: 2 Nos	All Days (including weekends & holidays)	BHEL Noida
07:00am – 11:00pm	L2: 1 No. (per shift)	All Working Days as per BHEL calendar. On holidays, if required.	BHEL Noida
08:00am – 04:30pm	Resident Engineer	As per BHEL Hyd Unit working days	BHEL HPEP Hyderabad

c) The bidder shall provide a **centralized integrated dashboard** to view and monitor the SOC and WAAP logs, alerts and security posture of the organization.

d) The bidder shall supply following equipment for the onsite Helpdesk at CDT Noida for monitoring, testing and troubleshooting purpose. BHEL will provide sitting space, power and network connectivity for the helpdesk at Noida.:

   i. Desktops (at least intel i7 processor, 32GB RAM, 1 TB HDD, 256 GB SSD, 24" LCD display, latest Windows OS) -- 2 Nos.
   ii. Laptops (at least intel i7 processor, 32GB RAM, 1 TB SSD, 15" FHD display, 1080p Camera, latest Windows OS) -- 2 Nos.
   iii. Display Units (at least 55" display, 16:9 aspect ratio, 3840 X 2160 resolution, 1100:1 contrast ratio, 500 cd/sq.m brightness, 178 degrees horizontal and vertical viewing angle, IPS/PLS/LED/OLED/QLED based display, OS based like IOS/Android, etc. display 2 HDMI, DVI, 1 USB 2.0 and 1 ethernet ports, inbuilt - wi-fi connectivity, Remote Control and necessary accessories) – 2 Nos.

e) The helpdesk staff shall be approved by the Owner and shall be on the regular rolls of the successful bidder. The proof of employment of the helpdesk staff shall be submitted to BHEL for verifying the same.

f) In case of any helpdesk resource is on leave, adequate replacement shall be provided so that the services are available as per schedule.

g) The helpdesk staff shall be covered under ESI/PF or any other statutory social security guidelines issued by Government.

h) The successful bidder will provide insurance cover to its resident engineer. The resident engineer or their legal heirs shall not claim any insurance benefit from BHEL in case engineer suffer any loss or damage to their life or person or property while working in the BHEL premises.

i) The successful bidder shall ensure compliance to all the obligations arising under the Contract Labour (Regulations & Abolition) Act, 1970, Minimum Wages Act, Workmen's Compensation Act, 1923 and other labour laws prevailing in the country. BHEL shall not be liable for any non-compliance on part of the successful bidder. BHEL shall have no liability, legal or otherwise, towards the manpower deployed by the successful bidder as part of this contract.

11.14.1 Qualifications of Helpdesk Staff:

Resource	Qualifications	Certifications
L1	B.E. / B.Tech. with min. 5 years' experience in dealing with SOC solution	1. SOC Analyst Certification from EC-Council or CompTIA Security+ Certification 2. Certified from OEM of the offered SIEM solution on the offered SIEM solution.
L2	B.E. / B.Tech. with min. 7 years' experience in dealing with SOC solutions.	1. SOC Analyst Certification from EC-Council or CompTIA Security+ Certification 2. CEH (Certified Ethical Hacker) from EC-Council. 3. OEM certifications for the SIEM product being proposed as part of the solution.
L3	B.E. / B.Tech. with min. 10 years' experience in dealing with SOC solutions.	1. CEH (Certified Ethical Hacker) from EC-Council. 2. CISSP (Certified Information Systems Security Professional) from ISC2. 3. GIAC / EC-Council Certified Incident Handler.
Resident Engineer	B.E. / B.Tech. / MCA / Diploma in IT / electronics / computers with min. 2 years' experience in dealing with IT hardware	Trained on OEM solution

11.14.2 Roles & Responsibilities of the onsite helpdesk

These are only indicative and not exhaustive

a) Proactive monitoring of all the security logs through the centralized dashboard for SOC and WAAP solution for any alert / incident. For each such event or incident, the team shall investigate and take necessary remedial action.

b) Coordination with BHEL units for security related issues.

c) Responsible for the complete life cycle management of security incidents (from occurrence to closure).

d) Carry out the root cause analysis (RCA) of security incidents, its mitigation steps, coordinate & implement the controls to prevent recurrence and maintain ATR (Action Taken Report) of the same.

e) Incident analysis and investigation. The team shall provide Root Cause Analysis (RCA) of each incident. incident.

f) Analyze the advisories received from CERT-In, NCIIPC, NCCC, STQC & other government agencies/ trusted sources regarding endpoint protection and act within 24hrs of such advisories.

g) Design, create and customize the dashboards as per the BHEL requirements.

h) Provide daily/weekly/monthly reports to BHEL as per mutually agreed checklist and periodicity.

i) Monitor security logs received from all integrated log sources on daily basis. In case, logs are not received from any of the log sources, the same shall be informed to BHEL team on immediate basis. If, the issue is with SIEM solution or forwarding agent or log collectors / forwarders, the successful bidder shall take immediate necessary action for the resolution of the same.

j) Maintain architecture, documentation of the supplied solution and update the same as and when changes take place.

k) Perform initial analysis for known issues/vulnerabilities and provide the appropriate recommendations for closure.

l) Provide notification and communication to BHEL team upon any threat detection.

m) Ensure compliance with Service Level Agreements (SLA), process adherence and process improvements to achieve operational objectives and mitigate threats, Monitoring & Reporting of system components health and take necessary action in case of any observed issue.

n) Optimization of response time to fetch data, logs in advanced queries, reports, dashboards, etc.

o) Carry out regular backup of configuration, software & patch updation on all components of solution as & when released by respective OEMs.

p) Provide reports on performance of the solution as per BHEL requirement.

q) Ensure that the necessary documents like operating procedures, configuration management, Low Level Design, etc. are up to date with the changes made in their respective areas.

r) Co-ordinate with the OEMs in case of any hardware or software/system/solution issue and ensure the issue is resolved.

s) Proactively monitor immediate notifications of serious system health issues for the deployed solutions.

t) Provide coordinated rapid response to any security incident to contain the attack & coordinate restoration of services.

u) Send alerts with details of mitigation steps to designated BHEL personnel.

v) Maintain evidence of any security incident in a tamper proof manner to preserve it for legal and regulatory purposes, as required.

w) Provide MIS reports to BHEL on daily, weekly and monthly basis. The analysts shall also provide reports on demand whenever required by BHEL.

x) Investigate and respond to detected threats using a streamlined threat review workflow that provides visibility into anomalous activity, source and supporting evidence.

y) Provide incident analysis, response and remediation within the defined timelines for all identified incidents.

z) Continuously monitor the BHEL's internet facing applications /devices (attack surface) to detect and assess new vulnerabilities and attack vectors in real time, and alert BHEL team about any detected vulnerabilities that need immediate attention.

aa) Coordinate with remote L3 support for any major incidents, persistent problems, health review of the solution.

bb) If required, L3 resource shall visit BHEL site for any incident investigation, major issues, health review, etc.

11.14.3 Remote support required from WAAP OEM during the entire contract period

These are only indicative and not exhaustive

a) The remote support shall ensure configuration, fine tuning and optimization of the solution.

b) The remote support shall be responsible for regular updates and upgrades of the WAAP solution.

c) The remote support shall be responsible for enabling / disabling of applications / websites through WAAP.

d) The remote support shall monitor the performance / response time of applications through WAAP.

e) The remote support shall monitor the volume of incoming requests to identify unusual spikes or traffic surges.

f) The remote support shall track and flag requests coming from unusual or unexpected geographical locations.

g) The remote support shall analyze the types of clients (browsers, bots, etc.) accessing the system to spot potentially malicious bots.

h) The remote support shall watch for unusually large or malformed payloads in requests, which may be an indicator of an attack or misuse.

i) The remote support shall detect attempts to gain unauthorized access to privileged sections of the application.

j) The remote support shall track failed authentication attempts and abuse of API keys.

k) The remote support shall identify instances of API misuse, such as excessive resource consumption or non-standard query usage.

l) The remote support shall look for abnormal query strings or payloads that attempt to exploit SQL injection vulnerabilities.

m) The remote support shall track any attempts to inject malicious JavaScript or HTML code into pages.

n) The remote support shall watch for suspicious requests that may attempt to perform unauthorized actions on behalf of an authenticated user.

o) The remote support shall identify any attempt to execute system commands via user input.

11.15 Training

a) The bidder shall organize 2-days training programme every year during the original / extended (if applicable) contract on all the features, operational, administration and technical aspects of the complete solution for BHEL's operations & security administration team (15 to 20 persons). The first training shall be conducted within 2 months of the issue of acceptance certificate at BHEL premises. The training course shall be approved by the owner and the faculty shall be OEM certified.

b) The bidder shall arrange training on following courses from the original training provider within 2 years of the contract period:

i. EC-Council SOC Essentials: For 10 persons
ii. EC-Council Digital Forensics Essentials: For 5 persons
iii. EC-Council Certified Incident Handler: For 5 persons
iv. DSCI Certified Ransomware Rapid Responder: For 5 persons

In case of subscription courses, the subscription shall be arranged for a period of one year along with certification.

In case of offline courses, the training shall be arranged at the training provider's premises. The travel, boarding and lodging expense for BHEL participants will be borne by BHEL.

12 Transitioning / Exit

a) This clause sets out the provisions which will apply upon completion of the contract period or upon termination of the agreement for any reasons.

b) The ownership of the data generated upon usage of the system, at any point of time during the contract or expiry or termination of the contract, shall rest absolutely with BHEL.

c) If decided by BHEL, successful OEM/ bidder shall provide support to migrate/port log data to Cloud Compatible / On-Prem Data Storage in BHEL without any loss of existing log data without any additional cost.

d) In case of premature termination or end of contract, BHEL may move to other compatible storage, either on-premises or in any other Cloud Service Provider. In such a situation, the successful OEM / bidder shall provide support for log migration activity involving moving/porting the data to new storage (on prem/Cloud) successfully.

e) The bidder shall ensure that no data is deleted at the end of the Contract period for a minimum duration of six months beyond the expiry of the Contract period.

f) The successful bidder shall be responsible for providing the tools for import / export of VMs / Application Instance and content including data, documents, etc.

g) The successful bidder shall be responsible for preparation of the Transition / Exit Management Plan and carrying out the transition.

h) The successful bidder shall provide necessary support for migration of the VMs, data, content and any other assets to the new environment created by BHEL or any other Agency (on behalf of BHEL) on alternate cloud service provider's offerings / BHEL's premise to enable successful deployment and running of the solution on the new infrastructure.

i) The successful bidder shall keep a backup of all the data till the time all data is transferred to ensure nothing is lost during transition.

j) The successful bidder shall provide the data at transition in commonly readable format (such as CSV, XLS, XML etc.).

k) The successful bidder shall ensure that all the documentation required for smooth transition are kept up to date and all such documentation is handed over at the time of transition.

13 Performance Acceptance Test (PAT) & Commissioning

13.1 Commissioning Cum Acceptance Test

a) Once the successful bidder has declared the successful implementation of the solution, the same shall be tested for performance, functional and technical acceptance by BHEL. The solution shall be tested continuously for 7 days as per mutually agreed checklist based on technical and functional requirements. If any deficiencies are found, the bidder will be given 7 days to rectify/fine tune the solution. After rectification, the solution will again be tested for 7 days. On successful performance of the solution for 7 days, acceptance certificate will be given by BHEL.

b) If after the 2nd testing, the supplied solution is not able to meet PAT requirements, the successful bidder will be given another 7 days to rectify the problem, followed by 7 days of performance testing again. If the solution fails to perform as per PAT requirements in the 2nd test also, BHEL reserves the right to reject the supplied solution.

13.2 Commissioning Certificate by the Owner

On successful PAT and provisioning of required manpower, the successful bidder shall submit a complete project report having the following:

i. Configuration details of Cyber SOC i.e. SIEM, SOAR, UEBA, WAAP and other **Bill of Material** items.
ii. Security scheme for entire solution.
iii. Details of Backup policy and configuration.

On submission of the complete project report as above, BHEL will issue a Commissioning Certificate mentioning the commission date.

14 Payment Terms

a) An amount equal to 10% of the total contract value (excluding DFIR charges) shall be paid on commissioning of the solution after the successful bidder has received **"Commissioning Certificate"** from BHEL. This payment will be made within 90 days from the date of submission of invoices in triplicate duly certified by BHEL executive, within 60 days for Medium enterprises and

within 45 days for micro and small enterprises falling under MSME Act. after adjusting any deductions due to Late Delivery.

b) The balance 90% of the contract value (excluding DFIR charges) will be paid in quarterly arrears of 20 equal installments.

c) The 100 hours of digital forensics and incident response services will be invoked only on occurrence of a major incident or breach and payment will be made in lumpsum on actual consumption basis.

d) The payments will be made within 90 days from the date of submission of invoices in triplicate duly certified by BHEL executive, within 60 days for Medium enterprises and within 45 days for micro and small enterprises falling under MSME Act. after adjusting any deductions due to SLA non-conformance.

e) Payment will be made as per calendar quarters in Indian Rupees only.

f) Deductions due to Noncompliance of SLA per quarter will be maximum up to 20% of the quarterly charges.

g) The final payment at the end / or premature termination of contract, shall be done after the successful bidder has successfully provided all the log data / archives to BHEL for migration to other compatible storage, either on-premises or in any other Cloud Service Provider's datacenter.

h) In case of additional capacity, payment will be made on pro-rata basis. For additional capacity, only 90% of the contract value of the line item (SOC Services (SIEM, SOAR, UEBA), WAAP Services) will be considered for calculating the pro-rata rate.

15 Special Terms and Conditions:

15.1 General

a) The successful bidder shall assign a Technical Account Manager (TAM) from OEM for BHEL for the entire contract period. The TAM should be available on phone, email and VC, as and when required. If required, the TAM shall physically visit the site in case of a critical situation.

b) The SIEM solution and all its components shall preferably be an integrated platform from the same OEM. In case of third-party Agent and Log Collectors, the same shall be certified by the OEM of proposed SIEM Solution for complete seamless integration and interoperability with the OEM SIEM Solution.

c) All the items to be supplied must be NEW.

d) All the Items must be supplied in full and complete.

e) No item shall be offered whose end-of-sale or end of life has been declared by the OEM or has been declared to be under phase out.

15.2 Procedure for Submission & Opening of Bids:

Bids shall be submitted as per GeM Portal schedule.

The techno- commercial bid (Part-I) consists of Bounded volume of:

i. Technical offer/ details including literature/leaflets. The bidder can offer only as per technical specifications of the equipment. BHEL reserves the right to accept or reject the technical offer.
ii. Compliance for Technical Specifications as per format enclosed as Annexure-III.
iii. A copy of complete RFP along with corrigendum, if any, where each page is signed & stamped by the bidder.
iv. Compliance documents as per Annexure-XVI
v. Any other documents as per requirements of tender.

Part-II: Price Bid

Prices including GST to be quoted on GeM portal.

Price bid containing PRICES only is to be submitted in the price bid format enclosed as Annexure-V only before placement of order. Prices shall be quoted in Indian Rupees only.

Price Bid should not contain any technical details and/or Commercial Terms & Conditions as the same are supposed to be contained in PART-I only, so that the same can be evaluated before opening of Price Bid(s) in GeM. price Bid format is enclosed as Annexure- V. The changes in the Tax rates will be applicable as per actuals, subject to documentary evidence.

15.3 Evaluation of the bids

Evaluation of the bids shall be done in the following stages:

Stage-I:

After opening of the Techno-Commercial bids, the bidders shall be evaluated as per the prequalifying criteria as specified in the tender. Bidders shall meet each criteria in Pre-qualification Requirements (PQR). Only bidders meeting all the requirements of PQR shall proceed to Stage-II of evaluation.

Stage-II:

Bids of only those bidders who have qualified in Stage-I, shall be processed for Stage-II of evaluation. At Stage-II, bids of the Stage-I qualified bidders will be technically evaluated as per the technical specifications and requirements of the RFP. If required, BHEL may ask for a detailed presentation on the offered solution and a technical demonstration of the features in BHEL environment. If the bidder fails to demonstrate the technical capabilities and functionalities of the offered solution as per BHEL's technical specifications and requirements, the bid will be rejected and not evaluated further.

Stage-III:

In Stage-III, bids of only those bidders whose bids meet all the technical specifications and requirements at Stage-II, shall be processed for price bid opening and Reverse Auction (RA).

The bid having the least total cash outflow for 5 years will be considered L1 bidder. Evaluation of L1 ranking will be on the basis of total Charges including all applicable Taxes and Duties but excluding all input credits available to BHEL so as to assign tender priority based on cost to BHEL.

15.4 Release of Payment:

The bidder shall submit the following documents, within 15 days of completion of services for release of payment:

a) On commissioning of solution:

i. GST Invoices, in triplicate
ii. Commissioning certificate signed by BHEL
iii. Copy of Insurance

b) Quarterly Charges:

i. GST Invoices, in triplicate, at end of every quarter.
ii. SLA conformance report signed by BHEL representative certifying the uptime / downtime achieved during the quarter.

c) Annually:

Copy of Renewal of Insurance valid for the next one year.

15.5 Penalty for Late Delivery & Commissioning:

The bidder shall supply, install, configure and commission the entire solution within the specified time period as per **Clause 7 (Delivery Timelines)** of this RFP. If any solution (SOC/WAAP) is not commissioned within the stipulated time period, a penalty shall be levied at the rate of 0.5% per week (or part thereof) subject to maximum of 10% of the total value of the undelivered solution, i.e. penalty due to LD will be levied individually on SOC and WAAP depending on which one is delayed. This penalty will be deducted from the first payment, and in case the penalty amount to be deducted is more than the first payment, the same will be adjusted from the subsequent payments.

In case penalty becomes recoverable, the applicable GST shall also be recoverable from the bidder.

15.6 Penalty for Continuous Poor SLA Conformance:

If uptime of any component of the solution or various SLA parameters falls below 90% continuously for two (02) quarters, BHEL will issue rectification notice to the successful bidder giving one month's time period to the successful bidder for rectification. If the successful bidder fails to improve the solution uptime or rectify the problem within the notice period, then, BHEL reserves the right to forfeit the security deposit / PBG of the successful bidder and / or terminate the contract in part or full. For the affected / terminated services, charges payable upto the issue date of rectification notice shall be payable, and no charges shall be payable for the affected / terminated services beyond the rectification notice.

15.7 Contract Extension:

The contract may be extended (in part or full) upto a period of 2 years (post completion of original contract period of 5 years) based solely on BHEL's requirement and at mutually agreeable terms & conditions.

15.8 Non-Disclosure Agreement (NDA):

a) The successful bidder shall comply with the Information Security Management System of BHEL (ISO/IEC 27001:2022) and work within the framework of ISMS as applicable in BHEL from time-to-time.

b) All the material / information sent to the successful bidder shall be treated as confidential and should not be disclosed in any matter to any unauthorized person under any circumstances. The successful bidder has to furnish a Mutual Non- Disclosure Agreement (NDA) ***(as per Annexure - VI***) in line with the Owner's Information Security Management System (ISMS).

16 General Terms & Conditions of the contract

16.1 Earnest Money Deposit (EMD)

a) Bidder has to deposit EMD of Rs.20,00,000/- (Rupees Twenty Lakhs only) as a part of subject tender and the same should be in the following forms:

i. Cash deposit as permissible under the extant Income Tax Act (before tender opening).
ii. Electronic Fund Transfer credited in BHEL account (before tender opening)

BANK NAME:	KOTAK MAHINDRA BANK
ADDRESS:	G-F 3A-3J GROUND FLOOR, AMBA DEEP, 14 K.G. MARG, NEW DELHI-1
IFSC:	KKBK0000172
CA No.:	9011196535
BANK ACCOUNT NAME:	BHARAT HEAVY ELECTRICALS LTD.

iii. Banker's cheque/ Pay order/ Demand draft, in favour of BHEL (along with offer)
iv. Fixed Deposit Receipt (FDR) issued by Scheduled Banks/ Public Financial Institutions as defined in the Companies Act (FDR should be in the name of the Contractor, a/c BHEL.
v. Insurance Surety Bonds

In addition to above, the EMD amount in excess of Rs Two lakh may also be accepted in the form of Bank Guarantee from scheduled banks as per Annexure XII.

For instance, if EMD amount is Rs.20,00,000/-, BG can be submitted for Rs.18,00,000/- and rest Rs.2,00,000/- to be submitted through other modes as mentioned above. The Bank Guarantee in such cases shall be valid for at least six months.

i. EMD in any other forms/modes except the forms/modes mentioned above will lead to the rejection of bid i.e. No other form of EMD remittance shall be acceptable to BHEL.
ii. EMD submitted by bidder will be forfeited if bidder revokes his tender within validity period.
iii. EMD to be submitted prior or at the time of bid submission. Tender without requisite EMD will not be considered for further evaluation.
iv. Exemption of EMDs shall be as per GeM terms & conditions.

b) **No interest shall be payable by BHEL on EMD amount.** The EMD shall be forfeited in case of:

i. Withdrawal of bid or increase in rates or change in bid conditions after opening of the tender.
ii. Refusal to enter into a contract after the award of contract.
iii. If operations of the contract are not commenced from the date indicated in the award of contract.

c) The EMD will be refunded to the unsuccessful bidders within fifteen days of acceptance of award of work by the successful bidder(s) / expiry of the validity of the bid, whichever is earlier.

16.2 Security Deposit / Performance Bank Guarantee (PBG):

a) Upon acceptance of Tender, the successful Tenderer should deposit the 10% of the contract value (excluding DFIR charges mentioned in part-II of Annexure -V) and excluding taxes, as Security Deposit towards fulfilment of any obligations in terms of the provisions of the contract.

EMD of the successful tenderer shall be converted and adjusted towards the required amount of Security Deposit.

b) **Modes of deposit:**

The balance amount to make up the required Security Deposit of the contract value may be accepted in the following forms:

i. Cash (as permissible under the extant Income Tax Act).
ii. Local cheques of Scheduled Banks (subject to realization)/ Pay Order/ Demand Draft/ Electronic Fund Transfer in favour of BHEL.
iii. Bank Guarantee from Scheduled Banks/ Public Financial Institutions as defined in the Companies Act. The Bank Guarantee format for Security Deposit shall be in the prescribed formats.
iv. Fixed Deposit Receipt issued by Scheduled Banks/ Public Financial Institutions as defined in the Companies Act (FDR should be in the name of the Contractor, a/c BHEL).
v. Securities available from Indian Post offices such as National Savings Certificates, Kisan Vikas Patras etc. (held in the name of Contractor furnishing the security and duly endorsed/ hypothecated/ pledged, as applicable, in favour of BHEL).
vi. Insurance Surety Bonds

(Note: BHEL will not be liable or responsible in any manner for the collection of interest or renewal of the documents or in any other matter connected therewith)

c) **Collection of Security:**

At least 50% of the required Security Deposit, including the EMD, should be collected before start of the work. Balance of the Security Deposit can be collected by deducting 10% of the gross amount progressively from each of the running bills of the Contractor till the total amount of the required Security Deposit is collected.

In case of delay in submission of performance security, enhanced performance security which would include interest (Repo rate + 4%) for the delayed period, shall be submitted by the bidder.
If the value of work done at any time exceeds the contract value, the amount of Security Deposit shall be correspondingly enhanced and the additional Security Deposit shall be immediately deposited by the Contractor or recovered from payment/s due to the Contractor.

The recoveries made from running bills (cash deduction towards balance SD amount) can be released against submission of equivalent Bank Guarantee in acceptable form, but only once, before completion of work, with the approval of the authority competent to award the work.

i. Payment can be released only after collection/ recovery of initial 50% Security Deposit.
ii. The Security Deposit shall not carry any interest.
iii. There is no exemption of Performance security deposit submission.
iv. In case the value of work exceeds the awarded / accepted value, the Security Deposit shall be correspondingly enhanced as given below:
    a) The enhanced part of the Security Deposit shall be immediately deposited by the Contractor or adjusted against payments due to the Contractor.

b) Contract value for the purpose of operating the increased value of Security Deposit due to Quantity Variation, shall be exclusive of Price Variation Clause, Over Run Compensation and Extra works done on man-day rates.
c) The recoveries made from running bills (cash deduction towards balance SD amount) can be released against submission of equivalent Bank Guarantee in acceptable form, but only once, before completion of work, with the approval of competent authority of BHEL.

v. The validity of Bank Guarantees towards Security Deposit shall be initially up to the completion period as stipulated in the Letter of Intent/ Award + Guarantee Period + 3 months, and the same shall be kept valid by proper renewal by the contractor till the acceptance of Final Bills of the Contractor by BHEL.
vi. In case of extension, the PBG shall be provided for a further period equivalent to the extended period. The PBG shall be kept valid till the extended Contract period plus 3 months.
vii. BHEL reserves the right of forfeiture of Security Deposit in addition to other claims and penalties in the event of the Contractor's failure to fulfil any of the contractual obligations or in the event of termination of contract as per terms and conditions of contract. BHEL reserves the right to set off the Security Deposit against any claims of other contracts with BHEL.

d) **Return of Security Deposit:**

Security Deposit shall be returned to the contractor upon fulfilment of contractual obligations as per terms of the contract and after completion of contract period plus 90 days, after deducting all expenses / other amounts due to BHEL under the contract / other contracts entered into with them by BHEL.

BANK GUARANTEES: Wherever Bank Guarantee is to be furnished/submitted by the Contractor, the following shall be complied with

i. Bank Guarantee shall be from Scheduled Banks / Public Financial Institutions as defined in the Companies Act.
ii. The Bank Guarantee shall be as per prescribed formats.
iii. It is the responsibility of the contractor to get the Bank Guarantee revalidated / extended for the required period, as per the advice of BHEL. BHEL shall not be liable for issue of any reminders regarding expiry of the Bank Guarantee.
iv. In case the Bank Guarantee is not extended before the expiry date, BHEL reserves the right to invoke the same by informing the concerned Bank in writing, without any advance notice/communication to the concerned contractor.
v. Bidders to note that any corrections to Bank Guarantee shall be done by the issuing Bank, only through an amendment in an appropriate non-judicial stamp paper.

16.3 Taxes & Duties

i. Price should be inclusive of all applicable Taxes/ Charges except GST. GST amount shall be included in price bid as per the price-bid format while submitting price bid in GeM. The Contractor shall pay all other taxes, fees, royalty, commission etc. which may be levied on the contractor in executing the contract. In case BHEL is forced to pay any of such taxes, it shall be recovered from Contactor's bills or otherwise as deemed fit.
ii. TDS under GST law as applicable shall be deducted.
iii. To enable BHEL to avail GST input tax credit, Vendor shall submit GST compliant invoice containing all the particulars as stipulated under Invoice Rules of GST Law. Payment shall be made to the Vendor only after submission of GST complaint invoice. The successful bidder shall raise GST compliant invoice affixing GSTIN of BHEL's unit availing the services. Vendor

to ensure that details of such invoice is furnished by him in his GSTR-1 return and the same is appearing in GSTR-2B of BHEL.

iv. BHEL reserves the right to protect its interest against any loss on account of non-availability of GST credit.
v. GSTIN of BHEL will be provided to the Vendor along with the work order.
vi. Any new/change in statutory levy as and when made applicable by the Government shall become applicable against documentary evidence.
vii. Statutory variation for GST is payable to the Seller during validity of the contract. However, for period beyond the contract validity, BHEL may reimburse the actual applicable increased tax, in exceptional circumstances, in case BHEL is able to take the input tax credit. However, the decision of BHEL in this regard will be final and binding on the seller/ contractor otherwise vendor/ contractor has to bear the differential upward increase in tax. Any decrease in GST rate shall be passed on to BHEL.
viii. Payment to the Vendor will be subjected to TDS as per rules in force from time to time. The Tax Deduction at Source (TDS) shall be done as per the provisions of Income Tax Act & GST, as amended from time to time and a certificate to this effect shall be provided to the Vendor by BHEL.
ix. Invoice submitted should be in the format as specified under GST Laws viz. all details as mentioned in Invoice Rules like GSTIN registration number, invoice number, quantity, rate, value, taxes with nomenclature – CGST, SGST, IGST mentioned separately, HSN (Harmonized System of Nomenclature) Code / SAC (Services Accounting Code) etc.
x. The Vendor has to give an undertaking that GST as mentioned in the invoice has been / will be paid and also file return as per respective extant rule

16.4 Sub-Contracting

Order / contract or any part thereof shall not be sub-contracted, assigned or otherwise transferred to any third party without prior written consent of BHEL.

16.5 Cost of Bidding:

The Bidder shall bear all costs associated with the preparation and submission of its bid and the Purchaser will in no case be responsible or liable for those costs.

16.6 Deviations:

Bids shall be submitted strictly in accordance with the requirements and terms & conditions of the Tender Enquiry. Vendors have to submit a “No Deviation Certificate” in Part-I of the offer as per **Annexure VI**.

Technical & Commercial - No deviation is acceptable.

16.7 Validity of Offer:

Offer shall be valid as per GeM portal and further offer validity extension may be sought during bid evaluation, if required.

16.8 Purchaser’s Right:

The Purchaser reserves the right to make changes within the scope of the contract in following respects at any point of time.

BHEL may, at any time during the contract period, by a written order given to the Service Provider, make changes within the general scope of the contract like change of location for provisioning of services within the campus.

BHEL reserves the right to cancel the tender process at any stage/time without providing any reason/justification.

16.9 Merger & Acquisition:

In case of merger / acquisition of the bidder / OEM during the contract period, all commitments and liabilities with respect to this contract will pass on to the acquiring entity.

16.10 Insolvency:

If during the execution of contract, the company or any member in case of JV/consortium / partnership becomes bankrupt or otherwise insolvent, the purchaser may terminate the contract by giving written notice to the supplier. Any charges payable up to the termination point will be paid by BHEL to the supplier. In case any recovery is due on supplier, the recoverable amount will be adjusted against the terminal payment to be made to the supplier. Such termination will not prejudice or affect any right of action or remedy which has accrued and/ or will accrue thereafter to BHEL.

16.11 Indemnification:

Seller/ Contractor/ Vendor shall fully indemnify and keep indemnified the Purchaser against all claims of whatsoever nature arising during the course and out of the execution of this Order/Contract.

16.12 Insurance:

The equipment supplied under this contract shall be fully insured by the bidder against any loss, theft, fire, damage due to any reason, etc., during transportation, storage, delivery, installation and operation for the entire period of the contract.

For any theft or damage to any of the supplied items, where the bidder / Service Provider is filing a claim with the insurance agency; the bidder shall replace the item on its own within 15 working days of the reporting of the incident, after which SLA clause of the contract will become applicable. The vendor shall submit evidence of insurance policy to BHEL at the time of commissioning of the solution, and thereafter every year on renewal of the policy.

16.13 Breach of contract, Remedies and Termination

a) The following shall amount to breach of contract:

i. Non-supply of material/ non-completion of work/services by the Supplier/Vendor within scheduled delivery/ completion period as per contract or as extended from time to time.
ii. The Supplier/Vendor fails to perform as per the activity schedule and there are sufficient reasons even before expiry of the delivery/ completion period to justify that supplies shall be inordinately delayed beyond contractual delivery/ completion period.
iii. The Supplier/Vendor delivers equipment/Service/ material not of the contracted quality.
iv. The Supplier/Vendor fails to replace the defective equipment/ material/ component as per guarantee clause, if applicable.
v. Withdrawal from or abandonment of the work/services by the Supplier/Vendor before completion as per contract.

vi. Assignment, transfer, subletting of Contract by the Supplier/Vendor without BHEL's written permission resulting in termination of Contract or part thereof by BHEL.
vii. Non-compliance to any contractual condition or any other default attributable to Supplier/Vendor.
viii. Any other reason(s) attributable to Vendor towards failure of performance of contract. In case of breach of contract, BHEL shall have the right to terminate the Purchase Order/ Contract either in whole or in part thereof without any compensation to the Supplier/Vendor.
ix. Any of the declarations furnished by the contractor at the time of bidding and/ or entering into the contract for supply are found untruthful and such declarations were of a nature that could have resulted in non-award of contract to the contractor or could expose BHEL and/ or Owner to adverse consequences, financial or otherwise.
x. Supplier/Vendor is convicted of any offence involving corrupt business practices, antinational activities or any such offence that compromises the business ethics of BHEL, in violation of the Integrity Pact entered into with BHEL has the potential to harm the overall business of BHEL/ Owner.

Note- Once BHEL considers that a breach of contract has occurred on the part of Supplier/Vendor, BHEL shall notify the Supplier/Vendor by way of notice in this regard. Contractor shall be given an opportunity to rectify the reasons causing the breach of contract within a period of 14 days.

In case the contractor fails to remedy the breach, as mentioned in the notice, to the satisfaction of BHEL, BHEL shall have the right to take recourse to any of the remedial actions available to it under the relevant provisions of contract.

b) **Remedies in case of Breach of Contract.**

i. Wherein the period as stipulated in the notice issued under clause 16.13.a has expired and Supplier/Vendor has failed to remedy the breach, BHEL will have the right to terminate the contract on the ground of "Breach of Contract" without any further notice to contractor.

ii. Upon termination of contract, BHEL shall be entitled to recover an amount equivalent to 10% of the Contract Value for the damages on account of breach of contract committed by the Supplier/Vendor. This amount shall be recovered by way of encashing the security instruments like performance bank guarantee etc. available with BHEL against the said contract. In case the value of the security instruments available is less than 10% of the contract value, the balance amount shall be recovered from other financial remedies (i.e. available bills of the Supplier/Vendor, retention amount, from the money due to the Supplier/Vendor etc. with BHEL) or the other legal remedies shall be pursued.

iii. Wherever the value of security instruments like performance bank guarantee available with BHEL against the said contract is 10% of the contract value or more, such security instruments to the extent of 10% contract value will be encashed. In case no security instruments are available or the value of the security instruments available is less than 10% of the contract value, the 10% of the contract value or the balance amount, as the case may be, will be recovered in all or any of the following manners:
    a) In case the amount recovered under sub clause (ii) above is not sufficient to fulfil the amount recoverable then; a demand notice to deposit the balance amount within 30 days shall be issued to Supplier/Vendor.
    b) If Supplier/Vendor fails to deposit the balance amount within the period as prescribed in demand notice, following action shall be taken for recovery of the balance amount:

a) from dues available in the form of Bills payable to defaulted Supplier/Vendor against the same contract.

b) If it is not possible to recover the dues available from the same contract or dues are insufficient to meet the recoverable amount, balance amount shall be recovered from any money(s) payable to Supplier/Vendor under any contract with other Units of BHEL including recovery from security deposits or any other deposit available in the form of security instruments of any kind against Security deposit or EMD.

vi) In-case recoveries are not possible with any of the above available options, Legal action shall be initiated for recovery against defaulted supplier/Vendor.

vii) It is an agreed term of contract that this amount shall be a genuine pre-estimate of damages that BHEL would incur in completion of balance contractual obligation of the contract through any other agency and BHEL will not be required to furnish any other evidence to the Supplier/Vendor for the purpose of estimation of damages.

viii) In addition to the above, imposition of liquidated damages, debarment, termination, de-scoping, short-closure, etc., shall be applied as per provisions of the contract.

Note:

The defaulting Supplier/Vendor shall not be eligible for participation in any of the future enquiries floated by BHEL to complete the balance work. The defaulting contractor shall mean and include:

i. In case defaulted Supplier/Vendor is the Sole Proprietorship Firm, any Sole Proprietorship Firm owned by same Sole Proprietor.
ii. In case defaulted Supplier/Vendor is The Partnership Firm, any firm comprising of same partners/ some of the same partners; or sole proprietorship firm owned by any partner(s) as a sole proprietor.

16.14 Termination of The Contract & Its Consequences

16.14.1 Purchaser reserves the right to terminate the order/contract, either wholly or in part, upon situations arising due to non-compliance of stipulations of the Order/contract by Vendor.

16.14.2 Vendor shall continue the performance of the order/contract under all circumstances, to the extent not cancelled.

16.14.3 BHEL reserves the rights to cancel the contract in case the services are not found to be satisfactory.

16.14.4 Consequences: As soon as the contract is cancelled / terminated by BHEL, no payment will be payable to Vendor.

16.15 Ethical Standard:

Bidders are expected to observe the highest standard of ethics during the procurement and execution of this Contract. In pursuit of this policy, the Purchaser will reject a proposal for award if it finds out that the Bidder being considered for award has engaged in corrupt or fraudulent practices

in competing for the Contract. For the purposes of this provision, the terms set forth below are defined as follows:

a) **"Corrupt practice"** means the offering, giving, receiving, or soliciting of anything of value to influence the action in the procurement process or in Contract execution; and
b) **"Fraudulent practice"** means a misrepresentation of facts in order to influence a procurement process including collusive practices designed to establish bid prices at artificial, non-competitive levels to deprive the Purchaser of the benefits of competition;

The Bidder along with its associate/ collaborators/ sub-contractors/ sub-vendors/ consultants/ service providers shall strictly adhere to BHEL Fraud Prevention Policy displayed on BHEL website http://www.bhel.com and shall immediately bring to the notice of BHEL Management about any fraud or suspected fraud as soon as it comes to their notice.

By signing the Bid Forwarding Letter, the Bidder represents that for the software it supplies, it is the owner of the Intellectual Property Rights in the software. Wilful misrepresentation of these facts shall be considered a fraudulent practice without prejudice to other remedies that the Purchaser may take.

16.16 Suspension of Business Dealings with suppliers/contractors:

The offers of the bidders who are under suspension as also the offers of the bidders, who engage the services of the banned firms / principal / agents, shall be rejected. The list of banned firms is available on BHEL web site www.bhel.com.

If any bidder / supplier / contractor during pre-tendering / tendering / post tendering / award / execution / post-execution stage indulges in any act, including but not limited to, mal-practices, cheating, bribery, fraud or and other misconduct or formation of cartel so as to influence the bidding process or influence the price or tampers the tendering process or acts or omits in any manner which tantamount to an offence punishable under any provision of the Indian Penal Code, 1860(Bhartiya Nyaya Samhita 2023) or any other law in force in India, or does anything which is actionable under the Guidelines for Suspension of Business dealings, action may be taken against such bidder / supplier / contractor as per extant guidelines of the company available on www.bhel.com and / or under applicable legal provisions. Guidelines for suspension of business dealings is available in the webpage:

http://www.bhel.com/vender_registration/vender.php.

Bid should be free from correction, overwriting, using corrective fluid, etc. Any interlineation, cutting, erasure or overwriting shall be valid only if they are attested under full signature(s) of person(s) signing the bid else bid shall be liable for rejection. In the event of any Technical or Commercial queries, the same may please be addressed to the following BHEL concerned before Part I opening-

For all clarifications/issues related to the tender, please contact:
Contact Person: Anwar Hussain, AGM / Devendra Sharma, SDGM
Contact Address: CDT, BHEL, Sector-16A Noida
Email: anwar.h@bhel.in / devendrasharma@bhel.in
Phone: 0120-2416546/6499

16.17 Cartel Formation

The Bidder declares that they will not enter into any illegal or undisclosed agreement or understanding, whether formal or informal with other Bidder(s). This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process. In case, the Bidder is found having indulged in above activities, suitable action shall be taken by BHEL as per extant policies/ guidelines.

16.18 Force Majeure

The conditions of Force Majeure shall mean the events beyond control of the parties effected such as act of God, Earthquake, Flood, Devastating fire, War, Civil Commotion, Cyclone, Industrial Lockout and Statutory Act of the Government having bearing on the performance of the Contract. The party affected by Force Majeure shall be obliged to notify the other party within 48 hours, by fax/cable, of the commencement and the end of the Force Majeure circumstances preventing its performance of all or any of its obligations under this order. If performance of obligations under this order is delayed for more than one month due to a continuous Force Majeure, the party not affected by Force Majeure may at any time thereafter while such Force Majeure continues, by notice in writing forth with terminate all or any part of the unperformed portion this order. If this order or any portion thereof is terminated under Force Majeure conditions, the Contractor shall be liable to BHEL for any damages, losses or liabilities as result thereof.

16.19 Integrity Pact (IP):

a) IP is a tool to ensure that activities and transactions between the Company and its Bidders/Contractors are handled in fair, transparent and corruption free manner. Following Independent External Monitors (IEMs) on the present panel have been appointed by BHEL with the approval of CVC to oversee implementation of IP in BHEL.

SI	IEM	Email
~~1~~	~~Shri Otem Dai, IAS (Retd.)~~	~~iem1@bhel.in~~
2	Shri Bishwamitra Pandey, IRAS (Retd.)	iem2@bhel.in
3	Shri Mukesh Mittal, IRS (Retd.)	iem3@bhel.in

b) The IP as enclosed with the tender (Annexure-VIII) is to be submitted (duly signed by authorized signatory who signs in the offer) along with bid. Only those bidders who have entered into such an IP with BHEL would be competent to participate in the bidding. In other words, entering into this Pact would be a preliminary qualification.

c) Please refer Section-8 of IP for Role and Responsibilities of IEMs. In case any complaint arising out of the tendering process, the matter may be referred to the IEM mentioned in the tender.

Note:

No routine correspondences shall be addressed to the IEM (phone/post/email) regarding the clarifications, time, extensions or any other administrative queries, etc. on the tender issues. All such clarifications/ issues shall be addressed directly to the tender issuing (procurement) department.

For all clarifications/issues related to the tender, please contact:

Contact Person: Nivedita, Manager / Pradeep Kumar, Engineer
Contact Address: CDT, BHEL, Sector-16A Noida
Email: Nivedita@bhel.in / pradeepkumar@bhel.in
Phone: 0120-2416482 / 6493

16.20 Settlement of Disputes:

If any dispute or difference of any kind whatsoever shall arise between BHEL and the Supplier/Vendor, arising out of the contract for the performance of the work whether during the progress of contract termination, abandonment or breach of the contract, it shall in the first place referred to Designated Engineer for amicable resolution by the parties. Designated Engineer (to be nominated by BHEL for settlement of disputes arising out of the contract) who within 60 days after being requested shall give written notice of his decision to the contractor. Save as hereinafter provided, such decision in respect of every matter so referred shall forthwith be given effect to by the Supplier/Vendor who shall proceed with the work with all due diligence, whether he or BHEL desires to resolve the dispute as hereinafter provided or not.

If after the Designated Engineer has given written notice of this decision to the party and no intention to pursue the dispute has been communicated to him by the affected party within 30 days from the receipt of such notice, the said decision shall become final and binding on the parties. In the event the Supplier/Vendor being dissatisfied with any such decision or if amicable settlement cannot be reached then all such disputed issues shall be resolved through conciliation in terms of the BHEL Conciliation Scheme 2018 as per 'Conciliation' clause below.

a) **Conciliation:**

Any dispute, difference or controversy of whatever nature howsoever arising under or out of or in relation to this Agreement (including its interpretation) between the Parties, and so notified in writing by either Party to the other Party (the "Dispute") shall, in the first instance, be attempted to be resolved amicably in accordance with the conciliation procedure as per BHEL Conciliation Scheme 2018. The proceedings of Conciliation shall broadly be governed by Part-III of the Arbitration and Conciliation Act 1996 or any statutory modification thereof and as provided in - "Procedure for conduct of conciliation proceedings" (as available on www.bhel.com)).

b) **Arbitration:**

i. Except as provided elsewhere in this Contract, in case Parties are unable to reach amicable settlement (whether by Conciliation to be conducted as provided in Clause 'Conciliation' herein above or otherwise) in respect of any dispute or difference; arising out of the formation, breach, termination, validity or execution of the Contract; or, the respective rights and liabilities of the Parties; or, in relation to interpretation of any provision of the Contract; or. in any manner touching upon the Contract (hereinafter referred to as the 'Dispute'), then, either Party may, refer the disputes to Arbitral Institution (IIAC" (India International Arbitration Centre) for Delhi/NCR offices) and such dispute to be adjudicated by Sole Arbitrator appointed in accordance with the Rules of said Arbitral Institution.

ii. A party willing to commence arbitration proceeding shall invoke Arbitration Clause by giving notice to the other party in terms of section 21 of the Arbitration & Conciliation Act, 1996 (hereinafter referred to as the 'Notice') before referring the matter to arbitral institution. The Notice shall be addressed to the Head of the Region, Power Sector/ Unit, BHEL, executing the Contract and shall contain the particulars of all claims to be referred to arbitration with sufficient detail and shall also indicate the monetary amount of such claim including interest, if any.

iii. After expiry of 30 days from the date of receipt of aforesaid notice, the party invoking the Arbitration shall submit that dispute to the Arbitral Institutions and identified by contract issuing agency and that dispute shall be adjudicated in accordance with their respective Arbitration Rules. The matter shall be adjudicated by a Sole Arbitrator who shall necessarily be a Retd Judge having considerable experience in commercial matters to be appointed/nominated by the respective institution. The cost/expenses pertaining to the said Arbitration shall also be governed in accordance with the Rules of the respective Arbitral Institution. The decision of the party invoking the Arbitration for reference of dispute to a specific Arbitral institution for adjudication of that dispute shall be final and binding on both the parties and shall not be subject to any change thereafter. The institution once selected at the time of invocation of dispute shall remain unchanged.

iv. The fee and expenses shall be borne by the parties as per the Arbitral Institutional rules.

v. The Arbitration proceedings shall be in English language and the seat and venue of Arbitration shall be New Delhi.

vi. Subject to the above, the provisions of Arbitration & Conciliation Act 1996 and any amendment thereof shall be applicable. All matters relating to this Contract and arising out of invocation of Arbitration clause are subject to the exclusive jurisdiction of the Court(s) situated at New DelhI.

vii. Notwithstanding any reference to the Designated Engineer or Conciliation or Arbitration herein, a. the parties shall continue to perform their respective obligations under the Contract unless they otherwise agree. Settlement of Dispute clause cannot be invoked by the Contractor, if the Contract has been mutually closed or 'No Demand Certificate' has been furnished by the Contractor or any Settlement Agreement has been signed between the Employer and the Contractor.

viii. It is agreed that Mechanism of resolution of disputes through arbitration shall be available only in the cases where the value of the dispute is less than Rs. 10 Crores.

ix. In case the disputed amount (Claim, Counter claim including. interest is Rs. 10 crores and above, the parties shall be within their rights to take recourse to remedies other than Arbitration, as may be available to them under the applicable laws after prior intimation to the other party. Subject to the aforesaid conditions, provisions of the Arbitration and Conciliation Act, 1996 and any statutory modifications or re-enactment thereof as amended from time to time, shall apply to the arbitration proceedings under this clause.

x. In case, multiple arbitrations are invoked (whether sub-judice or arbitral award passed) by any party to under this contract, then the cumulative value of claims (including interest claimed or awarded) in all such arbitrations shall be taken in account while arriving at the total claim in dispute for the subject contract for the purpose of clause 16.20.b.ix above. Disputes having cumulative value of less than 10 crores shall be resolved through arbitration and any additional dispute shall be adjudicated by the court of competent jurisdiction.

c) **In case of Contract with Public Sector Enterprise (PSE) or a Government Department, the following shall be applicable:**

In the event of any dispute or difference relating to the interpretation and application of the provisions of commercial contract(s) between Central Public Sector Enterprises (CPSEs)/ Port Trusts inter se and also between CPSEs and Government Departments/Organizations (excluding disputes concerning Railways, Income Tax, Customs & Excise Departments), such dispute or difference shall be taken up by either party for resolution through AMRCD (Administrative Mechanism for Resolution of CPSEs Disputes) as mentioned in DPE OM No. 05/0003/2019-FTS-10937 dated 14-12-2022 as amended from time to time.

16.21 Jurisdiction:

Subject to clause 'Settlement of disputes' above of this contract, the Civil Court having original Civil Jurisdiction (Delhi) shall alone have exclusive jurisdiction in regard to all matters in respect of the Contract.

16.22 Governing Laws

The contract shall be governed by the Law for the time being in force in the Republic of India.

16.23 No Interest Payable To contractor/vendor

No interest shall be payable on the security deposit or any other money due to the contractor/vendor.

16.24 Pre-Bid Conference:

a) The bidders are expected to carefully go through this Tender Document and understand all the requirements thoroughly before submitting their offer. All legitimate queries and clarifications regarding this tender must be submitted in enclosed Annexure -XV and addressed to the official inviting the offers. All these queries will be clarified in the Pre-Bid Meeting.
b) Pre-Bid conference of the Bidders shall be convened at the designated date, time and place. Each Bidder shall be allowed to participate on production of authority letter from the Bidder.
c) During the course of Pre-Bid conference, the Bidders will be free to seek clarifications and make suggestions for consideration. BHEL shall endeavor to provide clarifications and such further information as it may, in its sole discretion, consider appropriate for facilitating a fair, transparent and competitive Bidding Process
d) Vendors participating in pre-bid conference, preferably do site survey prior to the pre-bid conference with information and acceptance by BHEL.

16.25 Other Compliance:

The compliance to the labour and other laws shall be applicable which is also mentioned in GeM GTC.

16.26 Other Terms & Conditions:

All other term & conditions of this specification not mentioned above shall be governed by the pertinent provisions of GeM terms and Conditions.

16.27 List of Annexures:

1	Annexure-I	Make and Model Offered
2	Annexure-II	Illustrative Schematic of Architecture & Deployment
3	Annexure-III	Technical Specifications
4	Annexure-IV	Tentative list of data sources
5	Annexure-V	Price Bid Format.
6	Annexure-VI	Mutual Non-Disclosure Agreement Format
7	Annexure-VII	No-Deviation Format
8	Annexure-VIII	Integrity Pact
9	Annexure-IX	Declaration regarding Insolvency/Liquidation/Bankruptcy proceedings
10	Annexure-X	Declaration regarding compliance to Restrictions under Rule 144 (xi) of GFR (Local Content Certificate)
11	Annexure-XI	Model Certificate
12	Annexure-XII	Proforma of Bank Guarantee for Earnest money
13	Annexure-XIII	Proforma of Bank Guarantee for Performance Guarantee
14	Annexure-XIV	List of consortium banks
15	Annexure-XV	Pre-bid query format
16	Annexure-XVI	Tender Checklist

Make and Model Offered

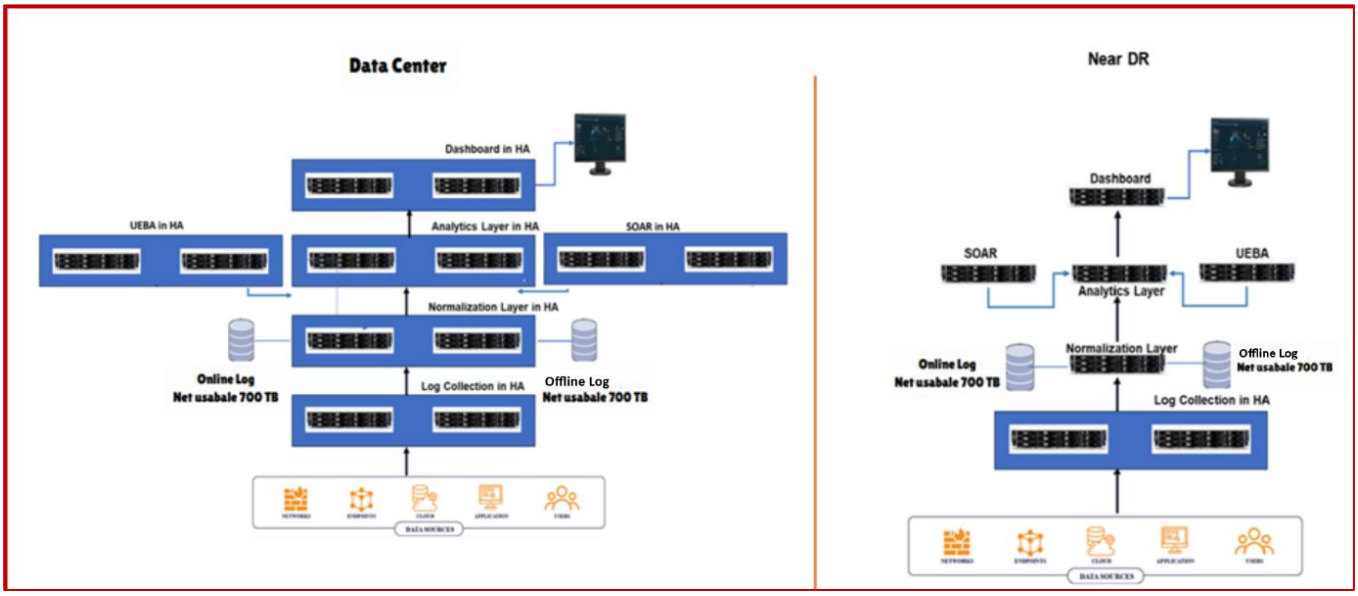
Product	**OEM**	**Model**
SIEM		
SOAR		
UEBA		
WAAP		
Display Units		
PC		
Laptops		

The detailed BOM (including hardware and software) for the complete solution to be provided by the bidder along with this Annexure.

Seal & Signature of the Company

Annexure - II

Illustrative Schematic of Architecture & Deployment



The above illustrative diagram depicting minimum level of redundancy and storage requirement is to be provisioned by the bidder and shall be vetted by the OEM of the solution.

Seal & Signature of the Company

Annexure – III

Technical Specifications

Cyber SOC		
General		
S. No.	**Specification**	**Bidder's Compliance (Yes/No)**
1	The SOC solution shall be on prem and must include log ingestion to on prem SIEM solution	
2	The SOC solution with all its components shall be an integrated solution preferably from a single OEM.	
3	The SOC solution must provide central management of all the components from a single web-based user interface.	
4	All underlying hardware, software, appliances, OS, application, database etc. required for establishment of SOC Solution including licenses, fiber modules, fiber patch cords should be bundled with the solution.	
5	The SOC solution shall be based on big data capabilities and should be scalable both horizontally and vertically.	
6	The SOC solution shall allow creation of different storage groups based on number of different data sources.	
7	The SOC solution shall collect, aggregate, filter, store, triage, correlate, and display security-relevant data, supporting both real-time and historical review and analysis.	
8	The SOC solution should be integrated with Global Threat feed. The solution should have provision to integrate additional 3rd party Threat feeds.	
9	The SOC solution must support log collection and correlation from all devices including Security devices, SAP, Applications, Databases, Network devices, Operating Systems, Storage Systems. Any un-supported device must be integrated at NO additional cost within the contract period. The Bidder must share the List of Out-Of-The-Box supported devices and Log types.	
10	The SOC solution should support standard log formats such as Syslog, CEF (Common Event Format), LEEF (Log Event Extended Format), JSON, etc.	
11	The SOC solution shall have the capability to encrypt data in transit and rest at all the layers/ components.	
12	The transmission of log data within the SOC solution (from one storage type to another) shall be encrypted.	
13	The proposed solution shall support both agent and agent less log collection, with customization/filtering.	
14	The Solution should provide the ability to encrypt communications between components without impacting log performance.	
15	The solution must integrate with 3rd party directory services (LDAP /AD) as an authentication method.	
16	The Solution should integrate asset information and use the same for Correlation and Incident Management.	

17	The solution shall be capable of capturing and displaying log collection time and event time of the logs. Collection time means when the logs have reached to the SIEM and event time means when the event has generated on end device.	
18	The solution shall support restricting data collection from only allowed IP addresses/ Hostnames/ FQDN etc.	
19	The shall collect raw data in it's native format and make it available for both real time and historical co-relations and searches.	
20	The SIEM shall have native capability to forward data in raw log format to other cloud based platforms.	
21	The Solution should have various Roles for SIEM Administration i.e. Administrator, Operator, Analyst etc.	
22	The proposed SIEM solution should support MITRE ATT&CK framework and provide a navigator for the same. It should allow mapping alerts and incidents with MITRE ATT&CK tactics, techniques and procedures. It should help in identifying gaps in log data for mapping alerts / incidents to MITRE ATT&CK Technique & Sub techniques.	
Log Collection & Aggregation Layer		
23	Log Collection Layer should be capable of log aggregation and filtration to ensure no unwanted logs travel upwards and consolidates multiple identical raw events into one processed event.	
24	Log Collectors should have a Log compression ability before forwarding the logs	
25	Log Collection should be capable to collect IP Flow logs of Network.	
26	Solution should support log collection for IPv4 as well as for IPv6.	
27	Log data shall be compressed(lossless Compression) for optimized network performance between log forwarder/collector to log forwarder/collector and log forwarder/collector to SIEM solution. Log forwarder/ collector shall have the capability of compressing (lossless compression) the raw logs.	
28	Solution should support Normalization, Categorization, Batching, Compression, Caching, Encryption and Filtering at collection layer:	
Log Consolidation Layer (Log management)		
29	The Solution should have a Log collection and archive architecture that supports both short-term (online) and long-term (offline) event storage. Both online and offline logs should have indexing to ensure that Log search is faster.	
30	Log Consolidation must function irrespective of availability or non-availability of SIEM layer.	
31	Log Management layer must support Log Search, Log analytics, log forensics, Dashboards, Reports.	
32	Logs stored must be tamperproof and provide integrity mechanism.	
33	The Solution should support configurable Data retention policy based on Legal requirement.	
34	The Solution should replicate Logs at DR site in real time.	
35	The Solution should have built-in system health check to troubleshoot Operational issues like:	
	1) Event Processing statistics	
	2) Compute Utilization (CPU, RAM etc.)	
	3) Resource utilization (Reports, dashboard, rules, filters etc.)	

Log Correlation Layer		
36	The solution should support correlation rules to detect complex attack patterns across disparate systems. The engine should be able to: - Detect multi-step, cross-platform attacks (e.g., lateral movement, privilege escalation, etc.). - Correlate events in real-time and over extended periods to identify trends and long-term threats.	
37	The system/solution should have the ability to correlate all the fields in a log.	
38	The solution should allow to create custom correlation rules based on unique business needs or threat models.	
39	The solution should integrate machine learning for anomaly detection and identifying novel attack patterns that might not yet be covered by predefined rules.	
40	The solution must provide intuitive mechanisms for troubleshooting such as proactive notifications, etc.	
41	All events/ incidents should be provided with a categorization and magnitude rating to help prioritize response and ensure effective Incident Handling.	
42	The solution should have provision to correlate Identity and Session information to assist in responding to incidents that are user centric.	
43	The solution must provide the ability to correlate DHCP, VPN and Active Directory events to provide session tracking of every user in order to identify the user using a particular workstation historically, during an incident investigation.	
44	The Solution should have capability to discover similar patterns of access, communication, etc. over a period of time.	
45	The Solution should have capability for correlation of Events / Flows generated from multiple sources at different locations.	
46	The event/ flows correlation on SIEM should be in real time.	
47	The Solution should be able to import the Vulnerability Information from scanning and Assessment Tools on real time basis and correlate them.	
48	The solution should have a Wizard / GUI based interface for rules (including correlation rules) creation.	
49	Solution must provide ability to monitor user transaction activity to detect anomalous transactions such as simultaneous user transactions from multiple geo-spatial locations, fraudulent activity and breaches.	
50	The Solution must provide ability to aggregate and suppress alerting with granular options and use conditional logic to determine if an alert should be generated.	
User and Entity Behaviour Analytics (UEBA)		
51	Solution should utilize machine learning algorithms and user behaviour as well as rules on logs and network flows collected to provide behavior analytics.	
52	Solution should have user behaviour analytics for minimum 18000 users and UEBA to monitor at least 2000 Entities/ Users.	

53	The solution should establish normal behavior baselines for users and entities (e.g., devices, accounts) by analyzing historical data over time to understand typical patterns, including: - Login frequency, times, and locations - Access to systems and applications - File access, modification, and downloads - Communication patterns (e.g., email, messaging) - Network traffic patterns, etc.	
54	The solution should be capable of detecting signs of insider threats, including but not limited to: - Data exfiltration (copying, sending, or transferring large volumes of data to unauthorized destinations) - Malicious behavior (e.g., unauthorized access to systems, intentional misconfigurations) - Abnormal escalation of privileges (e.g., users accessing sensitive or administrative resources beyond their typical scope)	
55	The solution should support AI/ML models to reduce false positives and improve accuracy,	
56	The ML algorithms should assign risk scores to user and entity activities, automatically ranking behaviors by likelihood of being malicious or anomalous.	
57	The solution should be able to adapt to evolving tactics, techniques, and procedures (TTPs) used by attackers, learning over time to detect new behaviors.	
58	The solution should allow creation of Watch Lists for suspicious users.	
59	The solution should provide the capability to rapidly respond to insider threats by automatically measuring and ordering the risk associated with suspicious users/ entities.	
60	The solution should add user context to logs, flow, etc. and identify outlying behaviors, generate risk scores for users, and provide security analysis with insight into high-risk and potentially compromised users/ entities.	
61	Solution should be able to drill down into log and flow data based on which the users/ entities have been identified and notified as high risk users/ entities.	
62	The solution should provide for analysts to investigate anomalies by querying historical data (e.g., access logs, event data) to see the full context of user or entity behavior over time.	
63	The solution should have a provision to search a device by Hostname, Mac Address, Username of user logged into that device, IP Address, etc.	
64	The solution should support natural language search capability without requiring to learn a custom search query language	
65	The solution should have support for virtual environment.	
Security Orchestration, Automation and Response (SOAR)		
66	The solution should provide min. 3 no. of named users.	
67	The solution must provide out- of-box playbooks based on SANS and NIST that provide incident response. The solution must dynamically augment incident playbooks in real time.	

68	The solution should be able to integrate with security devices like Firewall (Fortinet, Cisco), IDS/IPS (Fortinet, Cisco), endpoint Security and EDR solution (Checkpoint Harmony), APT solution, Offered WAAP Solution, SSE and ZTNA (Netskope), PAM, etc. from day one.	
69	Solution should be configured with the used cases with automation for response to the minimum basic threats like: 1. Blacklisted IP Communication 2. Possible Penetration Testing Activity 3. Connection to Known Malicious Actor in Published Host List 4. D-DOS Attack 5. Vulnerability scan detection 6. Phishing detection 7. Brute force attack 8. Malware /threat activity monitoring 9. Ransomware 10. Port & vulnerability Scans 11. Password cracking 12. Worm/virus outbreak 13. File access failures 14. Unauthorized server/service restarts 15. Unauthorized changes to firewall rules 16. Unauthorized ITSI access to systems	
70	The solution should provide the ability to create customize automated playbooks (workflows).	
71	The solution should have min 100 built in reusable playbooks for well-known Incident types like Phishing, Malware, IOC Hunt, etc). There should not be any restriction in creating number of playbooks i.e. out of box and customized playbooks.	
72	The solution should support for advanced logic within playbooks (e.g., if/then/else conditions, loops, decision points) to adapt to different types of incidents.	
73	The solution must be able to create incident by parsing email notification.	
74	The solution must provide UI to manually create incidents from APIs / web URLs / SIEM systems.	
75	The solution must provide auto creation of incident artifacts.	
76	The solution must be able to auto create a relationship between incidents based on similar artifacts.	
77	The solution must provide long term trend analysis of incidents.	
78	The solution must support the ability to take action related to an incident. For example, the solution should support the ability to block an intruder.	
79	The solution must correlate against any security data feeds (i.e. geographic mapping, known botnet channels, known hostile networks, etc.).	
80	The solution must provide visualization of incident correlation across IOCs and other artifacts automatically with timeline support.	
81	The solution must allow users to take remedial steps directly from within the visualization of incident correlation enabling an auto response.	
82	The solution must support creation of user and user groups and define role based access to incidents.	

83	The solution must provide central management of incidents and administrative functions from a single web based user interface.	
84	The solution must deliver multiple dashboards that can be customized to meet the specific requirements of different users of the system. The solution must provide a 'Dashboard' for incident visualization.	
85	The solution must maintain a database of incidents. The user must be able to search this database.	
Web Application and API Protection (WAAP)		
86	The successful bidder shall create an instance / tenant for BHEL in a dedicated or distributed architecture for provisioning of WAAP services on cloud. The WAAP service shall be adequately sized to meet peak data transfer rate and SLA.	
87	Solution must be cloud-based Web Application and API Protection (WAAP) which can inspect HTTP/HTTPS layer traffic and respond against application layer attacks.	
88	Should support integration with SIEM and other Monitoring and Reporting solution.	
89	The solution must address and mitigate the latest OWASP Top 10 web application & API security vulnerabilities.	
90	The solution should monitor and inspect incoming API traffic in real-time for threats such as SQL injection, Cross-Site Scripting (XSS), and other OWASP Top 10 vulnerabilities.	
91	All Internet traffic for the web facing applications that are integrated in WAAP shall be routed first to the WAAP on the cloud for scanning & only clean traffic shall be forwarded to the origin server.	
92	The solution should provide real time monitoring and analysis of incoming traffic to detect anomalous or malicious behavior.	
93	The solution should support TLS 1.2 and TLS 1.3 to ensure encrypted connection for all web traffic (port 80 and port 443)	
94	The solution should provide protection against common web application vulnerabilities, including SQL injection, XSS, CSRF (Cross-Site Request Forgery), file inclusion, etc.	
95	The solution should detect complex attack patterns, including zero-day threats, advanced persistent threats (APTs), and multi-vector attacks.	
96	The WAAP must be able to secure & protect web, mobile, and API applications on request.	
97	The solution should ensure that API traffic adheres to defined schema, and rejecting malformed or unexpected requests	
98	The solution should provide protection to APIs against unauthorized access.	
99	The solution should limit the number of requests to an API to prevent abuse and DDoS attacks.	
100	The solution should identify and block malicious bot traffic targeting APIs, such as scraping, brute-force attacks, and credential stuffing.	
101	The solution should support custom rules tailored to the specific application environment, including business logic and behavior-based rules.	

102	The offered solution shall provide WAAP service to BHEL applications primarily hosted in two domains i.e., bhel.in. bhel.com, etc. where each domain can have multiple applications. The solution should have provision to provide WAAP services to applications in 10 such domains.	
103	The WAAP solution should allow to grant access to specific users to specific domains for which they are authorized	
104	~~The solution should be able to modify and optimize TCP parameters to improve application performance~~. (This point has been deleted).	
105	The solution should Identify and mitigate malicious bot activity that targets both web applications and APIs	
106	The WAAP solution should provide protection from BOT and Man-in-The-Browser / Man-in-The-Middle Attack. Administrators must be alerted through mail/SMS in case of such attack.	
107	The solution should provide capability to configure custom rules.	
108	There should not be any restriction on the number of rules configured	
109	The solution should support different policies for different web applications and allow modification of these policies upon request.	
110	The solution should allow for exception handling like Whitelisting and Blacklisting of IPs and allow blocking of IPs based on geographic location.	
111	The solution should be able to hide sensitive server related information in the response body and response headers.	
112	The solution should have provision to detect violation of any defined file upload policy, i.e. it should prevent upload of any blacklisted file type.	
113	The solution must protect against HTTP, HTTPS and Application layer DOS and DDOS attacks	
114	The solution should protect from automated attacks on Web and mobile apps, and against bots that emulate human behavior	
115	Solution should be able to take threat intelligence feed to reveal inbound communication from malicious IP addresses, and enable threat reporting and automated blocking.	
116	The solution should provide behavioral DoS (BADoS)/ BOT feature to provide protection against DDoS / BOT attacks by analyzing traffic behavior using machine learning and data analysis.	
117	Solution must have advanced detection methods like- CAPTCHA Challenge / device fingerprinting.	
118	The solution should provide the application visibility and reporting with below metrics and entity for each application:	
	• IP address of clients and the geographical location from which they are accessing the application	
	• Total Transactions as well as Average and Max Transactions/sec	
	• Most commonly requested URLs	
	• Application Latency	
	• URL details	
Dashboard / Reports Configuration		
119	The Solution shall provide dashboards with dynamic / real-time display of events.	

120	Solution must provide the ability to visually represent event data into a dynamically updated graph. This will assist analysts in determining the expanse of attacks and pinpoint the original attacker during incident response and remediation.	
121	Solution must provide a level of confidence that reporting will continue to work and not have to be modified if a particular product, such as a Firewall or IDS product, is replaced with a newer product or bidder. The reports should continue to run and include the new technology into the report criteria automatically.	
122	Solution must provide ability to generate linked reports with a master report to drilldown into the data within the reports dynamically.	
123	Solution must provide the ability to allow analysts to drill-down from graphical dashboards to the underlying event data.	
124	The Reporting feature should be integrated in the solution. Bidder should design reports as desired by BHEL during the contract period.	
125	Customized reports should be configurable or designable via GUI.	
126	The WAAP dashboards should provide detailed reports showing attack patterns, blocked threats, traffic analytics, and system performance.	
127	UEBA dashboard should be provided that aggregates user/ entity data to show information such as the number of users being monitored, high risk users etc.	
128	The proposed solution shall support flexible fine grained Roles Based Access Control (RBAC) and Attribute Based Access Control (ABAC) for controlled user and API access. It shall restrict access, but not limited, to specific data sources, data types, time periods, specific views, reports or dashboards etc.	

Tentative list of Data Sources

Tentative List of Data Sources					
S. No.	**Data Sources**	**Qty**	**Make / Type**	**Model**	**On Prem / Cloud**
1	Internet Firewall	3	Cisco / Fortinet	FTD 2100/2000E*,2601F	On Prem
2	MPLS Firewall	10	Fortinet	2000E*,2601F	On Prem
3	Internet Routers	6	Cisco	ISR 4431	On Prem
4	MPLS Routers	100	Cisco	ISR 4431	On Prem
5	Load Balancers	2	Array/F5	5800, i2600	On Prem
6	Wireless Controller	30	AHP Aruba	Aruba9240	On Prem
7	L3 Switches	100	HP Aruba	Aruba6405, 8325, 8360, Aruba 6400, 6300,6200	On Prem
8	Internal DNS	30	Windows 2019		On Prem
9	External DNS	3	Linux		On Prem
10	File Storage System - Clusters (9 nodes each)	2	Nutanix	DELL 760-14	On Prem
11	SSE (18000 clients)	1	Netskope		Cloud
12	HCI (Hyper Converged Infrastructure) having 400 VMs - 2 clusters (12 nodes each)	400	Nutanix Acropolis (Windows / Linux on VMs)	DELL XC7625	On Prem
14	Database/Application Servers	30	Oracle DB / Oracle Weblogic / Apache Tomcat /IIS//MSSQL		On Prem
15	Email Security Devices	16	Ironport Virtual Appliance		On Prem
16	Web Application Firewall	1	Part of this RFP		Cloud
17	Endpoint, Detection & Response - 18000 clients (including 600 VDI clients)	1	Check Point	Harmony Advanced	Cloud
18	AD servers - 18000 clients	29	Windows 2016		On Prem
19	SAP Servers	20	AIX/HP-UX		On Prem
20	eOffice - 50 VMs (on HCI)	50	Oracle Linux	DELL XC7625	On Prem

Annexure – V

Price Bid Format

Part-I

S. No.	Item Description	Minimum Quantity Required	%age of Total Charges	Charges for 5 years (INR), excl. GST	Remarks
				A	
1	SOC Services (SIEM, SOAR, UEBA) as per Scope and Terms & Conditions of the RFP	**80,000 EPS**	**90.6**		Derived Charges
2	WAAP Services as per Scope and Terms & Conditions of the RFP	**500 Mbps** data transfer	**8.8**		Derived Charges
Charges for SOC (SIEM, SOAR, UEBA) & WAAP services for 5 Years (excl. GST), T1= ∑A					Derived Charges

Part-II

S. No.	Items Description	Minimum Quantity Required	%age of Total Charges	Charges for 100 Hours (INR), excl. GST	Remarks
				B	
1	Digital Forensics & Incident Response Services	100 Hours	**0.6**		Derived Charges
Charges for DFIR services for 100 hours (excl. GST), T2=B					

Total charges for SOC (SIEM, SOAR, UEBA), WAAP and DFIR services for 5 Years (excl. GST) (T=T1+T2)		Quoted Charges

Total offered price in words (T):

INR……

Applicable GST %: ……

Note:

1. The bidder shall fill only the total charges (T) for SOC (SIEM, SOAR, UEBA), WAAP and DFIR services for 5 Years (excl. GST).
2. All line item charges will be derived as per the fixed percentage.
3. The prices should be quoted in INR.
4. Evaluation of L1 will be decided on the basis of Total Charges (T), Excl. GST.
5. The total cost should be mentioned in this format. The prices shall be fixed. Use of vague terms such as “Extra as applicable’ to be avoided.
6. Taxes, other than GST as specified above shall be considered included in the price quoted.
7. Bidders to note that above format, duly filled & signed with word “quoted” in each column by authorized signatory, shall be submitted along with the techno-commercial offer.

Seal & Signature of the Company

MUTUAL NON-DISCLOSURE AGREEMENT

This Agreement is made and entered into as of the last date signed below (the "Effective Date") by and between **Bharat Heavy Electricals Ltd.(BHEL),** a Public Sector Organization having its principal place of business at BHEL House, Siri Fort, New Delhi - 110049 and _____, a _____ corporation, hereinafter called "The Bidder", whose principal mailing address is _____ .

WHEREAS in order to pursue the mutual business purpose of this particular project as specified in Bid document for setting up a cyber-security operation center, **BHEL** and the Bidder have an interest in participating in discussions wherein either Party might share information with the other that the disclosing Party considers to be proprietary and confidential to itself ("Confidential Information"); and

WHEREAS the Parties agree that Confidential Information of a Party might include, but not be limited to that Party's:

1. business plans, methods, and practices;
2. personnel, customers, and suppliers;
3. inventions, processes, methods, products, patent applications, and other proprietary rights; or
4. specifications, drawings, sketches, models, samples, tools, computer programs, technical information, or other related information;

NOW, THEREFORE, the Parties agree as follows:

1. Either Party may disclose Confidential Information to the other Party in confidence provided that the disclosing Party identifies such information as proprietary and confidential either by marking it, in the case of written materials, or, in the case of information that is disclosed orally or written materials that are not marked, by notifying the other Party of the proprietary and confidential nature of the information, such notification to be done orally, by e-mail or written correspondence, or via other means of communication as might be appropriate.
2. When informed of the proprietary and confidential nature of Confidential Information that has been disclosed by the other Party, the receiving Party ("Recipient") shall, for a period of three (3) years from the date of disclosure, refrain from disclosing such Confidential Information to any contractor or other third party without prior, written approval from the disclosing Party and shall protect such Confidential Information from inadvertent disclosure to a third party using the same care and diligence that the Recipient uses to protect its own proprietary and confidential information, but in no case less than reasonable care. The Recipient shall ensure that each of its employees, officers, directors, or agents who has access to Confidential Information disclosed under this Agreement is informed of its proprietary and confidential nature and is required to abide by the terms of this Agreement. The Recipient of Confidential Information disclosed under this Agreement shall promptly notify the disclosing Party of any disclosure of such Confidential Information in violation of this Agreement or of any subpoena or other legal process requiring production or disclosure of said Confidential Information.

3. All Confidential Information disclosed under this Agreement shall be and remain the property of the disclosing Party and nothing contained in this Agreement shall be construed as granting or conferring any rights to such Confidential Information on the other Party. The Recipient shall honor any request from the disclosing Party to promptly return or destroy all copies of Confidential Information disclosed under this Agreement and all notes related to such Confidential Information. The Parties agree that the disclosing Party will suffer irreparable injury if its Confidential Information is made public, released to a third party, or otherwise disclosed in breach of this Agreement and that the disclosing Party shall be entitled to obtain injunctive relief against a threatened breach or continuation of any such breach and, in the event of such breach, an award of actual and exemplary damages from any court of competent jurisdiction.

4. The terms of this Agreement shall not be construed to limit either Party's right to develop independently or acquire products without use of the other Party's Confidential Information. The disclosing party acknowledges that the Recipient may currently or in the future be developing information internally, or receiving information from other parties, that is similar to the Confidential Information. Nothing in this Agreement will prohibit the Recipient from developing or having developed for it products, concepts, systems or techniques that are similar to or compete with the products, concepts, systems or techniques contemplated by or embodied in the Confidential Information provided that the Recipient does not violate any of its obligations under this Agreement in connection with such development.

5. Notwithstanding the above, the Parties agree that information shall not be deemed Confidential Information and the Recipient shall have no obligation to hold in confidence such information, where such information:

    5.1. Is already known to the Recipient, having been disclosed to the Recipient by a third party without such third party having an obligation of confidentiality to the disclosing Party; or

    5.2. Is or becomes publicly known through no wrongful act of the Recipient, its employees, officers, directors, or agents; or

    5.3. Is independently developed by the Recipient without reference to any Confidential Information disclosed hereunder; or

    5.4. Is approved for release (and only to the extent so approved) by the disclosing Party; or

    5.5. Is disclosed pursuant to the lawful requirement of a court or governmental agency or where required by operation of law.

6. Nothing in this Agreement shall be construed to constitute an agency, partnership, joint venture, or other similar relationship between the Parties.

7. Neither Party will, without prior approval of the other Party, make any public announcement of or otherwise disclose the existence or the terms of this Agreement.

8. This Agreement contains the entire agreement between the Parties and in no way creates an obligation for either Party to disclose information to the other Party or to enter into any other agreement.

9. This Agreement shall remain in effect during the contract period from the Effective Date unless otherwise terminated by either Party giving notice to the other of its desire to terminate this

Agreement. The requirement to protect Confidential Information disclosed under this Agreement shall survive termination of this Agreement.

IN WITNESS WHEREOF:

FOR AND ON BEHALF OF	**FOR AND ON BEHALF OF**
_____	**BHARAT HEAVY ELECTRICALS LTD.**
Signature: _____	**Signature:** _____
Name: _____	**Name:** _____
Designation: _____	**Designation:** _____
Date: _____	**Date:** _____
Witness	**Witness**
1.	1.
2.	2.

Annexure-VII

No Deviation Certificate

This is to certify that our offer is exactly in line with your tender enquiry no. ……., dated …….. This is to expressly certify that our offer contains no deviation either Technical or Commercial in either direct or indirect form.

Signed By:

Name: _____

Designation: _____

Organization: _____

Date & Place: _____

Phone/Fax/Mobile: _____

Email: _____

Stamp & Seal: _____

Annexure-VIII

INTEGRITY PACT

Between

Bharat Heavy Electricals Ltd. (BHEL), a company registered under the Companies Act 1956 and having its registered office at "BHEL House", Siri Fort, New Delhi - 110049 (India) hereinafter referred to as "The Principal", which expression unless repugnant to the context or meaning hereof shall include its successors or assigns of the ONE PART

and

_____, (description of the party along with address), hereinafter referred to as "The Bidder/ Contractor" which expression unless repugnant to the context or meaning hereof shall include its successors or assigns of the OTHER PART

Preamble

The Principal intends to award, under laid-down organizational procedures, contract/s for _____

_____

_____ . The Principal values full compliance with all relevant laws of the land, rules and regulations, and the principles of economic use of resources, and of fairness and transparency in its relations with its Bidder(s)/ Contractor(s).

In order to achieve these goals, the Principal will appoint Independent External Monitor(s), who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

Section 1- Commitments of the Principal

1.1 The Principal commits itself to take all measures necessary to prevent corruption and to observe the following principles: -

1.1.1 No employee of the Principal, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

1.1.2 The Principal will, during the tender process treat all Bidder(s) with equity and reason. The Principal will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential/ additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.

1.1.3 The Principal will exclude from the process all known prejudiced persons.

1.1.4 If the Principal obtains information on the conduct of any of its employees which is a penal offence under the Indian Penal Code 1860 and Prevention of Corruption Act 1988 or any other statutory

penal enactment, or if there be a substantive suspicion in this regard, the Principal will inform its Vigilance Office and in addition can initiate disciplinary actions.

Section 2 - Commitments of the Bidder(s)/ Contractor(s)

2.1 The Bidder(s)/ Contractor(s) commit himself to take all measures necessary to prevent corruption. He commits himself to observe the following principles during his participation in the tender process and during the contract execution.

2.1.1 The Bidder(s)/ Contractor(s) will not, directly or through any other person or firm, offer, promise or give to the Principal or to any of the Principal's employees involved in the tender process or the execution of the contract or to any third person any material, immaterial or any other benefit which he/ she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender process or during the execution of the contract.

2.1.2 The Bidder(s)/ Contractor(s) will not enter with other Bidder(s) into any illegal or undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.

2.1.3 The Bidder(s)/ Contractor(s) will not commit any penal offence under the relevant Indian Penal Code (IPC) and Prevention of Corruption Act; further the Bidder(s)/ Contractor(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Principal as part of the business relationship, regarding plans, technical proposals and business details, including information contained or transmitted electronically.

2.1.4 Foreign Bidder(s)/ Contractor(s) shall disclose the name and address of agents and representatives in India and Indian Bidder(s)/ Contractor(s) to disclose their foreign principals or associates. The Bidder(s)/ Contractor(s) will, when presenting his bid, disclose any and all payments he has made, and is committed to or intends to make to agents, brokers or any other intermediaries in connection with the award of the contract.

2.2 The Bidder(s)/ Contractor(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

2.3 The Bidder(s)/ Contractor(s) shall not approach the Courts while representing the matters to IEMs and will await their decision in the matter.

Section 3 - Disqualification from tender process and exclusion from future contracts

If the Bidder(s)/ Contractor(s), before award or during execution has committed a transgression through a violation of Section 2 above, or acts in any other manner such as to put his reliability or credibility in question, the Principal is entitled to disqualify the Bidder(s)/ Contractor(s) from the tender process or take action as per the separate "Guidelines on Banning of Business dealings with Suppliers/ Contractors", framed by the Principal.

Section 4 - Compensation for Damages

4.1 If the Principal has disqualified the Bidder from the tender process prior to the award according to Section 3, the Principal is entitled to demand and recover the damages equivalent Earnest Money Deposit/ Bid Security.

4.2 If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to terminate the contract according to section 3, the Principal shall be entitled to demand and recover from the Contractor liquidated damages equivalent to 5% of the contract value or the amount equivalent to Security Deposit/ Performance Bank Guarantee, whichever is higher.

Section 5 - Previous Transgression

5.1 The Bidder declares that no previous transgressions occurred in the last 3 years with any other company in any country conforming to the anti-corruption approach or with any other Public Sector Enterprise in India that could justify his exclusion from the tender process.

5.2 If the Bidder makes incorrect statement on this subject, he can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason.

Section 6 - Equal treatment of all Bidders/ Contractors / Sub-contractors

6.1 The Principal will enter into agreements with identical conditions as this one with all Bidders and Contractors.

6.2 In case of sub-contracting, the Principal contractor shall be responsible for the adoption of IP by his sub-contractors and shall continue to remain responsible for any default by his sub-contractors.

6.3 The Principal will disqualify from the tender process all bidders who do not sign this pact or violate its provisions.

Section 7 - Criminal Charges against violating Bidders/ Contractors /Subcontractors

If the Principal obtains knowledge of conduct of a Bidder, Contractor or Subcontractor, or of an employee or a representative or an associate of a Bidder, Contractor or Subcontractor which constitutes corruption, or if the Principal has substantive suspicion in this regard, the Principal will inform the Vigilance Office.

Section 8 -Independent External Monitor(s)

8.1 The Principal appoints competent and credible Independent External Monitor for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this agreement.

8.2 The Monitor is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. He reports to the CMD, BHEL.

8.3 The Bidder(s)/ Contractor(s) accepts that the Monitor has the right to access without restriction to all contract documentation of the Principal including that provided by the Bidder(s)/ Contractor(s). The Bidder(s)/ Contractor(s) will grant the monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his contract documentation. The same is applicable to Sub-contractor(s). The Monitor is under contractual obligation to treat the information and documents of

the Bidder(s)/ Contractor(s) / Sub-contractor(s) with confidentiality in line with Non- disclosure agreement.

8.4 The Principal will provide to the Monitor sufficient information about all meetings among the parties related to the contract provided such meetings could have an impact on the contractual relations between the Principal and the Contractor. The parties offer to the Monitor the option to participate in such meetings.

8.5 The role of IEMs is advisory, would not be legally binding and it is restricted to resolving issues raised by an intending bidder regarding any aspect of the tender which allegedly restricts competition or bias towards some bidders. At the same time, it must be understood that IEMs are not consultants to the Management. Their role is independent in nature and the advice once tendered would not be subject to review at the request of the organization.

8.6 For ensuring the desired transparency and objectivity in dealing with the complaints arising out of any tendering process, the matter should be examined by the full panel of IEMs jointly as far as possible, who would look into the records, conduct an investigation, and submit their joint recommendations to the Management.

8.7 The IEMs would examine all complaints received by them and give their recommendations/ views to CMD, BHEL, at the earliest. They may also send their report directly to the CVO and the Commission, in case of suspicion of serious irregularities requiring legal/ administrative action. IEMs will tender their advice on the complaints within 10 days as far as possible.

8.8 The CMD, BHEL shall decide the compensation to be paid to the Monitor and its terms and conditions.

8.9 IEM should examine the process integrity, they are not expected to concern themselves with fixing of responsibility of officers. Complaints alleging mala fide on the part of any officer of the organization should be looked into by the CVO of the concerned organization.

8.10 If the Monitor has reported to the CMD, BHEL, a substantiated suspicion of an offence under relevant Indian Penal Code/ Prevention of Corruption Act, and the CMD, BHEL has not, within reasonable time, taken visible action to proceed against such offence or reported it to the Vigilance Office, the Monitor may also transmit this information directly to the Central Vigilance Commissioner, Government of India.

8.11 The number of Independent External Monitor(s) shall be decided by the CMD, BHEL.

8.12 The word `Monitor' would include both singular and plural.

Section 9 - Pact Duration

9.1 This Pact shall be operative from the date IP is signed by both the parties till the final completion of contract for successful bidder and for all other bidders 6 months after the contract has been awarded. Issues like warranty / guarantee etc. should be outside the purview of IEMs.

9.2 If any claim is made/ lodged during currency of IP, the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged/ determined by the CMD, BHEL.

Section 10 - Other Provisions

10.1 This agreement is subject to Indian Laws and jurisdiction shall be registered office of the Principal, i.e. New Delhi.

10.2 Changes and supplements as well as termination notices need to be made in writing. Side agreements have not been made.

10.3 If the Contractor is a partnership or a consortium, this agreement must be signed by all partners consortium members.

10.4 Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

10.5 Only those bidders / contractors who have entered into this agreement with the Principal would be competent to participate in the bidding. In other words, entering into this agreement would be a preliminary qualification.

For & On behalf of the Principal

(Office Seal)

Place----------

Date----------

Witness _____

(Name & Address) _____

_____

For & On behalf of the Bidder/ Contractor

(Office Seal)

……

……

Witness: _____

(Name & Address) _____

_____

ANNEXURE- IX

UNDERTAKING

(To be typed and submitted in the Letter Head of the Company/Firm of Bidder)

To,

BHEL, CDT Noida

Dear Sir/Madam,

Sub: DECLARATION REGARDING INSOLVENCY/ LIQUIDATION/ BANKRUPTCY PROCEEDINGS

Ref: GeM Bid Specification No:

I/We,

_____

____ declare that, I/We am/are not admitted under insolvency resolution process or liquidation under Insolvency and Bankruptcy Code, 2016, as amended from time to time or under any other law as on date, by NCLT or any adjudicating authority/authorities.

Sign. of the AUTHORISED SIGNATORY
(With Name, Designation and Company seal)

Place:

Date:

ANNEXURE – X

Local Content Certificate- Self-Declaration

Enquiry No.	
Enquiry Date	

In line with Government public procurement order Number P- 45021/2/2017-B.E-II dated 15.06.2017, and further modified order dt. 28.05.2018 and 04.06.2020.

I / We hereby declare that I / We are a "Local Supplier" means a supplier or service provider, whose goods, services or works offered for procurement, meets the minimum local content (…….%) defined in the above government notification against above mentioned enquiry Number.

Details of location at which local value addition will be made is as follows:

Door No.	
Street / Address 1	
Street / Address 2	
District	
State	
Country	
PIN Code	

We also understand that the false declarations will be considered as breach of Integrity and liable for action.

For Company Name:

Seal:

Signature:

Date:

Place:

(All the yellow color fields to be filled only by authorized signatory of the company)

Note: In cases of procurement for a value in excess of Rs. 10 crores, the 'Class-I local supplier'/ 'Class-II local supplier' shall be required to provide a certificate from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content.

ANNEXURE XI

Model Certificate

(DECLARATION REGARDING COMPLIANCE TO RESTRICTIONS UNDER RULE 144 (xi) OF GFR 2017)

Bid No. _____ "I have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India; I certify that this bidder is not from such a country or, if from such a country, has been registered with the Competent Authority. I hereby certify that this bidder fulfils all requirements in this regard and is eligible to be considered. [Where applicable, evidence of valid registration by the Competent Authority shall be attached.]"

Signature and stamp of the authorized signatory

Note: Bidders to note that in case above certification given by a bidder, whose bid is accepted, is found to be false, then this would be a ground for immediate termination and for taking further action in accordance with law and as per BHEL guidelines.

ANNEXURE – XII

PROFORMA OF BANK GUARANTEE FOR EARNEST MONEY

(On non-Judicial paper of appropriate value)

Bank Guarantee No…….
Date……..

To
(Employer's Name and Address)
……..
Dear Sirs,
In accordance with the terms and conditions of Invitation for Bids/Notice Inviting Tender No……1(Tender Conditions), M/s. ……. having its registered office at ……2 (hereinafter referred to as the 'Tenderer'), is submitting its bid for the work of**……**3 invited by ……4.(name of the Employer) through its Unit at ……(
The Tender Conditions provide that the Tenderer shall pay a sum of Rs ……. as Earnest Money Deposit in the form therein mentioned. The form of payment of Earnest Money Deposit includes Bank Guarantee executed by a Scheduled Bank.
In lieu of the stipulations contained in the aforesaid Tender Conditions that an irrevocable and unconditional Bank Guarantee against Earnest Money Deposit for an amount of .....5 ..... is required to be submitted by the Tenderer as a condition precedent for participation in the said Tender and the Tenderer having approached us for giving the said Guarantee,
we, the .....[Name & address of the Bank]
..... having our Registered Office at
……..(hereinafter referred to as the Bank) being the Guarantor under this
Guarantee, hereby irrevocably and unconditionally undertake to forthwith and immediately pay to the Employer without any demur, merely on your first demand any sum or sums of Rs.
..... 5 (in words Rupees.....) without any reservation, protest, and recourse and without the beneficiary needing to prove or demonstrate reasons for its such demand.

Any such demand made on the Bank shall be conclusive as regards the amount due and payable by the Bank under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding Rs. _____ _____.

We undertake to pay to the Employer any money so demanded notwithstanding any dispute or disputes raised by the Vendor/Contractor/Vendors in any suit or proceeding pending before any Court or Tribunal, Arbitrator or any other authority, our liability under this present being absolute and unequivocal.

The payment so made by us under this Guarantee shall be a valid discharge of our liability for payment hereunder and the Tenderer shall have no claim against us for making such payment.

We …….. Bank further agree that the Employer shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said Tender or to extend the time of submission of from time to time or to postpone for any time or from time to time any of the powers exercisable by the Employer against the said Tenderer and we shall not be relieved from our liability by reason of any such variation, or extension being granted to the said Tenderer or for any forbearance, act or omission on the part of the Employer or any indulgence by the Employer to the said Tenderer or by any such matter or thing whatsoever which under the law relating to sureties would but for this provision have effect of so relieving us.

The Bank also agrees that the Employer at its option shall be entitled to enforce this Guarantee against the Bank as a principal debtor, in the first instance without proceeding against the Tenderer and notwithstanding any security or other guarantee that the Employer may have in relation to the Tenderer's liabilities.

This Guarantee shall be irrevocable and shall remain in force upto and including……..6 and shall be extended from time to time for such period as may be desired by the Employer.

This Guarantee shall not be determined or affected by liquidation or winding up, dissolution or change of constitution or insolvency of the Tenderer but shall in all respects and for all purposes be binding and operative until payment of all money payable to the Employer in terms hereof. However, unless a demand or claim under this Guarantee is made on us in writing on or before the ……. 7 we shall be discharged from all liabilities under this Guarantee.

This Bank Guarantee shall be governed, construed and interpreted in accordance with the laws of India.

Courts at …… shall alone have exclusive jurisdiction over any matter arising out of or in connection with this Bank Guarantee

We, …… Bank lastly undertake not to revoke this guarantee during its currency except with the previous consent of the Employer in writing.

Notwithstanding anything to the contrary contained hereinabove:

a. The liability of the Bank under this Guarantee shall not exceed……5…….

b. This Guarantee shall be valid up to ……6

c. Unless the Bank is served a written claim or demand on or before _____7 all rights under this guarantee shall be forfeited and the Bank shall be relieved and discharged from all liabilities under this guarantee irrespective of whether or not the original bank guarantee is returned to the Bank

We, _____ Bank, have power to issue this Guarantee under law and the undersigned as a duly authorized person has full powers to sign this Guarantee on behalf of the Bank.
For and on behalf of
(Name of the Bank)
Date…….
Place of Issue…….
1 Details of the Invitation to Bid/Notice Inviting Tender
2 Name and Address of the Tenderer
3 Details of the Work
4 Name of the Employer
5 BG Amount in words and Figures
6 Validity Date
7 Date of Expiry of Claim Period
Notes:
1. Units are advised that expiry of claim period may be kept 3-6 months after validity date. It may be ensured that the same is in line with the agreement/ contract entered with the Vendor.

2. The BG should be on Non-Judicial Stamp paper/e-stamp paper of appropriate value as per Stamp Act prevailing in the State(s) where the BG is submitted or is to be acted upon or the rate prevailing in the State where the BG was executed, whichever is higher. The Stamp Paper/e-stamp paper shall be purchased in the name of Contractor/sub-contractor /vendor/ Bank issuing the guarantee.

3. In line with the GCC, SCC or contractual terms, Unit may carry out minor modifications in the Standard BG Formats. If required, such modifications may be carried out after taking up appropriately with the Unit/Region's Law Deptt.

4. **In Case of Bank Guarantees submitted by Foreign Vendors-**

a. From Nationalized/Public Sector / Private Sector/ Foreign Banks (BG issued by Branches in India) can be accepted subject to the condition that the Bank Guarantee should be enforceable in the town/city or at nearest branch where the Unit is located i.e., Demand can be presented at the Branch located in the town/city or at nearest branch where the Unit is located.

b. From Foreign Banks (wherein Foreign Vendors intend to provide BG from local branch of the Vendor country's Bank)

b.1 In such cases, in the Tender Enquiry/ Contract itself, it may be clearly specified that Bank Guarantee issued by **any of the Consortium Banks only** will be accepted by BHEL. As such, Foreign Vendor needs to make necessary arrangements for issuance of Counter- Guarantee by Foreign Bank in favour of the Indian Bank's (BHEL's Consortium Bank) branch in India. It is advisable that all charges for issuance of Bank Guarantee/ counter- Guarantee should be borne by the Foreign Vendor. The tender stipulation should clearly specify these requirements.

b.2 In case, Foreign Vendors intend to provide BG from Overseas Branch of our Consortium Bank (e.g. if a BG is to be issued by SBI Frankfurt), the same is acceptable. However, the procedure at **sl.no. b.1** will required to be followed.

b.3 The BG issued may preferably be subject to Uniform Rules for Demand Guarantees (URDG) 758 (as amended from time to time). The BG Format provided to them should clearly specify the same.

ANNEXURE – XIII

BANK GUARANTEE FOR PERFORMANCE SECURITY

(On non-Judicial paper of appropriate value)

Bank Guarantee No:
Date:
To

NAME
& ADDRESSES OF THE BENEFICIARY

Dear Sirs,

In consideration of Bharat Heavy Electricals Limited (hereinafter referred to as the 'Employer' which expression shall unless repugnant to the context or meaning thereof, include its successors and permitted assigns) incorporated under the Companies Act, 1956 and having its registered office at_____1 through its Unit at……..(name of the Unit) having awarded to (Name of the Vendor / Contractor / Supplier) with its registered office at_____2 hereinafter referred to as the ' Vendor / Contractor / Supplier ', which expression shall unless repugnant to the context or meaning thereof, include its successors and permitted assigns), a contract Ref No……dated ……3 valued at Rs……4 (Rupees ----------) / FC……(in words……..) for ……5 (hereinafter called the 'Contract') and the Vendor / Contractor / Supplier having agreed to provide a Contract Performance Bank Guarantee, equivalent to ……% (…. Percent) of the said value of the Contract to the Employer for the faithful performance of the Contract,

We, ……, (hereinafter referred to as the Bank), having registered/Head office at ……. and inter alia a branch at …… being the Guarantor under this Guarantee, hereby, irrevocably and unconditionally undertake to forthwith and immediately pay to the Employer any sum or sums upto a maximum amount of Rs ---------- 6 (Rupees ----------) without any demur, immediately on first demand from the Employer and without any reservation, protest, and recourse and without the Employer needing to prove or demonstrate reasons for its such demand.

Any such demand made on the Bank shall be conclusive as regards the amount due and payable by the Bank under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding Rs. _____.

We undertake to pay to the Employer any money so demanded notwithstanding any dispute or disputes raised by the Vendor / Contractor / Supplier in any suit or proceeding pending before any Court or Tribunal, Arbitrator or any other authority, our liability under this present being absolute and unequivocal.

The payment so made by us under this Guarantee shall be a valid discharge of our liability for payment thereunder and the Vendor / Contractor / Supplier shall have no claim against us for making such payment.

We the ……bank further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said Contract/ satisfactory completion of the performance guarantee period as per the terms of the Contract and that it shall continue to be enforceable till all the dues of the Employer under or by virtue of the said Contract have been fully paid and its claims satisfied or discharged.

We ……..BANK further agree with the Employer that the Employer shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said Contract or to extend time of performance by the said Vendor / Contractor / Supplier from time to time or to postpone for any time or from time to time any of the powers exercisable by the Employer against the said Vendor / Contractor / Supplier and to forbear or enforce any of the terms and conditions relating to the said Contract and we shall not be relieved from our liability by reason of any such variation, or extension being granted to the said Vendor / Contractor / Supplier or for any forbearance, act or omission on the part of the Employer or any indulgence by the Employer to the said Vendor / Contractor / Supplier or by any such matter or thing whatsoever which under the law relating to sureties would but for this provision have effect of so relieving us.

The Bank also agrees that the Employer at its option shall be entitled to enforce this Guarantee against the Bank as a principal debtor, in the first instance without proceeding against the Vendor / Contractor /

Supplier and notwithstanding any security or other guarantee that the Employer may have in relation to the Vendor /Contractor / Supplier 's liabilities.
This Guarantee shall remain in force upto and including…….. 7 and shall be extended from time to time for such period as may be desired by Employer.
This Guarantee shall not be determined or affected by liquidation or winding up, dissolution or change of constitution or insolvency of the Vendor / Contractor / Supplier but shall in all respects and for all purposes be binding and operative until payment of all money payable to the Employer in terms thereof.
Unless a demand or claim under this guarantee is made on us in writing on or before the ……8 we shall be discharged from all liabilities under this guarantee thereafter.
This Bank Guarantee shall be governed, construed and interpreted in accordance with the laws of India.
Courts at …… shall alone have exclusive jurisdiction over any matter arising out of or in connection with this Bank Guarantee
We, …… BANK lastly undertake not to revoke this guarantee during its currency except with the previous consent of the Employer in writing. Notwithstanding anything to the contrary contained hereinabove:
a. The liability of the Bank under this Guarantee shall not exceed…… 6
b. This Guarantee shall be valid up to ……7
c. Unless the Bank is served a written claim or demand on or before _____8 all rights under this guarantee shall be forfeited and the Bank shall be relieved and discharged from all liabilities under this guarantee irrespective of whether or not the original bank guarantee is returned to the Bank.

We, _____ Bank, have power to issue this Guarantee under law and the undersigned as a duly authorized person has full powers to sign this Guarantee on behalf of the Bank.
For and on behalf of
(Name of the Bank)
Dated…….
Place of Issue…….
1 NAME AND ADDRESS OF EMPLOYER i.e., Bharat Heavy Electricals Limited
2 NAME AND ADDRESS OF THE VENDOR /CONTRACTOR / SUPPLIER.
3 DETAILS ABOUT THE NOTICE OF AWARD/CONTRACT REFERENCE
4 CONTRACT VALUE
5 PROJECT/SUPPLY DETAILS
6 BG AMOUNT IN FIGURES AND WORDS
7 VALIDITY DATE
8 DATE OF EXPIRY OF CLAIM PERIOD

Note:
1. Units are advised that expiry of claim period may be kept 3-6 months after validity date. It may be ensured that the same is in line with the agreement/ contract entered with the Vendor.

2. The BG should be on Non-Judicial Stamp paper/e-stamp paper of appropriate value as per Stamp Act prevailing in the State(s) where the BG is submitted or is to be acted upon or the rate prevailing in the State where the BG was executed, whichever is higher. The Stamp Paper/e-stamp paper shall be purchased in the name of Vendor/Contractor/Supplier /Bank issuing the guarantee.

3. In line with the GCC, SCC or contractual terms, Unit may carry out minor modifications in the Standard BG Formats. If required, such modifications may be carried out after taking up appropriately with the Unit/Region's Law Deptt.

4. **In Case of Bank Guarantees submitted by Foreign Vendors-**

a. From Nationalized/Public Sector / Private Sector/ Foreign Banks (BG issued by Branches in India) can be accepted subject to the condition that the Bank Guarantee should be enforceable in the town/city or at nearest branch where the Unit is located i.e.
Demand can be presented at the Branch located in the town/city or at nearest branch where the Unit is located.

b. From Foreign Banks (wherein Foreign Vendors intend to provide BG from local branch of the Vendor country's Bank)

b.1 In such cases, in the Tender Enquiry/ Contract itself, it may be clearly specified that Bank Guarantee issued by **any of the Consortium Banks only** will be accepted by BHEL. As such, Foreign Vendor needs to make necessary arrangements for issuance of Counter- Guarantee by Foreign Bank in favour of the Indian Bank's (BHEL's Consortium Bank) branch in India. It is advisable that all charges for issuance of Bank Guarantee/ counter- Guarantee should be borne by the Foreign Vendor. The tender stipulation should clearly specify these requirements.
b.2 In case, Foreign Vendors intend to provide BG from Overseas Branch of our Consortium Bank (e.g. if a BG is to be issued by SBI Frankfurt), the same is acceptable. However, the procedure at **sl.no. b.1** will required to be followed.
b.3 The BG issued may preferably be subject to Uniform Rules for Demand Guarantees (URDG) 758 (as amended from time to time). The BG Format provided to them should clearly specify the same.

ANNEXURE XIV

List of Consortium Bank

S.NI.	**NAME OF THE BANK**
1	State Bank of India
2	Canara Bank
3	IDBI Bank Limited
4	ICICI Bank Limited
5	HDFC Bank Limited
6	AXIS bank
7	IndusInd Bank Limited
8	Bank of Baroda
9	Exim Bank
10	Indian Bank
11	Punjab National Bank
12	Union Bank Of India
13	Yes Bank Limited
14	RBL Bank Ltd.
15	Standard Chartered Bank
16	Indian Overseas Bank
17	Kotak Mahindra Bank Limited
18	Federal Bank Limited
19	Hongkong and Shanghai Banking Corporation Ltd

ANNEXURE XV

Pre-Bid Query Format

Date:__/__/____

Ref Bid Number: _____

Company Name:

_____

Representative Details:

Name: _____

Email IDs:

_____

Phone Nos: _____

Signatures: _____

Note: Only written queries shall be entertained in the Pre-Bid Meeting. Visiting Card (if available) may also be enclosed.

Queries:

NIT Clause No.	Query Details	Suggestive change in NIT Clause

Signed by authorized signatory only:

ANNEXURE-XVI

NOTE: - Bidders are required to fill in the following details in their Letterhead and no column should be left blank

A	**Name and Address of the Supplier**			
B	**GSTN No. the Supplier (Place of Execution of Contract / Purchase Order)**			
C	**Details of Contact person for this tender**	**Name: Mr./ Ms.** **this Tender Designation:** **Telephone No:** **Mobile No:** **Email ID:**		
D	**EMD DETAILS**			
E	**DESCRIPTION**		**APPLICABILITY (BY BHEL)**	**ENCLOSED BY BIDDER**
i	Whether Pre - Qualification Criteria is understood and provided proper supporting documents		Applicable	YES / NO
ii	Whether all pages of the tender documents including annexures, appendices etc are read and understood same dully stamped & signed		Applicable	YES / NO
iii	Audited Balance Sheet and profit & Loss Account for the last three years		Applicable	YES / NO
iv	Copy of PAN Card & GST registration		Applicable	YES / NO
v	Submission of MSE certificate as specified in Tender		Applicable	YES / NO
vi	Submission of Price bid format (Unpriced copy with the word "quoted" in each cells)		Applicable	YES / NO
vii	Submission of Certificate of No Deviation as per Annexure		Applicable	YES / NO
viii	Declaration regarding Insolvency/ Liquidation/ Bankruptcy Proceedings as per Annexure		Applicable	YES / NO
ix	Submission of Non-Disclosure Certificate as per Annexure		Applicable	YES / NO
x	Submission of Integrity Pact as specified in Tender as per Annexure		Applicable	YES / NO
xi	Declaration reg. minimum local content in line with revised public procurement as per Annexure		Applicable	YES / NO
xii	Declaration regarding model certificate		Applicable	YES / NO
xiii	Proforma of Bank Guarantee for Earnest Money as per Annexure		Applicable	YES / NO

xiv	Proforma of Bank Guarantee for Security Money as per Annexure	Applicable	YES / NO

NOTE: Strike off 'YES' or 'NO', as applicable. Tender not accompanied by the prescribed **above applicable documents** are liable to be summarily rejected.

DATE:

Sign. of the AUTHORISED SIGNATORY
(With Name, Designation and Company seal)

AGREEMENT BETWEEN BIDDER AND THEIR PARENT COMPANY (TO BE MADE ON STAMP PAPER OF REQUISITE VALUE AND NOTORISED)

This agreement made this _____ day of month _____ year by and between M/s. (Bidder's particular) _____ hereinafter referred to as Bidder of the first part and M/s. (Parent Company's particulars) hereinafter referred to as "Parent Company " on the other part, whereas Bharat Heavy Electricals Ltd. (hereinafter referred to as “BHEL”) has invited offers for the said tender for “Cyber Security Operations Centre (Cyber SOC) Services and Web Application and API Protection (WAAP) Services “and whereas M/s. (Bidder) intends to bid against the said tender and desires to use credentials of M/s. (Parent Company) to meet the pre-qualifying requirement (**PQR**) of tender no. and whereas Parent Company represents that they have gone through and understood the requirements of subject tender and are capable and committed to provide the services as required by the bidder for successful execution of the contract, if awarded to the Bidder.

Now, it is hereby agreed to by and between the parties as follows:

1. M/s. (Bidder) will submit an offer to BHEL for the full scope of work as envisaged in the tender document as a Bidder and liaise with BHEL directly for any clarifications etc. in this context. The Bidder will use the credentials of the Parent Company referred in the offer.
2. If the bid of the Bidder is accepted by BHEL, M/s. (parent Company) as a holding company undertakes to provide all financial, technical support and expertise, expert manpower and procurement assistance and project management to support the Bidder to discharge its obligations as per the scope of work of the tender / contract, including taking over performance the contact, in case of default of Bidder.
3. This agreement will remain valid till validity of Bidder's offer to BHEL including extension if any and till satisfactory performance of the contract in the event the contract is awarded by BHEL to the Bidder.
4. It is further agreed that for the performance of work during contract period Bidder and Parent company shall be jointly and severally responsible to BHEL for satisfactory execution of the contract.
5. However, the Bidder shall have the overall responsibility of satisfactory execution of the contract awarded by BHEL.

In witness whereof, the parties hereto have executed this agreement on the date mentioned above.

For and on behalf of **For and on behalf of**

(**Bidder**) (**Parent Company**)

Witness:

Annexure - D

	Existing		Modification	
S. No.	**Qualification Criteria**	**Documents to be Provided**	**Qualification Criteria**	**Documents to be Provided**
For bidder				
1	The bidder should have a registered office in India having a valid PAN No. and GST Registration No.	a) Copy of Certificate of registration. b) Copy of PAN Card c) Copy of GST Registration	No Change	No Change
2	The bidder shall be OEM / OEM's Subsidiary / OEM's authorized partner or system integrator.	Documentary evidence for OEM / OEM's Subsidiary / OEM's authorized partner or system integrator. (In case bidder is not OEM, an authorization letter from OEM to be submitted by the bidder specifically authorizing the bidder to quote in this tender)	No Change	No Change
3	The Bidder should be ISO 27001:2013 / ISO 27001:2022 certified.	Appropriate documentary evidence to be provided. Copy of valid ISO 27001:2013 / ISO 2700:2022 certificate.	No Change	No Change
4	The bidder should have executed similar work in the **last 7 years,** preceding the bid submission date as follows: One Order of similar work for minimum 60000 EPS (events per second). OR Two orders of similar work for minimum 50000 EPS each. OR Three orders of similar work for minimum 40000 EPS each. Note: (a) Executed here means the bidder should have implemented and commissioned the solution and should have maintained the same for at least one year from the date of commissioning in the last 7 years, preceding the bid submission date . (b) Similar work here means the bidder should have implemented and maintained/maintaining a SIEM solution in combination with either SOAR or UEBA or both in the last 7 years, preceding the bid submission date.	a) copy of PO / WO / LOI b) copy of commissioning certificate c) Satisfactory services certificate / confirmation from customer d) Bidder shall provide contact details (name, email id, phone no.) of customers for verification.	No Change	No Change

S. No.	Qualification Criteria	Documents to be Provided	Qualification Criteria	Documents to be Provided
5	The bidder should have executed SIEM solution for at least **5** customers in India in the **last 7 years**, preceding the bid submission date. with a cumulative 120000 EPS Note: (a) Executed here means the bidder should have implemented and commissioned the solution and should have maintained the same for at least one year from the date of commissioning in the last 7 years, preceding the bid submission date.	a) copy of PO / WO / LOI b) copy of commissioning certificate c) Satisfactory services certificate / confirmation from customer d) Bidder shall provide contact details (name, email id, phone no.) of customers for verification.	No Change	No Change
6	The bidder should have had a positive networth in the preceding three financial years, i.e., 2023-24, 2022-23, 2021-22.	Copy of Audited Balance Sheets and Profit and Loss Account for the year 2021-22, 2022-23 and 2023-24 or Networth certificate from a CA with UDIN no.	No Change	No Change
7	The bidder should have had an average turn-over of Rs 50 crores in the preceding 3 financial years, i.e., 2023-24, 2022-23, 2021-22	Copy of Audited balance sheets and Profit and Loss Account for the year 2021-22, 2022-23 and 2023-24 or Turnover certificate from a CA with UDIN number	No Change	No Change
8	The bidder should not have been banned in the last 3 years, preceding the bid submission date, in any BHEL Units / Divisions, CPSE or Central Govt entities for any unlawful or immoral business dealings.	Self-attested certificate from the bidder on letter head.	No Change	No Change
9	The bidder of the proposed solution should have minimum following certified professionals on its own rolls.	Copy of certificates. All certificates should be current and valid. Expired certificates will not be considered. Signed Letter on company's letterhead from Company HR Head to be submitted for being on company's rolls.	The bidder of the proposed solution should have minimum following certified professionals on its own rolls.	No Change
	Certified Information Systems Security Professional (CISSP) / Certified Information Security Manager (CISM) / GIAC Security Leadership Certification (GSLC): **5 nos. out of which minimum 2 should be CISSP**		Certified Information Systems Security Professional (CISSP) / Certified Information Security Manager (CISM) / GIAC Security Leadership Certification (GSLC): ~~5 nos. out of which minimum 2 should be CISSP~~ 2 nos.	
	Certified Ethical Hacker (CEH from EC-Council): **5 nos.**		Certified Ethical Hacker (CEH from EC-Council): ~~5 nos.~~ 2 nos.	
	Certified Digital Forensics Analysts / Professionals (SANS / GIAC or EC-Council certified): **5 nos.**		Deleted	
For OEMs and Proposed Solutions				

S. No.	Qualification Criteria	Documents to be Provided	Qualification Criteria	Documents to be Provided
1	The OEMs of the SIEM, SOAR and UEBA solutions should have a registered office in India.	Copy of certificate of registration.	No change	No change
2	The OEMs of the SIEM and WAAP solutions should have been present in India for at least last 5 years before the date of submission of the bid.	Certificate of incorporation /Audited Balance Sheet /Merger, Amalgamation or Demerger agreement alongwith relevant order /Purchase Agreement, etc.	No change	No change
3	The OEM of the WAAP solution should have its own datacentre in India (MeitY empanelled) or should have a pre-tie-up with an Indian Data Center Service Provider (MeitY empanelled) from which the solution offered to BHEL shall be rendered.	Valid MeitY empanelment certificate of the OEM data centre in India / service agreement or hosting agreement between the OEM and the MeitY empanelled Data Centre (where the proposed WAAP solution would be hosted), etc..	No change	No change
4	The proposed SIEM and WAAP solutions must have been deployed in India for at least **10 customers (each solution, i.e., SIEM, WAAP)** in the **last 7 years,** preceding the bid submission date and it should be currently operational for at **least 5 customers** (each solution).	a) copy of PO / WO / LOI b) copy of commissioning certificate c) Satisfactory services certificate / confirmation from customer d) Bidder shall provide contact details (name, email id, phone no.) of customers for verification.	No change	No change
5	The proposed SIEM solution should have been deployed in India for a minimum cumulative **240000 EPS in the last 7 years**, preceding the bid submission date.	a) copy of PO / WO / LOI b) copy of commissioning certificate c) Satisfactory services certificate / confirmation from customer d) Bidder shall provide contact details (name, email id, phone no.) of customers for verification.	No change	No change
6	The proposed SIEM solution should have been deployed at a single customer in India for a sustained minimum **60000 EPS** (events per second) in the **last 7 years**, preceding the bid submission date. The solution should have been commissioned and successfully running for a minimum one year in the **last 7 years**, preceding the bid submission date.	a) copy of PO / WO / LOI b) copy of commissioning certificate c) Satisfactory services certificate / confirmation from customer d) Bidder shall provide contact details (name, email id, phone no.) of customers for verification.	No change	No change
7	The proposed SIEM (with SOAR / UEBA or both) solutions should have been deployed at a central PSU or a PSB (Public Sector Bank) or Govt agency in India for a sustained minimum **40000 EPS** (events per second) at a single customer, in the last 7 years, preceding the bid submission date.	a) copy of PO / WO / LOI b) copy of commissioning certificate c) Satisfactory services certificate / confirmation from customer d) Bidder shall provide contact details (name, email id, phone no.) of customers for verification.	Deleted	Deleted

S. No.	Qualification Criteria	Documents to be Provided	Qualification Criteria	Documents to be Provided
8	The proposed WAAP solution should have been deployed in India for a customer for a minimum **100Mbps** data transfer rate or at least **50 applications** / **websites** in the **last 7 years**, preceding the bid submission date.	a) copy of PO / WO / LOI b) copy of commissioning certificate c) Satisfactory services certificate / confirmation from customer d) Bidder shall provide contact details (name, email id, phone no.) of customers for verification.	No change	No change
9	The OEMs of the SIEM, SOAR, UEBA and WAAP solutions should have their own customer support centre in India.	a) Address of the Customer Support Centre b) Copy of lease agreement / rent agreement / electricity bill / Telephone bill, etc.	No change	No change

Notes:

1)	All criteria of PQR (for bidder and for OEM's of proposed solution) have to be met for the bid to be qualified for next stage of evaluation. The bidder shall submit necessary documentary proof in support of the PQR criteria. All documentary proof submitted by the bidder should be verifiable by BHEL. BHEL's decision on PQR criteria, interpretation and acceptance or rejection of any documentary evidence shall be final and binding on all the bidders.	No change
2)	Bidder shall not be under Bankruptcy proceedings (IBC) by NCLT or under liquidation / BIFR, which will render it ineligible for participation in this tender. The bidder shall submit an undertaking towards this effect.	No change
3)	For evaluation of the PQR, the credentials of the bidder, and not the group company shall be considered.	For the purpose of evaluating the Pre Qualification Requirements (PQR), only the credentials of the Bidder will be considered. However, if the Bidder is a subsidiary company, the credentials of its Parent Company will be considered, provided that the Bidder submits satisfactory documentary evidence acceptable to BHEL. Acceptable documentary evidence may include any of the following, but is not limited to: i. Board Resolution ii. Slump Sale Agreement iii. Demerger Agreement Credentials of any other subsidiaries or associates of the Parent Company will not be taken into account. Additionally, an agreement between the Bidder and its Parent Company must be executed in the format provided in **Annexure-XVII** and submitted as part of the bid.
4)	The bidder's representative/individual signing the bid documents on behalf of the bidder should have an authorization letter / power of Attorney, etc. from the bidder specifically authorizing the representative/individual to sign in this tender.	No change