NOTICE INVITING EXPRESSION OF INTEREST

EOI NO. RCIL/SR/ERS/2025-26/EOI/03 DTD. 27-05-2025

Expression of Interest (EOI) For

"Setting up Security Operations Centre (SOC) as part of KSEBL Data Centre under RDSS Scheme"

रेलटेल
RAILTEL
A Navratna CPSE
Govt of India

Issued by:

RailTel Corporation of India Ltd

(A Nava-Ratna PSU under Ministry of Railways)

Kerala Territory Southern Region,

1st Floor Eastern Entry Tower Ernakulam Junction

Railway Station Ernakulam, 682016

Disclaimer

RailTel Corporation of India Ltd. (herein after called the RailTel) has prepared this Expression of Interest (EOI) document solely to assist prospective bidders in making their decision of whether bid or not to bid.

While the RailTel has taken due care in the preparation of information contained herein and believes it to be accurate, neither the RailTel or any of its Authorities or Agencies nor any of their respective officers, employees, agents or advisors give any warranty or make any representations, express or implied as to the completeness or accuracy of the information contained in this document or any information which may be provided in association with it. This information is not intended to be exhaustive and interested parties are required to make their own inquiries and do site visits that it may require in order to submit the EOI. The information is provided on the basis that it is non– binding on RailTel, any of its authorities or agencies or any of their respective officers, employees, agents or advisors. The RailTel reserves the right not to proceed with the bidding/EOI process at any stage without assigning any reasons thereof, or to alter the timetable reflected in this document or to change the process or procedure to be applied. It also reserves the right to decline to discuss the EOI further with any party submitting an EOI. No reimbursement of cost of any type will be paid to persons or entities submitting the EOI

EOI NOTICE

RailTel Corporation of India Limited,
Kerala Territory Office, 1st Floor,
Eastern Entry Tower,
Ernakulam South Railway Station,
Ernakulam-682016

EOI NO. RCIL/SR/ERS/2025-26/EOI/03 DTD. 27-05-2025

RailTel Corporation of India Ltd., (here after referred to as "RailTel") invites EOIs for Selection of Partner Request for Setting up Security Operations Centre (SOC) as part of KSEBL Data Centre under RDSS Scheme from RailTel Empanelled/In Process of Empanelment Business Associates for exclusive TEAMING ARRANGEMENT for the following "Setting up Security Operations Centre (SOC) as part of KSEBL Data Centre under RDSS Scheme"

KEY INFORMATION

Closing date for Submission of e-Bids	30-05-2025 at 15:30 Hours
Date of opening of E-Bids	30-05-2025 at 16:00 Hours
EMD at the time of submission of bid	Rs. 2,00,000/-
Bid Validity Period	210 days
e-EoI portal for Submission of Bids	https://railtel.eNivida.com
Cost of EoI Document	Nil
Place of Opening of EoI	Online RailTel Corporation of India Limited, Kerala Territory Office, 1st Floor, Eastern Entry Tower, Ernakulum South Railway Station, Ernakulam-682016

Note:

RailTel reserves the right to change the above dates at its discretion. Bids received after due date and time will be summarily rejected.
EoI Notice and link for EoI Document are available on RailTel's website and e-EoI portal https://railtel.eNivida.com for download. For online bid submission the bidder will have to necessarily download an official online copy of the EoI documents from e-Nivida Portal. All future Information viz. corrigendum/addendum/ amendments etc. for this EoI shall be posted on the RailTel's website and e-EoI Portal only. Printed copy of EoI document will not be sold from RailTel office. Bid will be submitted online on e-Nivida Portal only.

Sd/- (JGM/TERRITORY MANAGER)

Earnest Money Deposit (EMD)

1) **EMD payable**: To be submitted by the selected BA shall be submitted in the form of Bank Guarantee/Online Bank Transfer/Fixed Deposit as Total EMD, including the EMD submitted.

2) EMD Rs **2,00,000/-** is to be submitted at the time of submission of EoI in the form of RTGS/Bank Guarantee/ Fixed Deposit.

3) **Validity of the EMD**: The EMD shall be valid till the finalization of end customer RFP/Tender i.e. award of order and till submission of Performance Guarantee of requisite value with due regards to the validity of the offer.

Bids without EMD will be summarily rejected.

The EMD should be in the favour of RailTel Corporation of India Limited payable at Secunderabad through online bank transfer. The Partner needs to share the online payment transfer details like UTR No. date and Bank along with the proposal.

RailTel Bank Details for Submission of EMD / PBG:

Union Bank of India, **Account no.327301010373007, IFSC Code: UBIN0805050.**

Demand Draft shall be submitted in Favor of RailTel Corporation of India Limited payable at Secunderabad.

EMD will be forfeited in case of non-submission of remaining EMD and PBG in time. EMD of unsuccessful Bidders will be refunded by RailTel on finalizing the EoI.

Eligible Business Associates are required to direct all communications related to this Invitation for

EOI document, through the following Nominated Point of Contact persons:

Contact Details for this EOI:

Level: 1 Contact: Shri. Suvin Varghese, DM/Marketing/Ernakulam

Email: suvinvarghese@railtelindia.com Contact: +91-8075285582

Level: 2 Contact: Shri. M Pazhanivelan, JGM/Ernakulam

Email: pazhani@railtelindia.com Contact: +91-90031 44207

Note to Bidders:

1. The response to EOI is invited from **Eligible Empanelled/In Process of Empanelment Partners of RailTel only.**
2. All the document must be submitted with proper indexing and page nos.
3. This is an exclusive pre-RFP partnership arrangement with empanelled business associate of RailTel for participating in the end customer RFP. Selected partner's authorized signatory has to give an undertaking that they will not submit directly or indirectly their bids and techno- commercial solution/association with any other Organization once selected through this EOI for pre- bid teaming arrangement (before and after submission of bid to prospective customer Organization by RailTel). **This undertaking has to be given with this EOI Response.**
4. Transfer and Sub-letting: The Business Associate has no right to give, bargain, sell, assign or sublet or otherwise dispose-off the Contract or any part thereof, as well as to give or to let a third party take benefit or advantage of the present Contract or any part thereof.
5. Bidder has to agree to comply with all OEM technical & financial documentation including MAF, Technical certificates/others as per end-to-end requirement mentioned in the end customer's RFP as applicable and further issued corrigendum's as mentioned below:

Detail regarding END CUSTOMER Tender for reference:

End customer Tender Ref. No.	**CEIT/ITCSD/16/2024-25 dated 30.12.2024**
Tender ID	**2024_KSEB_721478_1**
Date of floating by End customer	**30.12.2024**
Closing time & date	**24.05.2025 at 18.00 hrs**
Floated on portal	**etender Kerala Portal (https://etenders.kerala.gov.in/)**

6. Bidder also shall undertake to submit MAF of major items of the proposed solution and other documents required in the end Customer Organization's tender in favour of RailTel against the proposed products. The selected BA has to provide MAF from the OEM in the name of RailTel for bidding in the concerned tender of KSEBL, if their proposed solution is quoted to the customer as applicable and required.
7. The selected bidder will have to accept all Terms & Conditions of KSEBL RFP on back-to- back basis, wherever applicable.
8. Any corrigendum(s) issued by KSEBL against pertinent tender/RFP shall be the part and scope of this EOI document on back-to-back basis and the BA's shall be on the lookout of corrigendum's issued from time to time by RCIL & KSEBL, in the interest of their own Bid.
9. No exemption/relaxation is applicable to MSME/Start-ups.

10. Only, the eligibility clause/criteria and marks scoring criteria for SI/BA (Prospective BA/SI) as mentioned in KSEBL's RFP is not applicable on the Bidder/BA applying against this EOI. Rest all Terms & Conditions of RFP floated for pertinent tender will be complied by SI/BA/Bidders.

11. However, OEM considered by SI/BA for this project have to mandatorily comply all the eligibility & technical criteria/compliance on back-to-back basis in line with end customer RFP and corrigendum(s) issued thereof.

12. **Please refer KSEBL RFP Payment terms as this will remain applicable on back-to-back basis on Successful bidders. Payment shall be made only after actual receipt of payment from KSEBL on submission of required documents.**

13. Bidder may check the price/commercial bid as per BOQ and match the same with FORMATS FOR SUBMISSION OF THE COMMERCIAL BID of KSEBL RFP and if found any discrepancy, may be brought to the notice of RCIL immediately and may modify their financial bid format as per KSEBL RFP financial bid document.

14. This is a customer centric bid on back-to-back basis and therefore the benefits of MSME shall not be applicable on this EoI & Work Order.

Table of Contents

Contents

1 About RailTel

RailTel Corporation of India Ltd (RailTel) is one of the largest neutral telecom infrastructure providers in the country owning a Pan-India Optic fibre network on exclusive Right of Way (ROW) along Railway track. The OFC network presently reaches to over 4500 towns & cities of the country including several rural areas. With its Pan India high-capacity network, RailTel is working towards creating a knowledge society at various fronts. The portfolio of services provided by RailTel includes Data Centre & DR services, Tele-presence as a service, NLD services, IP-1 services, Internet and Broadband services on a pan-India basis.

Equipped with an ISO 9001, 20000-1:2011 & 27000 certification, RailTel offers a wide gamut of managed telecom services to Indian Telecom market including Managed lease lines, Tower co location, MPLS based IP-VPN, Internet, Data Centre services, NGN based voice carriage services to Telecom Operators, Dark fibre leasing to MSOs/LCOs. The major customer segment for RailTel comprises of Enterprises, Banks, Government Institutions/Department, Educational Institutions/Universities, Telecom Service Providers, Internet Service Providers, MSOs, etc. RailTel being a "Nav Ratna (Category-I)" PSU is steaming ahead in the enterprise segment with the launch of various services coupled with capacity augmentation in its Core network.

The main Project of RailTel/ERS Territory on hand are KFON, KSWAN, Wi–Fi service at Kerala Govt. Secretariat, E health Mission, IOCL, VSS Project etc.

(Please visit ***railtelindia.com*** for more insight)

2 Background of EOI

RailTel Corporation of India Ltd (hereafter referred to as 'RailTel') an ICT arm of Indian Railways has been in the forefront of building innovative platforms and solutions and vision to build range of Information and Communication Technology (ICT) Services for its customers.

In this context, RailTel intends to participate in response to the RFP floated by KERALA STATE ELECTRICITY BOARD Ltd as above (hereafter referred to as 'KSEBL) and accordingly seeks to select a suitable partner for pre-bid arrangement through this EoI for the work of "Setting up Security Operations Centre (SOC) as part of KSEBL Data Centre under RDSS Scheme"

Bidder has to agree to comply with all OEM technical & financial documentation including MAF, Technical certificates/others as per end-to-end requirement mentioned in the end customer's RFP. Bidder also shall undertake to submit MAF of major items of the proposed solution and other documents required in the end Customer Organization tender in favour of RailTel against the proposed products. The selected BA has to provide MAF from the OEM in the name of RailTel for bidding in the concerned tender of KSEBL, if their proposed solution is quoted to the customer, wherever applicable.

The details of tender are as below:

Tender Title: Request for Proposal (RFP) for "Setting up Security Operations Centre (SOC) as part of KSEBL Data Centre under RDSS Scheme"

Ref. No.: CEIT/ITCSD/16/2024-25 dated 30.12.2024; latest amendment/ Corrigendum / clarifications. **Floated on etender Kerala Portal (https://etenders.kerala.gov.in/)**

Method of Quoting

System Integrator (SI)/BA shall quote for single OEM/ make and model for each item description, subject to the confirmation of the given specification equivalence. The make and model shall be clearly mentioned in the proposal. However the subsistence/subcomponents offered shall be compatible with inter-operability to the main system, if different makes/models offered. Deviation to be this will not be accepted/shall be summarily rejected, Wherever applicable.

3 Scope of Work & Partner Selection

The scope of work will be as mentioned in the pertinent end Customer organization RFP/Tender for "**Setting up Security Operations Centre (SOC) as part of KSEBL Data Centre under RDSS Scheme**" on the website **(https://etenders.kerala.gov.in/)** with all latest amendment/Corrigendum/ clarifications. All materials that propose to use with the work shall be approved by the Employer / Engineer-in-charge. The scope of work is subject to addition / deletion by the Employer.

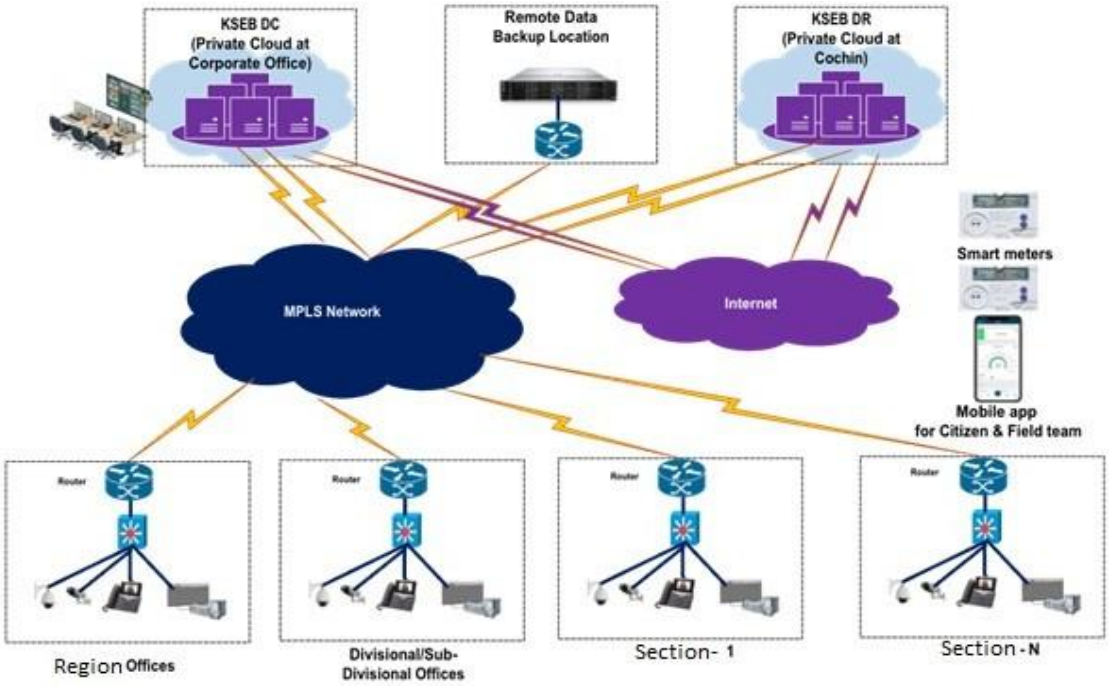
The purpose of the RFP is for setting up On-premises NextGen Security Operations Centre which will be a part of KSEB Data Centre to monitor, assess, detect, respond and defend against cyber threats so as to protect the critical information systems and IT infrastructure installed in KSEB Data Centre.

KSEBL has a Data Centre of tier-III standards functioning at the Corporate HQ located at Vydyuthi Bhavanam, Pattom, Thiruvananthapuram, Kerala with a Server farm area of 1800 Sq.ft. and a rack capacity of 48 nos. of 42U racks. The Disaster Recovery Centre of KSEB is functioning at Infopark, Cherthala, Ernakulam in almost a similar replica of the Data Centre. Both of the above infrastructure were established as part of implementation of Part-A of RAPDRP in 2013. Since the IT infrastructure at DC and DR are becoming old and obsolete, revamping and up-gradation of the same has been included as a key initiative under the RDSS project funded by GoI. As part of the above, it is proposed to carry out the revamping of compute clusters, network infrastructure, storage, backup systems etc. in the Data Centre and DR Centre in accordance with the state of the art technologies and industry standards. Tender processes for the above are in progress.

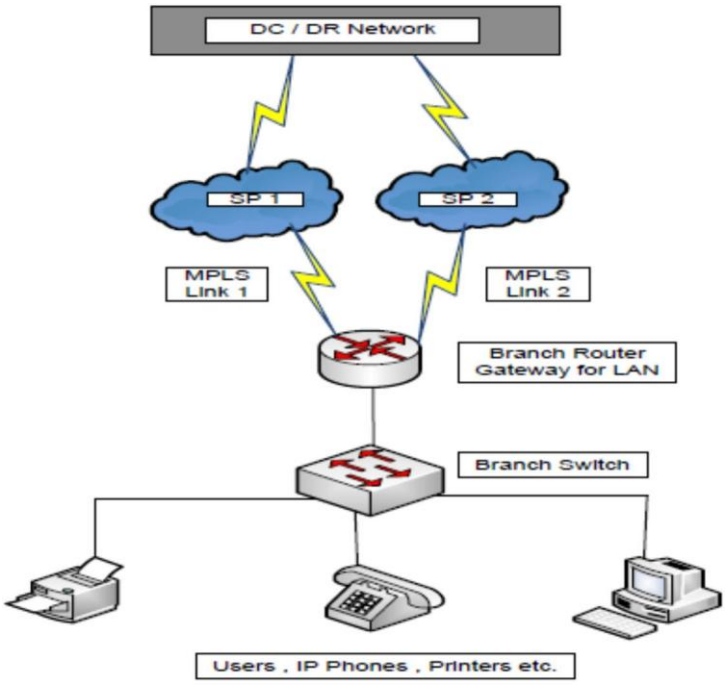
Apart from the Data Centre and DR Centre, KSEB is having around 890 field offices under Distribution Wing at which various activities related power distribution is taking place. Steps are also being taken to carry out the ramping of the existing MPLS WAN connecting the DC, DR and field offices by setting up SDWAN among the Data Centre, DR Centre and Field offices all over Kerala utilizing the existing MPLS links, Internet leased lines and FTTH connectivity available in the above locations.

The proposed Security Operation Centre which will be setup as part of the Data Centre will monitor, assess, detect, respond and defend against cyber threats so as to protect the critical information systems and IT infrastructure installed in KSEB Data Centre and WAN.

EXISTING ARCHITECTURE OF KSEB WAN

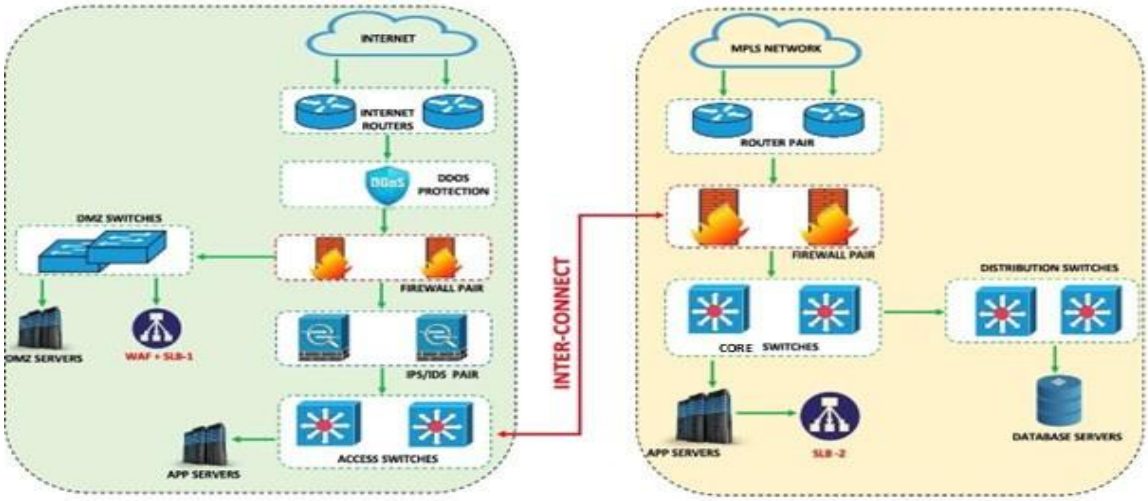


EXISTING NETWORK CONNECTIVITY AT FIELD OFFICES



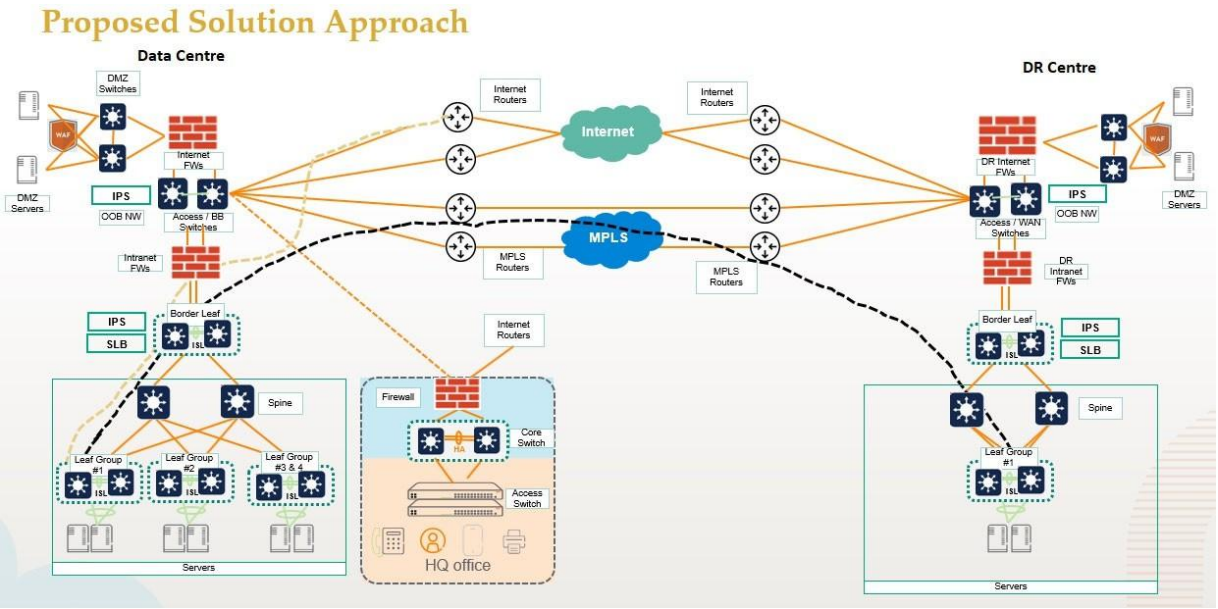
EXISTING NETWORK ARCHITECTURE AT DATA CENTRE / DR CENTRE

The following schematic describes the equipment housed in the Data Centre (DC), including routers, switches, firewalls, servers, SAN (Storage Area Network) storage, backup solutions, and other devices critical to the IT infrastructure. It provides a clear overview of the hardware components supporting the Data Centre's operations and their respective roles in the system.



The DR Centre located at Infopark, Cherthala is also having a similar architecture of IT infrastructure in terms of Servers, network equipment, security devices, Storage etc. The existing infrastructure at DC as wells as DR is nearing obsolescence, especially the Servers, network equipments, Storage etc., pointing to the need for a revamping.

In view of the above, KSEB has invited RFP for revamping of the existing DC/DR IT infrastructure as per the following network architecture.



The tender processes for carrying out the revamping of the DC/DR IT infrastructure as mentioned above are in

progress and it is expected that the works will be completed within a period of 8 months. Hence the successful bidder for SOC shall have to setup the SOC as per the present architecture which shall be reconfigured to work with the new architecture as and when the revamping works of DC/DR will be completed as per the ongoing RFP.

Similarly, since the existing MPLS WAN equipments connecting DC, DR and field office is nearing obsolescence, KSEB has invited RFP for migration of MPLS WAN to SDWAN. On completion of the above, the Core routers at DC and DR will be replaced by SDWAN Hub devices. Hence the successful bidder shall have to configure the SDWAN devices also to the SOC.

SETTING UP SECURITY OPERATIONS CENTRE (SOC)

The proposed on-premises Security Operations Centre shall be functioning in the following stages so as to defend the cyber threats:

Detection Stage - This phase would involve the collection of threat feeds from various devices/equipment/applications spread across the Data Centre and WAN. These feeds would be primarily provided visibility and insight into the entire network traffic being generated across the IT Infrastructure of KSEB; these feeds are incorporated into the SOC to provide visibility into the entire architecture. Detection stage leverages various technologies to identify, Triage and Prioritize response against sophisticated cyber threats. This helps in content visibility and Multi-Vector Inspection.

Analyse Stage - During this phase advance analysis is undertaken based on the information collected and discovered in the Detection stage. Activities undertaken in this stage primarily involve detecting anomalies/ behavioral changes in the network infrastructure, threats against various assets in the network and their corresponding vulnerabilities. This Stage would involve deep host and network forensics, content normalization, Heuristic file and code analysis leveraging the following technologies.

Respond Stage - Once the attack has been detected after analysis, the appropriate action needs to be undertaken in the most automated manner, which would involve blocking of real time threat and attacks across the network infrastructure of KSEB. Response should focus on to identify, isolate, and remediate threats. Response leverages detection and analysis framework to enrich contextual awareness and intelligent capturing. Each of the above defined stage provides input at each level of collection, analysis, confirmation and as far as possible automated responses to the alerts and incidents created across the enterprise-wide dashboard.

Below mentioned is the list of security devices currently deployed at the Data Centre:

Sl. No.	Security Device	Qty. (Nos)
1	Intrusion Detection System/Intrusion Pretension System (IDS/IPS) (Radware Defense Pro)	4
2	NextGen Firewall - Checkpoint	4
3	Web Application Firewall (WAF) - Radware	2
4	Server Load Balancer - Radware	2
5	Distributed Denial of Service (DDoS) Appliance - Radware	1
6	Single Sign-On System (Citrix)	2

Additionally, the Data Centre and HQ network contain the following major Servers and network devices:

Sl. No.	Item	Qty. (Nos)
1	Core Router (HP)	4
2	Core/Distribution/Access Switch (HP)	6
4	Application/Database Servers (HP)	50
5	VM/Containers	200
6	Endpoints (Desktops)	700

Considering the total numbers of Servers, network devices and security equipments, the estimated logged Events Per Second (EPS) is 12,000. Accordingly, the proposed Architecture, Scope, and Technical Specifications for setting up the SOC are furnished as follows:

SOC- FUNCTIONAL REQUIREMENTS

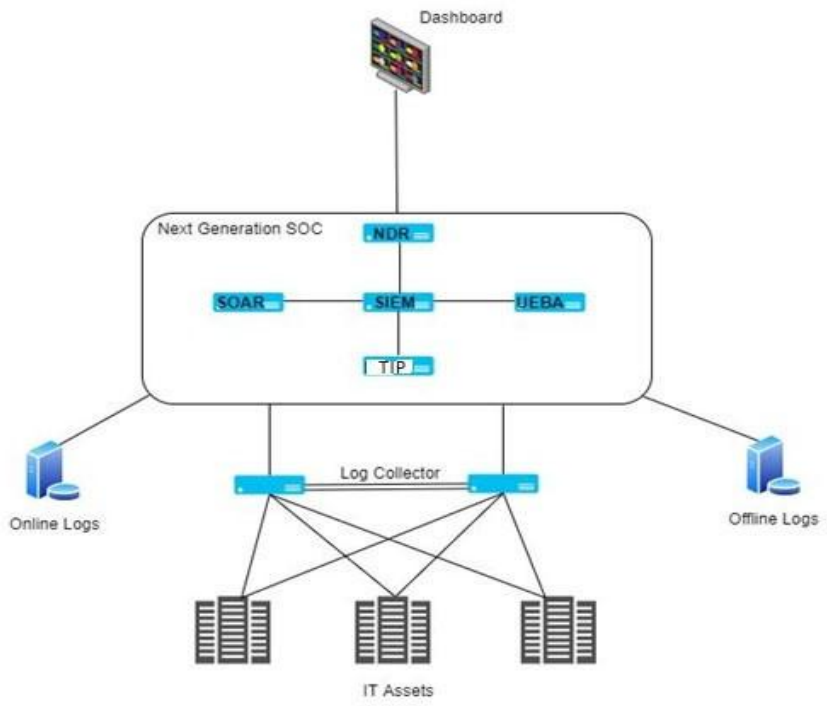
Monitoring and Log Analysis Services

1. Monitoring of 2000 devices– Provision to increase 20% every year on SOC expansion. The proposed SOC solution shall support 12000 EPS which shall be scalable to 20000.
2. The proposed SOC solution shall include the following modules: SIEM, SOAR, UEBA, NDR and TIP
3. Monitoring & Recording of all ingress points traffic for the above mentioned traffic with full packet capture replay capabilities.
4. Management of Security devices deployed as per the scope of setting up the Security Operations Centre including rule base audit and management of devices creation of rules during non-business hours. Monitoring of 24x7 logs & audit trails for the security events to detect known as well as unknown attacks and raising alerts on any suspicious events that may lead to security breach into SOC environment. Monitoring of 24x7 performance and service availability so that the desired state and integrity of the devices and services levels are maintained.
5. To be able to support and provide scalability for any additions/modifications or integration of applications, services, devices and networks with the existing architecture.
6. Performing Analysis of any suspicious traffic and initiating response in co-ordination with the SOC/DC IT team
7. Providing initial review (Level 1) of security incidents and the determination if escalation to Level 2, 3 supports is warranted.
8. Carrying out event analysis with the statistical events correlation rules. This should include the correlation of the events from the devices under scope.
9. Creation and adding custom correlation rules for the SOC/DC's devices under scope. SOC will review and fine-tune rules as and when required.
10. Providing online secured portal (web-based Dashboard) for viewing real-time monitoring data of all the security devices in scope.
11. To Review, Develop& recommend improvement plans for the SOC monitored SOC/DC's facilities as needed

to maintain an effective and secure computing environment. The activity to be carried out once in 6 months.

12. Monitoring alerts and events reported by devices under the SOC scope; to record the incidents, classify, and recommend remedial action. All types of incidents will have to be reported immediately as per the escalation matrix.
13. Initiation of prompt corrective countermeasures to stop/prevent attacks as per predetermined procedures.
14. Complete analysis and correlation of logs from all the devices under scope.
15. Carrying out due forensic activities to identify the origin of threat, mitigation steps and measures to prevent recurrence.
16. Preparation of the daily/ weekly / monthly reports to summarize the list of incidents, security advisories, vulnerability management, and other security recommendations. It should include the operations trend analysis with the reports correlation of the present month's operations data with the previous months' data.

SOC - Basic Architectural Diagram



The major functional components of the Security Operations Centre are explained below:

SIEM (Security Information and Event Management)

Security information and event management, SIEM for short, is a solution that helps organizations detect, analyze, and respond to security threats before they harm business operations. SIEM tools collect, aggregate, and analyze volumes of data from an organization's applications, devices, servers, and users in real-time so security teams can detect and block attacks. SIEM tools use predetermined rules to help security teams define threats and generate alerts. SIEM systems can mitigate cyber risk with a range of use cases such as detecting suspicious user activity, monitoring user behavior, limiting access attempts and generating compliance report

SOAR (Security Orchestration, Automation and Response)

SOAR (Security Orchestration, Automation, and Response) refers to a collection of software solutions and tools that

allow organizations to streamline security operations in three key areas: threat and vulnerability management, incident response, and security operations automation. Orchestration, as a term, covers threat and vulnerability management, which include all the technologies that assist with the resolution of cyber threats. Automation refers to security automation, which describes the process of utilizing progressive automation and machine learning to automate particular areas of security operations. The term response refers to security incident response, which measures in detail how the organization responds to threats, in order to use that information to strategically increase the effectiveness of SecOps.

UEBA (User and Entity Behaviour Analytics)

User and entity behaviour analytics (UEBA), also known as user behaviour analytics (UBA), is the process of gathering insight into the network events that users generate every day. Once collected and analyzed, it can be used to detect the use of compromised credentials, lateral movement, and other malicious behaviour. This allows organizations to quickly identify and respond to potential threats that might otherwise go unnoticed.

NDR (Network Detection and Response)

Network Detection and Response (NDR) is a cybersecurity technology that continuously monitors network traffic from physical and cloud-based environments to enable security teams to detect adversary activity, respond to incidents, and shore up their security posture. NDR solutions analyze network traffic to detect malicious activity inside the perimeter—otherwise known as the east-west corridor—and support intelligent threat detection, investigation, and response.

Central Log Collection Server

A central log collection server is a crucial component of a Security Operations Center (SOC) infrastructure. It acts as a centralized repository that gathers and stores log data from various network devices, systems, and applications. By consolidating logs in one location, SOC analysts can easily access, analyze, and correlate information to identify potential security threats, investigate incidents, and proactively respond to emerging risks. This centralized approach streamlines the monitoring and detection process, enhancing the SOC's ability to safeguard the organization's critical assets and data from cyber threats.

Log Archive Server

A log archive server in a Security Operations Center (SOC) is a dedicated system responsible for securely storing historical log data from various sources within the organization's network. It acts as a long-term storage repository, allowing SOC teams to retain log information beyond standard retention periods. This archival capability is valuable for conducting in-depth forensic investigations, compliance requirements, and historical analysis of security events. By having a log archive server, the SOC can maintain an extensive record of past activities, facilitating a comprehensive understanding of the organization's security posture and aiding in future threat prevention strategies. The Log Archive Server shall be capable of retaining the archived logs for a period of three years.

Indexed Log Server

An indexed log server in the context of SOAR is a specialized system that organizes log data in a structured manner for efficient and quick retrieval. It creates searchable indexes of log entries, allowing SOAR platforms to access and analyze relevant information rapidly during incident investigations and response. This indexed approach streamlines the SOC's ability to correlate and contextualize security events, enabling faster decision-making and automated response actions based on historical data. Ultimately, the indexed log server enhances the overall effectiveness and speed of the SOAR platform in addressing cyber security threats.

SURVEY AND ASSESSMENT

CONDUCT A COMPREHENSIVE SURVEY OF THE EXISTING DATA CENTRE COMPONENTS

- Security Infrastructure: Comprehensive review of firewalls, access controls, encryption mechanisms and vulnerability management to ensure robust security measures are in place
- Hardware Evaluation:
  - Review of network components, Servers, Storage systems to ensure optimal network performance
- Software & Applications:
  - Assessment of operating systems, applications etc. for compatibility and security.
- Network Architecture:
  - Analysis of network topology, bandwidth usage, latency, and redundancy for optimized connectivity and fault tolerance.
- Assess short-listed potential areas for service rollout.

SOC DESIGN AND PLANNING

- Develop a detailed design, deployment and integration plan
  - Infrastructure Architecture:
    - Design the overall architecture including network systems, security systems etc. to ensure optimal performance, scalability, and redundancy including rack design
  - Network Design:
    - Develop a robust network topology that supports high bandwidth and redundancy with clear paths for internal and external connectivity, load balancing and failover mechanisms.
    - Optimal Integration with existing/revamped Data Centre, MPLS WAN / SDWAN, HQ network Endpoints etc.
  - Implementation Plan
  - Security Framework:
    - Integrate with existing security solutions like DDoS, IDS/IPS, NGFW, WAF etc. in correlation with overall Organisation security policies
  - Disaster Recovery & Business Continuity:
    - Design a comprehensive disaster recovery plan for service availability, failover systems and high availability to minimize downtime and ensure quick recovery in case of disruptions in the SOC services
  - Compliance & Governance:
    - Ensure the design meets regulatory and industry standards (e.g., ISO, GDPR) for data security, privacy, and operational procedures.
  - Submit the following documentation:
    - SOC Solution Design Document including HLD/LLD
    - Implementation /Migration Plan

The above mentioned documents/plan will be finalized after joint discussion with KSEB officials and OEM. The implementation shall be started only after approval of the above documents from the KSEB. Bidder has to start OEM engagement immediately after receiving of LoA and has to submit the plan within 1 weeks from the date of LoA.

SOC INSTALLATION, CONFIGURATION AND INTEGRATION

1) Bidder is required to supply, install, configure, test and commission the required Hardware, software and compute (inclusive of all active & passive components and subcomponents, accessories) as per the technical

and functional specification mentioned in the RFP document.

2) The licenses supplied by the selected bidder should be in the name of KSEB valid perpetual for life and handover to KSEB.
3) Bidder is required to provide Racks with PDU & other components as per industry standards for tier-III Data Centre for hosting the SOC hardware
4) The bidder should provision the required hardware and software components which mentioned in the RFP to be implemented under this RFP Scope.

5) The Bidder has to ensure that if any additional component(s) required for overall solution to comply with the implementation to achieve desired objectives and SLA levels, then in such case it should be the responsibility of the bidder to provide the same as a part of the entire solution.
6) The architecture needs to be scalable to meet future demand.
7) Bidder shall be responsible for setting up of on premise SOC at KSEB DC premises and provide the required security services for period of 5 years. The Onsite resources (People, Process and Technology) required to run and manage the SOC shall be deployed from the bidder's own sources to manage, monitor, analyze and report incidents as they occur
8) The requirements in the captive Security Operations Centre (SOC) shall at the minimum include the following functionalities/capabilities. Accordingly, the bidder shall:
   a) Implement, Integrate, customize, manage, and maintain Security Information & Event Management (SIEM), SOAR, UEBA, NDR and Resources to meet SOC's Requirements.
   b) Perform gap analysis between the SOC's requirements and the services functionality of SIEM, SOAR product and other tools and technologies
   c) Setup SOC solution as a framework that is comprehensive, scalable and addresses all security aspects.
   d) Integrate and Monitor security incidents of tools/devices - Network, Security, and other devices
   e) Manage and carry out rule-based Audit of Security Devices:
      - NextGen Firewalls
      - IDS/IPS
      - DDoS
      - Web Application Firewall
      - SOC Rules Intelligences
      - SOC Operations
   f) Build custom interfaces if required for integration
   g) Provide Security Intelligence for SOC Solutions
   h) Provide post implementation monitoring & management support.
   i) Integrate any other device procured by KSEB.
   j) Provide on-site monitoring services for
      - 24x7x365 Real-time Security Monitoring in a Fully Managed Service Delivery Model
      - Correlation of event logs with other relevant security information including vulnerability information, network flows etc.
      - Leverage the SIEM solution detect, analyze, and qualify security alerts for various use-cases
      - Escalate qualified security incidents to SOC for further investigation.
      - Create incident tickets in a ticketing tool for the qualified incidents and alerts
      - Analyze false positives and recommend modification/deletion of correlation rules.
      - Provide remediation recommendations.
      - 24x7x365 SOC Tools & SOC Infrastructure Administration and Support in a Co-Managed Service

Delivery Model

- Perform Health and Availability monitoring and notification of the SOC solution
- Perform Validation of successful configuration backup and log archival based on KSEB policies

k) Provide single integrated and consolidated enterprise view of security and compliance in the dashboard

l) Provide roll-out plans for each of the deliverable and adhere to the same

9) Bidder has to submit the HLD, LLD, detailed project plan etc. for SOC. It is preferable that configuration, Implementation, and commissioning will be done by respective OEM for particular device.

- Bidder should provide the overall program management and should undertake OEM support for their respective technologies from various OEMs so as to ensure seamless implementation as per the design goals.
- The OEM resources should be engaged to collect the Customer requirement to achieve business outcomes and based upon that provide the specific solution designing (OEM High-Level & Low- Level Design) with Implementation & configuration implementation support to the bidder for deployment. OEM should also provide a test plan that should be executed by the bidder before go-live to ensure that OEM supplied technology & products work as per the design objectives.
- OEM to design and implement the complete security policy and workflow as per industry best practice in consultation with SOC to meet their business requirements.
- The bidder shall obtain sign-offs from OEM on the system design & deployment architecture before go-live of the envisaged system and submit before Acceptance Test.

10) The support including spares, patch updates, for the quoted products shall be available for the entire period of the Project without any additional cost.
11) Successful bidder is required to undertake the Operation and Maintenance of the entire solution on completion of Go-live.
12) The bidder needs to provide a comprehensive, on-site training on deployed solution to the team nominated by KSEB.

COMMISSIONING & ACCEPTANCE

1. Date of Commissioning of SOC shall be considered on the day when the below tasks are completed-
   - Installation and deployment of all Data Centre SOC components.
   - Integration, configuration and finetuning with all existing network, security and Server components.
   - Fully functional Monitoring, Analytics, Reporting and Dashboards.
   - 24x7 SOC Monitoring facility is functional with all infrastructure facilities and technical resources as per RFP requirements
   - Submission of all concerned technical documents as per RFP

2. **Acceptance:** Acceptance of the total Solution will be provided by the KSEB to the bidder after accomplishment of all stated below task
   - The bidder has to submit certificate from OEM to the KSEB after thorough examination stating that all Data Center components deployment has been completed and integration of all security devices and systems to be monitored has been done, as per the OEM recommended best practices.
   - All the points specified in the technical specifications of this RFP are met.
   - The solution shall be thoroughly tested against the following (but not limited to) set of test cases for

acceptance.

- Active-Passive failover test for all the DC SOC components.
- Monitoring Tools: Validate that monitoring tools are correctly configured to track key performance metrics, resource usage, and security incidents.
- Alerting Mechanisms: Test alerting systems to ensure timely notifications in case of performance issues, security breaches, or hardware failures.

POST IMPLEMENTATION SUPPORT, MAINTENANCE AND UPGRADES

1) Bidders shall support the SOC Solution and its associated items/components including OS/firmware during the period of Warranty/Extended Warranty as per the provisions of SLA specified in this RFP.
2) During the warranty period, Service Provider will have to undertake comprehensive support of the entire Product (hardware/components/ operating software/firmware) supplied by them at no additional cost to KSEB. During the support period (warranty), bidder shall maintain the Product (hardware/ software, etc.) to comply with parameters defined for acceptance criteria and bidder shall be responsible for all costs relating to labour, spares, maintenance (preventive and corrective), compliance of security requirements and transport charges from and to the designated site in connection with the repair/ replacement of the Product (hardware/ equipment/ components/ software or any component/ part thereunder), which, under normal and proper use and maintenance thereof, proves defective in design, material or workmanship or fails to conform to the specifications, as specified.
3) During the support period, bidder shall ensure that services of professionally qualified personnel are available for providing comprehensive on-site maintenance of the Products and its components as per KSEB's requirements. Comprehensive maintenance shall include, among other things, day to day maintenance of the system as per OEM guidelines, reloading of firmware/software, compliance to security requirements, etc. when required or in the event of system crash/malfunctioning, arranging and configuring facility as per the RFP, fine tuning, system monitoring, log maintenance, etc. In case of failure of Product (hardware, system software or any of its components), bidder shall ensure that the Product is made operational to the full satisfaction of KSEB within the given timelines.
4) On site comprehensive warranty for the Product would include free replacement of spares, parts, kits, resolution of problem, if any, in the total solution.
5) Support would be on-site and comprehensive in nature and must have back-to-back support from the OEM. Bidder warrants Products against defect arising out of faulty design, materials, etc. during the specified support period. Bidder will provide support for operating systems and other pre- installed software components/system software during the specified period of the hardware on which these software and operating system will be installed. Service Provider shall repair or replace worn out or defective parts including all active/passive components of the Equipment at his own cost including the cost of transport.
6) In the event of system break down or failures at any stage, the following measures shall be ensured by the bidder:
   - Diagnostics for identification of systems failures
   - Protection of data/ Configuration
   - Recovery/ restart facility
   - Backup of system software/ Configuration
7) Prompt support shall be made available as desired in this RFP during the support period as and when required.
8) The support staff should be well trained to effectively handle queries raised by the employee(s) or authorized user(s) of KSEB.

9) Updated escalation matrix shall be made available to KSEB once in each quarter and each time the matrix gets changed.

ONSITE RESOURCES:

The bidder shall provide dedicated onsite L1 and L2/L3 resources at the Data Centre for the entire contract period from the date of commissioning for carrying out the SOC operations on 24x7 basis. The onsite resources shall have required qualification and experience as specified in this RFP. Prior approval of KSEB shall be sought for appointment of the above personnel at the Data Centre. The responsibilities of the Onsite Resource must include, but not be limited to, the following :-

- Attend, Coordinate and Rectify all support activities/cases at Data Centre for addressing issues related to SOC implementation and maintenance at DC
- Raising a TAC case on behalf of KSEB.
- Onboard the relevant teams (of OEM or bidder) for support as per requirement.
- Getting the relevant updates / upgrades for the solution components and the required support for installation / application of the same.
- Resolution of any VA points by way of bug fixes, security updates etc. this shall include development of any new patches / bug fixes as required.
- OS upgradation suggestions and recommendations according to the KSEB's environment.
- Periodic assessment and suggestion regarding upgradation, mitigation of repetitive issues, possible threats, effective compliance check, better visibility and controls etc.

SOC Operations Team Specifications

The asset list and service deliverables are provided in this RFP for the bidder to assess the volume of work and accordingly provide the below mentioned personnel with appropriate skills. The minimum team structure is provided in the table below. The table lists the roles, skill sets of personnel required for the above deliverables.

Sl No.	Role	Qualifications and Experience	Minimum No of resources	Level
1.	Sr. Security Analyst/ Sr. Technology Specialist	▪ Education: B.E. / B. Tech / MCA degree. Certified with: EC Council-CEH/CompTIA Security+/ CISSP/ CHFI or Professional OEM certification. ▪ 5+ years of relevant experience in managing all aspects of risk and incident analysis in SOC. Must have experience in managing at least 1 projects for enterprise scale Clients. ▪ Shall be responsible for deployment, maintaining, tuning, monitor and managing all aspects of client SOC. Responsible for coordinating, in a timely manner, all activities	1	L2/L3

	(on 8x6 basis)	necessary for security incident monitoring, analysing incidents / risks, incident / risk containment, identifying root cause, initiate problem resolution, incident / risk response and communication. ▪ Shall have experience of monitoring the database security logs/alerts and shall take complete ownership for the same.		
		▪ Well versed with aspects of database security, access control, identity management etc. ▪ Should have experience of firewall, IDS/IPS, Anti-APT solution etc.		
2.	Security Analyst (on 24x7x365 basis)	B.E/B. Tech/ MCA degree Certified with: OEM Certification/ Certified SOC Analyst (CSA)-EC Council/ CompTIA CySA+ 3+ years of overall experience with at least 1 years of relevant experience in all aspects of Incident monitoring in SOC	1	L1

General Guidelines for Soc Operations Team

- The SOC team will work in 24x7x365 environment and personnel resources should be able to work in shifts and flexible working hours to support the operations.
- KSEB reserves the right to interview all the personnel resources to be deployed on the project and reject if not found suitable for the project.
- At a later stage also if any of the personnel resources are found unsuitable to perform duties or any of the personnel resources violates any of the KSEB guidelines, KSEB may seek removal of all such personnel resources.
- KSEB expects to build a strong team and there should be no single point of dependency on any one individual. DC services should always remain immune to any such dependencies.
- Bidder is required to obtain permission from KSEB in writing before removing any of the personnel resources from the project.
- KSEB expects deployed resource / personnel resources to constantly keep upgrading their product / domain knowledge & skills.
- As soon as KSEB adopts a newer version of an existing technology, KSEB expects the existing staff working in the project to get certified on the same or the Bidder should arrange for the additional resources with requisite qualifications/certifications.
- Proper on-boarding and off-boarding processes are required to be followed.
- All the staff are required to abide by the KSEB's applicable policies and NDA.
- The teams should be adequate to ensure the unhindered 24x7x365 operations and support.
- L2/L3 Engineer /Team Lead would be the single point of contact for SOC.
- A detailed shift roster must be published at the start of the month in consultation KSEB
- The onsite resources must work as per KSEB's working days and hours or as decided by KSEB for smooth

functioning of SOC.

- Bidder will be responsible for police verification & background checks of all resources before on boarding

Minimum Roles and Responsibilities:

Resource Level	Roles & Responsibilities
L2/L3 (Sr. Security Analyst)	• Monitor SOC Solution Console & Dashboards and provide response to the reported incidents Filtered by L1. • Monitor and review the L1/L2 activities • Support the day-to-day operation of a highly available distributed multi-clustered multi-tenant SOC Solution deployment. • Perform initial analysis for known issues and provide the appropriate recommendations for closure. • Monitor & Reporting of system components health and take necessary action in case of any observed issue. • Provide notification and communication with Incident management and respective application team upon threat detection. • Perform analysis on the reported incidents, determine the root cause, recommend the appropriate solution. • Should provide real time situational awareness to the KSEB stakeholders. • Use and apply learnings from incident and provide recommendation for standardizing the SOC Solution. • Develop and implement processes for interfacing with operational teams and other supporting teams. • Ensure the SOC Solution integration is intact among the SOC/DC SOC solutions, other assets • Design, create and customize the dashboards as per the SOC/DC's requirements. • ensure the necessary SOC/DC SOC documents like operating procedures, configuration management, Low Level Design etc. are up to date with the changes made in their respective areas. • Automating Day to Day Tasks related with SOC Solution Operations • Above is illustrative list of general activities. All Technology specific activities Related to SOC Solution to be carried out. • SOC Solution Management, SOC Solution Monitoring, SOC Solution Operations, SOC Solution Automation, Content Development to fine-tune existing rules & develop new content based on latest threat vectors. Ensure & keep improving SOC Solution platform for better Return on Investment. • Should have good understanding on MITRE ATT&CK framework. • Take up the resolved/serious security issues with the OEM backend team for timely support and rectification

L1 (Security Analyst)	• Level 1 analyst will identify, categorize, prioritize, and investigate events rapidly utilizing triage and response guidelines for the enterprise using commonly available SOC log sources that include: • Firewalls and network devices. • Infrastructure server and end-user systems. • Threat intelligence platforms. • Web proxies. • Application logs and web-application firewalls. • Identity and access management systems. • Cloud and hybrid-IT provisioning, access and infrastructure systems. • Antivirus systems.
	• Intrusion detection and prevention systems. • Monitor incoming event queues for potential security incidents. • Perform initial investigation and triage of potential incidents and escalate or close events as applicable. • Monitor SOC ticket (or email) queue for potential event reporting from outside entities and individual users. • Maintain SOC shift logs with relevant activity from the shift. • Document investigation results, ensuring relevant details are reported to level 2 analyst for final event analysis. • Update or refer SOC collaboration tool as necessary for changes to SOC process and procedure as well as ingest SOC daily intelligence reports and previous shift logs. • Conduct security research and intelligence gathering on emerging threats and exploits. • Perform additional auxiliary responsibilities as outlined in the console monitoring procedure. • Communicating emergency alerts & warnings to designated stakeholder/ departments/ SOC.

COMPLIANCE AND REGULATORY REQUIREMENTS

- Ensure the design and implementation meets regulatory and industry standards (e.g., ISO, ISMS, GDPR etc.) for information/cyber security, privacy, and operational procedures.

DOCUMENTATION AND REPORTING

- Maintain detailed documentation of the SOC infrastructure, configurations, and system specifications.
- Prepare regular progress reports, including project milestones, implementation status, and key performance indicators.
- Provide comprehensive documentation and handover materials to facilitate future operations and maintenance.
- In addition, provide documentation standards for SOC Architecture diagrams, configurations, and operating procedures; reporting requirements, including progress reports, milestone updates, and key performance indicators; and system documentation.

PROJECT MANAGEMENT

- Assign a dedicated Project Manager onsite responsible for overseeing and coordinating all project activities.
- Develop a detailed project management schedule with clear milestones, timelines, and deliverables.
- The project management schedule shall be submitted to KSEB Nodal Officer for approval.
- Conduct regular project meetings and maintain open communication channels with all stakeholders to ensure that timelines are met.

Training

- The bidder shall ensure comprehensive certification training to be conducted by the OEM for 10 KSEB officials within a period of 3 months from the date of commissioning of the project.
- The necessary study material for training shall be arranged by the bidder. The bidder shall provide all necessary means and expenses for SOC training (up to Expert level) to the KSEB staff without any extra cost to KSEB.
- The bidder shall provide a comprehensive training plan from Basic level up to Expert level (Highest). This should include all relevant study materials, lab access, etc. to carry out the training for the designated KSEB officials.
- The bidder shall ensure that training shall be offline (in-person) and shall include hands-on training session and labs along with theoretical sessions. A suitable venue for training shall be arranged by the Bidder after consultation with KSEB.
- The bidder shall ensure that training session should be conducted by OEM certified professional trainer / professional services resource.
- Cost of training material, trainer fees, accommodation and travel of trainer, training site etc. shall be borne by the Bidder.

INDICATIVE BILL OF MATERIALS

INDICATIVE BILL OF MATERIAL AT DC, DR AND FIELD OFFICES

The following is an indicative bill of materials required to carry out the revamping works as per the RFP specifications at DC, DR and Field Offices from Day 1.

Sl No.	Item	Qty (Nos.)
Data Centre		
1.	SOC Services with SIEM, SOAR, UEBA and NDR	1
2.	Threat Intelligence Platform Service	1
3.	Central Log Collection Services	1
4.	Log Archival Services	1
5.	Indexed Log Services	1
6.	75” Professional Display	2

7.	Professional Workstation with dual monitors	7
8.	Installation, integration, testing and commissioning	1
9.	Man Power charges for L1 resources (24x7x365 basis) for five years	1
10.	Man Power charges for L2/L3 resources (8x6 basis) for five years	1

Note:

1. The cost quoted shall include the charges for all hardware, software, licenses and accessories required for providing the SOC solution as per the RFP requirements in High Availability mode at the Data Centre, with onsite warranty/support for five years. The details of the hardware requirement for each module shall be furnished by the bidder in the format given in the RFP.

2. The BoQ items mentioned above are indicative only. The bidder is liable to provide additional items/ services/ accessories required, if any, for providing all required features/ functionalities/ services mentioned in the Scope of Work.
3. Cyber Security Compliance: All products (hardware/software) quoted by the bidder shall comply with the statutory guidelines of Government of India related to Cyber Security, industry standards etc.

HARDWARE, TOOLS, RESOURCES REQUIREMENT FOR SOC

Bidder shall submit the hardware sizing in below table along with Bid. Supply of required hardware will be under the scope of the Bidder. Any other Items like OS, DB licenses requirement need to be factored by Bidder along with SIEM, SOAR, UEBA and NDR Software cost. Bidder will provide all required software licenses from day 1.

S/N	Application Name	Physical/VM	No. of Instance	vCPU per VM	RAM/ VM	OS Storage (GB)	External Storage (TB)	Total External Storage (TB)	Disk type for External Storage	OS Details	Database Software if any

INDICATIVE BILL OF MATERIAL DURING NEXT FOUR YEARS (UPGRADE BASED ON DEMAND)

The following is an indicative bill of materials which may be required to scale up or upgrade the existing SOC solutions during first four years of the Contract Period of 5 years for which PO will be raised based on the Utility's demand. The below BoM will also be considered for price discovery and price bid evaluation purposes.

Sl.No	Specifications	Qty (Nos.)
Data Centre		

1.	Additional License for SOC solution for 1000 EPS (1 Unit)	5

PROJECT SCHEDULE

Sl No.	Items	Timeline	Deliverables
1.	Issue of LoA	T0	-
2.	Kick of meeting	T0 + 1 weeks	Project Plan, Minutes of meeting
3.	Delivery of Components	T0 + 6 weeks	• Software components • Hardware components
4.	Installation, integration & commissioning (all software, hardware, licenses etc.)	T0 + 14 weeks	• Solution Architecture documents. • Logical & physical design • Completion of UAT and closure of observations • Integration testing report • Test cases & SOPs for SOC
5.	Acceptance testing, Go-Live & training	T0 + 18 weeks = T	• Successful Implementation of SOC solution as per specification and functional requirements in the RFP
6.	• Deployment of man power proposed for O&M for SOC • Warranty Support	T + 5 years	• Providing onsite resources as per RFP • Comprehensive warranty support for all supplied products

3.1 Warranty & AMC

The warranty would be valid for the performance of products, service and application as applicable in the **KSEBL RFP on Back to Back basis for** 5 years On-site OEM comprehensive warranty.

On-site comprehensive warranty: The warranty shall be on-site and comprehensive in nature with back- to-back support from the OEM. The bidder shall warrant all the hardware and software against defects

arising out of faulty design, materials and media workmanship etc. for a period of 5 years from date of Date of Installation. Warranty period starts from the Date of Installation and commissioning.

The bidder shall also provide support for Operating Systems and other preinstalled software during the warranty period of the hardware on which this software & operating system will be installed.

The bidder shall repair or replace the worn out or defective parts including any auxiliary component/equipment (active or passive devices) at their own cost including the cost of transport.

Scope & services covered under warranty: As part of the warranty services bidder shall provide:

- Comprehensive on-site warranty for 5 years from the date of Go-live for proposed solution
- Warranty and Support of all devices & tools will be considered only after successful Go-live date.
- Bidder shall also obtain the five years OEM premium support on all licensed software, OSS, any other third-party tool, hardware, and other equipment for providing OEM support during the warranty period.
- Wherever specific clause is not defined, by default support of all devices and tools should be premium one i.e., 4/8 hrs replacement and according to SLA
- Bidder shall provide the comprehensive manufacturer's warranty and support in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. covered by the bid. Bidder must warrant all hardware, equipment, accessories, spare parts, software etc. procured and implemented as per this bid against any manufacturing defects during the warranty period.
- Bidder shall provide the performance warranty in respect of performance of the installed hardware and software to meet the performance requirements and service levels in the bid.
- Bidder is responsible for sizing and procuring the necessary hardware and software licenses as per the performance requirements provided in the bid. During the warranty period bidder, shall replace or augment or procure higher-level new equipment or additional licenses at no additional cost in case the procured hardware or software is not adequate to meet the service levels.
- Mean Time between Failures (MTBF): If during contract period, any equipment has a hardware failure on four or more occasions in a period of less than three months, it shall be replaced by equivalent or higher-level new equipment by the bidder at no cost. For any delay in making available the replacement and repaired equipment’s for inspection, delivery of equipment’s or for commissioning of the systems or for acceptance tests / checks on per site basis, KSEB reserves the right to charge a penalty.
- During the warranty period bidder, shall maintain the systems and repair / replace at the installed site, at no charge, all defective components that are brought to the bidder notice.
- The bidder shall as far as possible repair/ replace the equipment at site.
- Bidder shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.
- Bidder shall ensure that the warranty complies with the agreed Technical Standards, Security Requirements, Operating Procedures, and Recovery Procedures.
- Any component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA).
- To provide warranty support effectively, OEM should have spare depo in India and will be asked to deliver spare as per SLA requirement.

EXTENDED WARRANTY:

The Bidder shall be liable to provide Extended Warranty for a period of two years on expiry of the 5 year warranty period, if KSEB desires so at that point of time. The extended warranty charges shall be quoted by the bidder in BoQ and the same shall be considered for price bid evaluation. The Extended Warranty would be on-site and comprehensive in nature with back-to-back support from the OEM. All support terms and conditions including performance security of Warranty shall be applicable for the Extended Warranty also.

3.2 Warrant Support

This shall be applicable as per RFP/Tender terms and conditions of End customer, unless otherwise specified.

Bidder shall be liable to provide Extended Warranty for a period of two years on expiry of the 5 year warranty period, if KSEB desires so at that point of time. The Extended Warranty would be on-site and comprehensive in nature with back-to-back support from the OEM. All support terms and conditions of Warranty shall be applicable for the Extended Warranty also.

3.3 Quality of Service, Service Level Agreement and penalty

This shall be applicable as per RFP/Tender terms and conditions of End customer, unless otherwise specified.

PURPOSE OF THIS AGREEMENT

The purpose of this SLA is to clearly define the levels of service to be provided by bidder to Purchaser for the duration of this contract or until this SLA has been amended. The benefits of this SLA are to:

a) Trigger a process that applies Purchaser and Bidder management attention to some aspect of performance only when that aspect drops below an agreed upon threshold, or target.
b) Makes explicit the performance related expectations on performance required by the Purchaser
c) Assist the Purchaser to control levels and performance of services provided by Bidder
d) This SLA is between Bidder and Purchaser.

DESCRIPTION OF SERVICES PROVIDED

Bidder shall provide services as defined in Section V - Scope of Work, in accordance with the definitions and conditions mentioned in the 'Terms and Conditions' of the RFP.

DURATION OF SLA

This Service level agreement would be valid for entire period of contract.

SERVICE LEVEL AGREEMENTS & TARGETS

This section is agreed to by Purchaser and Bidder as the key bidder performance indicator for this engagement. The following section reflects the measurements to be used to track and report systems performance on a regular basis. The targets shown in the following tables are for the period of contact or its revision whichever is later.

SOC DELIVERABLES & SLA

All the services delivered by the bidder should comply with the SLA mentioned in the table below. SLA will be reviewed on a monthly basis.

S No.	Service Area	Service Level

1.	SOC Monitoring & Log Analysis Services	• 24x7 event / log monitoring and correlation of the assets in Scope. • 24x7 monitoring of the Database Activity • 24x7 Monitoring & recording of Security events at all the ingress points. • Event alerts within 15 minutes of the event • Mitigation of security events / threats • Availability of relevant logs for last 3 months • Real time dashboard view • Weekly consolidated on every Monday • Monthly consolidated report by 5th of every month • Quarterly Reports • Standard / Exception reports
2.	Reports & Dashboard	• SOC should provide daily/ weekly/ monthly/ quarterly reports for each of the services in a timely manner. • Dashboard should give online view of all devices monitored with their status
3.	Others	• Bidder should provide up-to-date contacts and Escalation matrix. • The Bidder should provide all commercial tools / software's for SOC operations. • Availability of operation staff on 24/7 basis. • Rule-based Review of Firewalls

SOC Service / Man Power SLA

Sl. No.	Definition	Measurement Interval	SLA Target	Penalty terms
1.	Device uptime / Service availability	Monthly	>=99.90%	>=99.90% No Penalty
				>=98.00% and <99.90% 0.01% of total contract amount
				>=95.00%; < 98.00% 0.02% of total contract amount
				<95.00% 0.03% of total contract amount
2.	SOC application/ Software (SIEM/ SOAR/ UEBA/ NDR)	Monthly	>=99.90%	>=99.90% No penalty
				>=98.00%; <99.90% 0.01% of total contract amount
				>=95.00%; < 98.00% 0.02% of total contract amount

	availability			<95.00% 0.03% of total contract amount
3.	Manpower availability	Monthly	100% attendance as per defined in RFP document.	Resource replacement with equivalent skills and experience / with approval from department – no penalty.
				Level 1 resource absent: Equal cost of the resource charges quoted by the bidder per day on pro rata basis.
				Level 2/3 resource absent: Equal cost of the resource charges quoted by the bidder per day on pro rata basis.

Operational SLAs

SLA Definition	Metric	Severity	SLA	Measurement	Penalty
Incident Management	Incident Response Time	Level 4	15 minutes	Monthly	Rs. 10000/hour for every hour of delay
		Level 3	30 minutes	Monthly	Rs. 7000/hour for every hour of delay
		Level 2	3 hours	Monthly	Rs. 5000/hour for every hour of delay
		Level 1	6 hours	Monthly	Rs. 2000/hour for every hour of delay.
		Level 4	4 hours	Monthly	0.03% of total contract amount for every hour of delay
		Level 3	8 hours	Monthly	0.02% of total contract amount for every hour of delay
		Level 2	2 days	Monthly	0.01% of total contract amount for every day of delay.
		Level 1	4 days	Monthly	0.005% of total contract amount for every day of delay.
		Emergency	4 Hrs	Monthly	0.01% of total contract amount for every day of delay.

		Normal	2 days	Monthly	0.005% of total contract amount for every day of delay.
		Emergency	4 Hrs	Monthly	0.01% of total contract amount for every day of delay.
		Normal	2 days	Monthly	0.005% of total contract amount for every day of delay.
		Emergency	4 hrs	Monthly	0.02% of total contract amount for every hour of delay
		Normal	2 days	Monthly	0.01% of total contract amount for every day of delay
		Normal	Once in 3 Months	Quarterly	0.005% of total contract amount for every week of delay
		Normal	Once in a year	Yearly	0.01% of total contract amount for every month of delay
		Critical	-	Monthly	0.02% of total contract amount for every noticed incident
Log Management	Availability of online logs for 6 months	Normal	-	Monthly	0.02% of total contract amount for every noticed incident
	Availability of archived logs for 3 years	Normal	-	Monthly	0.02% of total contract amount for every noticed incident

Note:

1. The bidder is liable to provide post implementation support (during Warranty/Support period) as mentioned in the detailed descriptions in the Scope of Work in accordance with the concerned SLA Clauses listed above.
2. In case of Breach of SLA Clauses, penalty will be deducted from the quarterly payable man power charges or Performance Bank Guarantee submitted by the bidder.
3. The total deduction of penalty per month shall not exceed 0.2% of the total contract amount

4. The Agreement Authority shall have the right to make suitable amendments in the above SLA conditions based on the requirements from time to time, on mutually agreed terms and conditions

SERVICE LEVELS/ CRITICALITY

Typical SOC Service availability & duration of their requirements are tabulated below for reference.

SERVICE AVAILABILITY & CRITICALITY CHART

SERVICE	DURATION	CRITICALITY
SOC Service	24 HOURS	CRITICAL – 24X7
VENDOR MANAGEMENT SERVICES	8X6	MEDIUM
SOC ADMINISTRATION	24X7	CRITICAL
ANTIMALWARE & SECURITY ADMINISTRATION	24x7	CRITICAL
LOG MANAGEMENT	24X7	CRITICAL

Table 2: Severity Definition Chart

S/N	Support Category	Criteria
1.	Critical (Level 4)	The system is unable to be used for normal business activities. There is certainty of financial loss to PURCHASER.
2.	Urgent (Level 3)	There is a problem with part of the system, which impacts on Purchaser's decision making. No viable workaround is available. There is a likelihood of financial loss.
3.	High (Level 2)	The efficiency of users is being impacted, but has a viable workaround.
4.	Medium (Level 1)	A low impact problem that affects the efficiency of users but has a simple workaround.
5.	Low	A fault, which has no particular impact on processing of normal business activities.

MONITORING AND AUDITING

IT Team of Purchaser will review the performance of Supplier against the SLA parameters each month, or at any periodicity defined in the contract document. The review / audit report will form basis of any action relating to imposing penalty or breach of contract. Any such review / audit can be scheduled or unscheduled. The results will be shared with the Supplier as soon as possible. Purchaser reserves the right to appoint a third-party auditor to validate the SLA.

ESCALATION MATRIX FOR SOC OPERATIONS

1. L1 resource shall respond to an alert within 15 minutes.
2. L1 resource shall decide if the alert is false positive within 2 hours from occurrence of alert. In case it is false positive, L1 resource will close the alert and report to the L2/L3 Resource and KSEB team at End of Day.

3. If alert is true positive, L1 will report to L2/L3 resource for further analysis within 2 hours.
4. L2/L3 responds within 30 minutes of receiving the alert. Checks if it is critical alert. (decision about criticality of alert)
5. If it is critical alert, L2/L3 resource take immediate action against the alert and shall report to OEM backend team for further analysis and remedial action. The incident shall also be reported to the Data Centre Administrator within 2 hours from occurrence of the alert.
6. If it is not critical alert, L2 resource shall further analyze the incident and report the remediation plan to Data Centre Administrator within 3 hours from occurrence of the alert.
7. L2/L3 Resource shall report about all the alerts and incidents at the end of the day to Data Centre Administrator

3.4 Purpose of EOI

Detailed as above

3.5 Solution provider/BA need to implement and manage the Entire system and oversee the overall functioning of the organization's network infrastructure, including planning, design, implementation, and maintenance with failure free environment and without any downtime in operations of KSEBL. **SLA shall be applied as per KSEBL's tender document and corrigendum released, if any on back-to-back basis.**

3.6 Bidder may submit their response in the prescribed form of duly signed and stamped for techno commercial bid through Online mode vide email sent to https://railtel.eNivida.com , within the stipulated date and time, as mentioned in this EOI document. The Bidder shall accompany necessary documents as prescribed in the EoI.

3.7 Partners may note that this is a single stage, single Packet Bid Interested

3.8. Only those bids shall be opened, which have been submitted within the stipulated time as mentioned in this EOI document with required credentials and EMD.

3.9. <u>Technical Bid contains following</u>:-

Eligibility Criteria

S.N	Type	Description	Document Required
1	Existence / Origin	• The company must be registered in India. • The bidder should have been in the IT related services for the last 5 years.	• Incorporation/registration Certificate along with Memorandum & Articles of Association • Certificate consequent to change of name, if applicable
2	General	The company must have: I. Valid PAN card. II. Been registered with GST.	I. Copy of PAN Card. II. Copy of GST registration certificate.

3	General	The company should not be blacklisted by any Government institution/ Government PSU	Self-declaration, in case this is discovered to be otherwise, the bidder will be declared ineligible at any stage of the tender.
4	Turnover	Minimum Average Annual turnover of Rs. 7 Crores for any of the three financial years during the last five years ending 31st March 2024.	Audited Balance Sheet & CA Certificate .
6	Empanelment	Bidder must be empanelled/in process of empanelment with RailTel as Business associate.	i) Copy of Empanelment letter or application details for BA with RCIL OR ii) If the Bidder is not empanelled with RailTel and has applied for empanelment and issue of letter of empanelment is pending, then Bidder has to submit proof of payment of empanelment fee/EMD or acknowledgement letter of submission of empanelment documents.
7	Experience	The bidder should have experience in setting up On premises SOC/Managed SOC/Hybrid SOC for at least three projects each with a minimum order value of 25 lakhs	1. Proof of Work Order Client certificate for successful completion
8	General	The Bidder/OEM from a Country which shares a land border with India will be eligible only if they are registered with the competent authority as per Govt. of India Order, issued by Ministry of Finance vide No.F.No.6/18/2019-PPD dated 23/07/2020	Copy of document of registration with DPIIT, Govt. of India.
9	General	The bidder should submit valid letter from the OEMs in the specified format for all active components and associated software in the BoQ confirming the following: Authorization for bidder Confirm that the products quoted are not end of life products within next 5 years Undertake that the support including spares, patches etc. for the quoted products shall be available for next 7 years	OEM support letter to be submitted in the specified format
10	General	Bidder should have valid ISO 9001 and ISO 27001 Certifications.	Copy of certification from authorized certification body
11	General	The bidder should have technically qualified SOC professionals in its team as per the different skill levels defined in the RFP document	Certificate from HR head confirming compliance. CVs along with copies of Certifications also required for evaluation purpose.
12	General	The OEMs of SOC Solution quoted by the bidder should have presence in IT industry in the country for the past 4	Self-declaration by the OEM Proof for previously supplied

		years.	orders of the OEM
13	General	The OEM of SOC should have valid ISO 9001, ISO 14001, ISO 27001 certifications.	Copy of valid Certification documents
14	General	All products offered by the bidder should be available with the concerned OEMs as on date and should be publicly referenceable.	Self-declaration by the OEM
15	General	The OEMs of SOC Solution should have local Technical Assistance Centre (TAC) support in India	Details of Technical Assistance Centre
16	General	The OEM of SOC should have supplied and installed at least three On-premises SOC implementations containing SIEM and SOAR modules, each with a minimum order value of Rs. 10 Crore in Govt./PSU/Banks/Corporate Organisations in India. Out of the above projects, one project shall be with 25000 EPS and working satisfactorily for the past two years.	Copy of Work Orders and its satisfactory project completion Certificate

Note:

- If any of the Bids is found to be incomplete, it will be liable for rejection.
- Bidder is to fill the above annexure and indicate the page numbers of the supporting document in the Proof while submitting response to the eligibility criteria.
- Relevant portions, in the documents submitted in pursuance of eligibility criterion mentioned above, shall be highlighted.
- Bidders must ensure that all required documents have been uploaded/submitted along with the bid to justify his/her eligibility.
- Bidder should be an authorized partner/seller of all the proposed solutions/products and should provide Manufacturer Authorization in the template provided in the RFP.

Price quote in the attached format (Annexure 8).

i. Compliance of OEM/Vendors with their MAF's and all mandatory documents asked by KSEBL from OEM/Vendors.
ii. Unconditional Acceptance of contents the Tender document of KSEBL and any Other/General Document of KSEBL Tender RFP along with corrigendum and addendum.
iii. Acceptance Letter of EoI
iv. Annexure Formats as mentioned in this EOI.
v. All documents mentioned in checklist and annexures of this EOI
vi. The BA agrees to undertake Warranty, Maintenance contract for a minimum **period as per KSEBL.** Undertaking in this regard is to be submitted along with the technical bid.
vii. **Contract Period Undertaking** – As per pertinent tender floated by KSEBL Request for Proposal (RFP) for Setting up Security Operations Centre (SOC) as part of KSEBL Data Centre under RDSS Scheme by Kerala state electricity board limited (KSEBL contract period shall be initially for a period of sixty-four months (4 months project completion and 60 months onsite warranty period) from the date of commencement of installation, which includes four months implementation period and sixty months for onsite warranty period.

viii. The bid should be duly signed and submitted by Authorized Signatory. The bidder has to submit notarized of non-judicial stamp paper of appropriate value Power of Attorney having authorized signatory's nomination along with board resolution in favour of power of attorney.

ix. The bidder has to mandatorily submit notarized Annexure-11 on non-judicial stamp paper of requisite value of Rs. 200, else bid shall be summarily rejected.

3.10. Prospective bidder's bid evaluation will be done based on above mentioned documents. Bids of those Bidders who submit Technical Documents without OEM/Vendor Name, Make and Model, technical Compliance, and unconditional acceptance of the KSEBL hard Copies, will be summarily rejected.

3.11. further complying technical requirement with supporting documents of OEM/Vendor MAF, datasheets, BOQ/BOM (wherever applicable) may be treated as technically qualified partner for Stage-1.

3.12. Bidders selected as per Para 3.11 above will be treated as eligible for financial bid opening.

3.13 <u>Financial Bid:</u>

The Annexure 8 of for financial quote to be submitted for evaluation

3.14 Selection of Bidder: as per outcome of Clause 3.9 above

The bidder will be selected on the **lowest quote (L-1)** basis for complete 'Scope of Work' as mentioned in the EOI document and Physical documents of technical specifications of CIAL, subject to the respective overall bid is in compliance to the requirements of this EOI. The partner selected will be termed as 'Commercially Suitable Partner (hereafter referred to as 'CSP')'. It is ascertained, that the final selection of CSP will be on the L-1 basis only. Further, RailTel reserves the right to have negotiation with the CSP if required. However, RailTel reserves the right to select any Bidder irrespective of the ranking in the Bid list without assigning any reasons.

3.15 The partner selected through this EOI shall be deemed to be responsible for delivering of complete 'Scope of Work' as mentioned in the KSEBL tender document and subsequent corrigendum. However, RailTel at its discern, may take- up a certain portion / percentage of 'Scope of Work' by communicating to the CSP at any point of time during the engagement period. (The day at which 'CSP' is declared, will mark the start of engagement period. The period will be valid till final outcome of this tender as announced by KSEBL. In case, RailTel comes out to be winner of the KSEBL tender, then the engagement period will get auto-extended to the period RailTel serves KSEBL for the concerned tender, unless terminated earlier by RailTel as per terms and conditions mentioned in this EoI document). In this scenario, commercial engagement with the CSP will be for that portion / percentage only, which has not been taken by RailTel. Accordingly, resultant value of work will be derived on the basis of negotiated (in case) commercial bid of the CSP.

3.16 RailTel on the basis of inputs / factors available to it from various resources, past experiences of its ICT projects and on the basis of negotiated (in case) commercial bid of the CSP, will endeavour to place best techno-commercial bid in response to the pertinent KSEBL tender. Further relationship with CSP will be based on the outcome pertinent KSEBL tender.

4 General Requirements and Eligibility Criteria for Bidders

4.1. The interested bidder should be an Empaneled Partner/ In process of Empanelment with RailTel on the last date of bid submission of EOI & has to provide relevant documents to qualify as per relevant Clause of this EOI.

4.2. The interested bidder should submit Earnest Money Deposit (EMD) if applicable, in the format as mentioned in this EOI document along with the bid.

4.3. The interested bidder should be in compliance to insertion of Rule 144(xi) in the GFR, 2017 vide office OM no. 6/18/2019-PPD dated 23-July-2020 issued by Ministry of Finance, Government of India, including revisions.

4.4. The interested bidder should submit an undertaking for maintaining of 'Local Content Compliance' and shall submit a certificate mentioning the 'Local Content Percentage' duly signed and stamped by statutory auditor or cost auditor or authorized signatory of the interested partner. This will not be a binding clause in cases where end customer has not asked Local Content Clause/Make in India Clause in their Current RFP.

4.5 **The bidder has to mandatorily provide all Annexures of this EoI and corrigendum(s) thereof.**

4.6. The interested bidder should not be backlisted by any State / Central Government Ministry / Department / Corporation / Autonomous Body on the last date of submission of EOI.

4.7. There should not be any ongoing or past, arbitration case(s) between 'RailTel or Organizations under Indian Railways' and 'Interested Bidder' on the last date of submission of EOI.

4.8. The interested bidder shall not have a conflict of interest with one or more bidding parties. Participation of interested bidder(s) with a conflict-of-interest situation will result in the disqualification of all bids in which it is involved. A bidder may be in a conflict of interest with one or more parties if including but not limited to:

a. Have controlling shareholders as his/her family members viz. spouse, son, daughter, father, mother or brother etc. in common or;

b. Have a relationship with each other directly or through common third parties that puts them in a position to have access to information about or influence on the bid of another interested partner.

4.9. The interested bidder should not be seeking/extending/exploring similar arrangements /engagements with any other organization except RailTel, for the KSEBL tender.

4.10. The interested partner should have a valid Goods and Service Tax Identification Number (GSTIN), as on the last date of submission of EOI.

4.11. In addition to above clauses, bid of interested bidder should be in compliance to terms and conditions and technical requirements of the pertinent KSEBL tender as referred above.

Note: The interested bidder should submit duly signed and stamped EOI cover letter as per the format mentioned at Annexure-02 of this EOI document, as unconditional submission of meeting the clauses mentioned above, from Clause **4.1. to Clause 4.11**

5 Resources to be Deployed

i. The bidder shall carry out all necessary activities during execution of the work and all along thereafter as may be necessary for proper fulfilling of the obligations under the contract.

ii. Adequate training, required to carry out the activities mentioned in the scope of work above, shall be provided by Bidder to all deployed resources.

iii. Boarding, lodging, transportation, and all other expenses of the deployed resources are to be borne by bidder,

iv. The Authority shall be at liberty to object to and require the bidder to remove from the works any person who in his opinion misconducts himself or is incompetent or negligent in the performance of his duties or whose employment is otherwise considered by the Authority to be undesirable. Such person shall not be employed again at works site without the written permission of the Authority and the persons so removed shall be replaced with in a week's time by competent substitutes.

v. The Authority has agreement with the bidder only, it is the responsibility of the bidder to ensure all due diligence is carried out for background verification of resources deployed. And in any case, the Authority will not be responsible for the violation of due diligence or offence committed by the bidder or any of its resources.

6 Proposal Preparation and Submission Cost

6.1. The interested partner is responsible for all costs incurred in connection with participation in this EOI process, including, but not limited to, cost incurred in conduct of informative and other diligence activities, participation in meetings/discussions/presentations, preparation of proposal, in providing any additional information required by RailTel to facilitate the evaluation process or all such activities related to the bid process. RailTel will i n no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process. This EOI document does not commit to award a contract or to engage in negotiations.

7 Amendment to EOI Document

7.1. At any time prior to the deadline for submission of bids, RailTel, may, for any reason can modify the EOI document by an amendment. All the amendments made in the document would be informed by displaying on RailTel's (www.railtelindia.com) website only. The interested bidders are advised to visit the RailTel website on regular basis for checking necessary updates. RailTel also reserves the rights to amend the dates mentioned in this EOI for bid process. RailTel may, at its discretion, extend the last date for receipt of EoI response Individual advices in this connection is not treated as mandatory.

8 Bid, PBG and SD Validity Period

8.1. Bid of Interested partners shall remain valid for the period of 210 days from the date of opening the price bid.

8.2. RailTel may request for an extension of the period of validity. The validity of the 'EMD', should also be suitably extended if called upon to do so by RailTel. The request and the responses thereto shall be made in writing through e-mail communication only. Further, whenever the bid validity extension is submitted by the interested partner, it should be ensured by interested partner that their PBG (Performance bank Guarantee) and Security Deposit (SD) related to the empanelment should have minimum validity of 120 days from the last date of extended completion period.

9 Right to Terminate the Process

9.1. RailTel may terminate the EOI process at any time without assigning any reason. RailTel makes no commitments, express or implied, that this process will result in a business transaction with anyone. This EOI does not constitute an offer by RailTel. The interested bidder's participation in this process may result in RailTel selecting the CSP to engage in further discussions and negotiations toward execution of a contract. The commencement of such negotiations does not, however, signify a commitment by RailTel to execute a contract or to continue negotiations. RailTel may terminate negotiations at any time without assigning any reason.

10 Language of Bid

10.1. The bid prepared by the interested partner and all correspondence and documents relating to the bids exchanged by the bidder and RailTel, shall be written in English Language, provided that any printed literature furnished by the Bidder in another language shall be accompanied by an English translation in which case, for purposes of interpretation of the bid, the English translation shall govern. If any supporting documents submitted are in any language other than English, translation of the same in English language is to be duly attested by the Authorised Signatory of the interested partner.

11 Submission of Bid

11.1. The Bidder should take into account any Corrigendum to this EOI document that may have been published before submitting their EOI response. The bid is to be submitted in the mode as mentioned in this EOI document. EOI response submitted in any other mode will not be entertained.

11.2. Bidders in their own interest are advised to submit the EOI response well in time before the last date and hence to avoid any inconvenience at the last moment.

11.3. An Organization / Bidder can submit only 'One EOI Response'. Submission of multiple EOI Response by bidder(s) may lead to rejection of all of its bid.

12 Rights to Accept / Reject any or all EoI Response

12.1. RailTel reserves the right to accept or reject any EOI Response, and to annul the bidding process and reject all Bids at any time prior to award of the Contract, without thereby incurring any liability to the affected interested bidder(s), or any obligation to inform the affected Bidders of the ground for RailTel's action.

13 Payment Terms

Back-to-back basis as per KSEBL RFP No. CEIT/ITCSD/16/2024-25 dated 30.12.2024 and as per Payment terms below:

13.1 Terms of Payment:

Activity	Payment Schedule	Milestones
Milestone-I Supply of all hardware and software components with accessories required for setting up On-Premises SOC solution at the Data Centre as per BoQ	60% of the total project cost except man power charges	Supply of items by the bidder and then purchaser confirmation that materials are received as per the Work Order conditions
Milestone-II Installation, configuration, system integration, testing, and commissioning all hardware and software components with accessories for setting up on-premises SOC at the Data Centre	30% of the total project cost except man power charges	On purchaser approval that installation, configuration, system integration, testing and commissioning of hardware and software components at Data Centre and DR Centre have been successfully completed
Milestone-III		

• Acceptance testing and go-live • Training for KSEB employees	10% of the total project cost except man power charges	On purchaser approval that the SOC services are functioning properly as per the RFP requirements and training has been provided
Man Power charges – Onsite L1/L2/L3 Resources	Payment will be made on quarterly basis and pro-rata basis after completion of each quarter	On purchaser approval that all duties of onsite resource has been carried out satisfactorily

13.2 Annual Maintenance Charges as per RFP if applicable.

13.3. Documents list required (as applicable) at the time of payment/invoice submission by selected bidder shall be: -

- Valid Tax Invoice (in Triplicate, where supply is Involved)
- Delivery Challan and e way bill
- Factory Test Report
- QA& COQ inspection certificate duly signed by OEM.
- Inspection Certificate or Approval of waiver for the same as applicable.
- Packaging List
- Purchaser's Inspection certificate
- Consignee receipt
- Warranty certificate of OEM
- Insurance certificate
- A certificate duly signed by the firm certifying that equipment/ materials being delivered are new and conform to technical specification.
- A certificate duly signed by the firm certifying that the equipment/ materials being delivered are complete in all respect for the concerned items for which the payment is being released.

All payments shall be released after sign-off by the CIAL.

14 Performance Bank Guarantee

Bidder has to furnish bank guarantee as performance security for the supplied equipments and services

A Performance Bank Guarantee 10% of the accepted value of work (without limit) shall be furnished by the Successful Bidder within 15 days of receipt of LOA. The said bank guarantee shall be initially valid up to ninety (90) days. No interest shall be paid by the Purchaser on the Bid Security deposited by the Bidder

14.1. RailTel shall also be entitled to make recoveries from the CSP's bills, PBG or from any other amount due to him, the equivalent value of any payment made to him due to inadvertence, error, collusion, misconstruction or misstatement.

14.2. If the service period / contract value undergo variation PBG also shall be varied accordingly

14.3. During the contract period, RailTel may issue Purchase Order(s) for the additional services ordered by CIAL (in case) to RailTel. In such scenario(s) also, Clause No. 13.1. to Clause No. 13.4. are to be followed by the CSP.

14.4. In case the CIAL has sought PBG of the contract in the terms of Indemnity Bond from RailTel, the selected bidder has to provide the equivalent value PBG from scheduled Bank to RailTel. No Indemnity Bond from Selected Bidder will be accepted in lieu of PBG from Scheduled Bank.

14.7. In case CIAL has sought any other types of PBG, at present or in future or else Integrity Pact PBG (presently or in future), same remain applicable on selected Bidder. The Said PBG will be issued by Selected Bidder from Scheduled Bank favouring RailTel Corporation of India Limited. No Indemnity Bond in lieu of such PBG will be accepted by RailTel.

14.8 Integrity pact in the format if any, as per KSEBL to be provided by the Bidder.

Note

1. All PBG upto Rs 5,00,000 /- will be accepted only through Bank transfer only.
2. As per RBI guidelines BG above Rs 50,000 /- should be signed by two Bank officials.
3. PBG should be from scheduled commercial Bank (either private or PSU) but not from any cooperative Bank or NBFC.
4. It is to be ensured that BG issuing Bank must be SFMS enabled. Under SFMS system, a separate advice of the BG (via SFMS IFN 760COV) to be sent to the advising Bank (RailTel) through SFMS by the issuing Bank (Applicant). Similar process to be followed for Bank Guarantee amendment also and separate advice (via SFMS IFN 767COV) is sent to the advising bank (RailTel).
5. The minimum gap between BG expiry date and BG claim date should be 12 months.

The Bank guarantee (BG) if required, should be extended by the bidder at least 90 days before its expiry; failure to do so will result in the encashment of the BG.

15 Details of Commercial Bid / Financial Bid

15.1. Partner should submit commercial bid strictly as per the format mentioned by CIAL or in subsequent corrigendum's (if any).

15.2. The commercial bid should clearly bring out the cost of the services with detailed break- up of taxes.

15.3. The rates mentioned in the commercial bid of the CSP will form basis of commercial transaction between RailTel and bidder.

15.4. The quantity of 'Line Items' may vary at the time of placing of Purchase Order or during the Contract Period, as communicated by CIAL (in case) to RailTel. In such scenarios, the 'Per Unit' cost will be considered to arrive on contractual amount between RailTel and CSP.

15.5. It is also possible that CIAL may surrender / increase, some or all of the quantities of service items ordered to RailTel during the contract period and accordingly the contractual amount between RailTel and CSP shall be considered, at sole discern of RailTel.

15.6. It is also possible that during the contract period, KSEBL may raise Purchase Order to RailTel for the line items (and respective quantities) which are not mentioned in the pertinent tender of KSEBL. In such scenario, RailTel at its sole discretion, may extend the scope of the contract with CSP by placing order to KSEBL, on back-to- back basis.

15.7. In addition to the Payment Terms, all other Contractual Terms will also be on 'back- to-back' basis between RailTel and CSP, as mentioned in the pertinent KSEBL tender. MAF (Manufacturer's Authorization Form) in the name of RailTel and another MAF in Bidders Name (separately with reference to this EOI) from the OEMs, whose product is mentioned in commercial bid format, should also be ensured by the partner. The MAF format and required content should be in-line with KSEBL tender, if specifically asked by KSEBL in a particular format.

16 Duration of the Contract Period

16.1. The contract duration shall be same as of KSEBL contract duration with RailTel until otherwise terminated earlier. Indicative contract duration is as per KSEBL RFP, unless otherwise terminated/modified, as mentioned in this EOI document and subject to award of contract to RailTel. The contract duration can be renewed /extended by RailTel at its discern, in case KSEBL extends / RailTel renews services with RailTel by virtue of extending / renewing / new issuance of one or more Purchase Order(s) placed by KSEBL to RailTel.

17 Restrictions on 'Transfer of Agreement'

17.1. The CSP shall not assign or transfer its right in any manner whatsoever under the contract / agreement to a third party or enter into any agreement for sub- contracting and/or partnership relating to any subject matter of the contract / agreement to any third party either in whole or in any part i.e., no sub-contracting / partnership / third party interest shall be created.

18 Suspension, Revocation or Termination of Contract / Agreement

18.1. RailTel reserves the right to suspend the operation of the contract / agreement, at any time, due to change in its own license conditions or upon directions from the competent government authorities, in such a situation, RailTel shall not be responsible for any damage or loss caused or arisen out of aforesaid action. Further, the suspension of the contract / agreement will not be a cause or ground for extension of the period of the contract / agreement and suspension period will be taken as period spent. During this period, no charges for the use of the facility of the CSP shall be payable by RailTel.

18.2. RailTel may, without prejudice to any other remedy available for the breach of any conditions of agreements, by a written notice as per GCCA of contract or as per CIAL tender condition whichever is issued to the CSP.

RailTel shall terminate/or suspend the contract /agreement under any of the following circumstances:

a) The CSP failing to perform any obligation(s) under the contract / agreement.

b) The CSP failing to rectify, within the time prescribed, any defect as may be pointed out by RailTel.

c) Non adherence to Service Level Agreements (SLA) which RailTel has committed to CIAL.

d) The CSP going into liquidation or ordered to be wound up by competent authority

e) If the CSP is wound up or goes into liquidation, it shall immediately (and not more three days) inform about occurrence of such event to RailTel in writing. In such case, the written notice can be modified by RailTel as deemed fit under the circumstances. RailTel may either decide to issue a termination notice or to continue the agreement by suitably modifying the conditions, as deemed fit. It shall be the responsibility of the CSP to maintain the agreed Quality of Service, even during the period when the notice for surrender/termination of contract / agreement is pending and if the Quality of Performance of Solution is not maintained, during the said notice period, it shall be treated as material breach liable for termination at risk and consequent of which CSP's PG related to contract / agreement along with PG related to the Empanelment Agreement with RailTel shall be forfeited, without any further notice.

f) Breach of non-fulfilment of contract / agreement conditions may come to the notice of RailTel through complaints or as a result of the regular monitoring. Wherever considered appropriate RailTel may conduct an inquiry either Suo- moto or on complaint to determine whether there has been any breach in compliance of the terms and conditions of the agreement by the successful bidder or not. The CSP shall extend all reasonable facilities and shall endeavour to remove the hindrance of every type upon such inquiry. In case of default by the CSP in successful implementation and thereafter maintenance of services / works as per the conditions mentioned in this EOI document, the PG(s) of CSP available with RailTel can be forfeited.

19 Dispute Settlement

19.1 In case of any dispute concerning the contract / agreement, both the CSP and RailTel shall try to settle the same amicably through mutual discussion / negotiations. Any unsettled dispute shall be settled in terms of Indian Act of Arbitration and Conciliation 1996 or any amendment thereof. Place of Arbitration shall be New Delhi.

19.2 The arbitral tribunal shall consist of the Sole Arbitrator. The arbitrator shall be appointed by the Chairman & Managing Director (CMD) of RailTel Corporation of India Ltd.

19.3 All arbitration proceedings shall be conducted in English.

20 Governing Laws

20.1. The contract shall be interpreted in accordance with the laws of India. The courts at New Delhi shall have exclusive jurisdiction to entertain and try all matters arising out of this contract.

21 Statutory Compliance

21.1. During the tenure of this Contract nothing shall be done by CSP in contravention of any law, act and/ or rules/regulations, there under or any amendment thereof and shall keep RailTel indemnified in this regard.

22.2. The Bidder shall comply and ensure strict compliance by his/her employees and agents of all applicable Central, State, Municipal and Local laws and Regulations and undertake to indemnify RailTel, from and against all levies, damages, penalties and payments whatsoever as may be imposed by reason of any breach or violation of any law, rule, including but not limited to the claims against RailTel or its Customer under Employees Compensation Act, 1923,The Employees Provident Fund and Miscellaneous Provisions Act, 1952, The Contract Labour (Abolition and Regulation) Act 1970, Factories Act, 1948, Minimum Wages Act and

Regulations, Shop and Establishment Act and Labour Laws which would be amended/modified or any new act if it comes in force whatsoever, and all actions claim and demand arising therefrom and/or related thereto.

22 Intellectual Property Rights

22.1. Each party i.e., RailTel and CSP, acknowledges and agree that the other party retains exclusive ownership and rights in its trade secrets, inventions, copyrights, and other intellectual property and any hardware provided by such party in relation to this contract / agreement.

22.2. Neither party shall remove or misuse or modify any copyright, trade mark or any other proprietary right of the other party which is known by virtue of this EoI and subsequent contract in any circumstances

23 Severability

23.1. In the event any provision of this EOI and subsequent contract with CSP is held invalid or not enforceable by a court of competent jurisdiction, such provision shall be considered separately and such determination shall not invalidate the other provisions of the contract and Annexure/s which will be in full force and effect.

24 Force Majeure

24.1. If during the contract period, the performance in whole or in part, by other party, of any obligation under this is prevented or delayed by reason beyond the control of the parties including war, hostility, acts of the public enemy, civic commotion, sabotage, Act of State or direction from Statutory Authority, explosion, epidemic, quarantine restriction, strikes and lockouts (as are not limited to the establishments and facilities of the parties), fire, floods, earthquakes, natural calamities or any act of GOD(hereinafter referred to as EVENT) , provided notice of happenings of any such event is given by the affected party to the other, within twenty one (21) days from the date of occurrence thereof, neither party shall have any such claims for damages against the other, in respect of such non- performance or delay in performance. Provided service under this contract shall be resumed as soon as practicable, after such EVENT comes to an end or ceases to exist.

24.2. In the event of a Force Majeure, the affected party will be excused from performance during the existence of the force Majeure. When a Force Majeure occurs, the affected party after notifying the other party will attempt to mitigate the effect of the Force Majeure as much as possible. If such delaying cause shall continue for more than sixty (60) days from the date of the notice stated above, the party injured by the inability of the other to perform shall have the right, upon written notice of thirty (30) days to the other party, to terminate this contract. Neither party shall be liable for any breach, claims, and damages against the other, in respect of non-performance or delay in performance as a result of Force Majeure leading to such termination.

25 Indemnity

25.1. The CSP agrees to indemnify and hold harmless RailTel, its officers, employees and agents (each an “Indemnified Party”) promptly upon demand at any time and from time to time, from and against any and all losses, claims, damages, liabilities, costs (including reasonable attorney’s fees and disbursements) and expenses (collectively, “Losses”) to which the

Indemnified party may become subject, in so far as such losses directly arise out of, in any way relate to, or result from:

a) Any mis -statement or any breach of any representation or warranty made by CSP

b) The failure by the CSP to fulfil any covenant or condition contained in this contract by any employee or agent of the Bidder. Against all losses or damages arising from claims by third Parties that any Deliverables (or the access, use or other rights thereto), created by CSP pursuant to this contract, or any equipment, software, information, methods of operation or other intellectual property created by CSP pursuant to this contract, or the SLAs (i) infringes a copyright, trade mark, trade design enforceable in India, (ii) infringes a patent issues in India, or (iii) constitutes misappropriation or unlawful disclosure or used of another Party's trade secrets under the laws of India (collectively, "Infringement Claims"); or

c) Any compensation / claim or proceeding by any third party against RailTel arising out of any act, deed or omission by the CSP

d) Claim filed by a workman or employee engaged by the CSP for carrying out work related to this agreement. For the avoidance of doubt, indemnification of Losses pursuant to this section shall be made in an amount or amounts sufficient to restore each of the Indemnified Party to the financial position it would have been in had the losses not occurred.

25.2. Any payment made under this contract to an indemnity or claim for breach of any provision of this contract shall include applicable taxes.

26 Limitation of Liability towards RailTel

26.1. The CSP (SI/BA) liability under the contract shall be determined as per the Law in force for the time being. The CSP shall be liable to RailTel for loss or damage occurred or caused or likely to occur on account of any act of omission on the part of the CSP and its employees (direct or indirect), including loss caused to RailTel on account of defect in goods or deficiency in services on the part of CSP or his agents or any person / persons claiming through under said CSP, However, such liability of the CSP shall not exceed the total value of the contract.

26.2. This limit shall not apply to damages for bodily injury (including death) and damage to real estate property and tangible personal property for which the CSP is legally liable.

27 Confidentiality cum Non-disclosure

27.1. The Receiving Party agrees that it will not disclose to third party/parties any information belonging to the Disclosing Party which is provided to it by the Disclosing Party before, during and after the execution of this contract. All such information belonging to the Disclosing Party and provided to the Receiving Party shall be considered Confidential Information. Confidential Information includes prices, quotations, negotiated issues made before the execution of the contract, design and other related information. All information provided by Disclosing Party to the Receiving Party shall be considered confidential even if it is not conspicuously marked as confidential.

27.2. Notwithstanding the foregoing, neither Party shall have any obligations regarding non- use or non-disclosure of any confidential information which:

27.2.1. Is already known to the receiving Party at the time of disclosure:

27.2.2. Is or becomes part of the public domain without violation of the terms hereof;

27.2.3. Is shown by conclusive documentary evidence to have been developed independently by the Receiving Party without violation of the terms hereof:

27.2.4. Is received from a third party without similar restrictions and without violation of this or a similar contract.

27.3 The terms and conditions of this contract, and all annexes, attachments and amendments hereto and thereto shall be considered Confidential Information. No news release, public announcement, advertisement or publicity concerning this contract and/or its contents herein shall be made by either Party without the prior written approval of the other Party unless such disclosure or public announcement is required by applicable law.

27.4 Notwithstanding the above, information may be transmitted to governmental, judicial, regulatory authorities, if so, required by law. In such an event, the Disclosing Party shall inform the other party about the same within 30 (thirty) Days of such disclosure.

27.5 This Confidentiality and Non- Disclosure clause shall survive even after the expiry or termination of this contract.

28 Assignment

28.1 Neither this contract nor any of the rights, interests or obligations under this contract shall be assigned, in whole or in part, by operation of law or otherwise by any of the Parties without the prior written consent of each of the other Parties. Any purported assignment without such consent shall be void. Subject to the preceding sentences, this contract will be binding upon, inure to the benefit of, and be enforceable by, the Parties and their respective successors and assigns.

29 Insurance

The CSP shall agree to take insurances to cover all the elements of the project under this EOI including but not limited to Manpower, Hardware, Software and Services etc. as per CIAL tender specified terms.

30 Exit Management

30.1 Exit Management Purpose

30.1.1 This clause sets out the provision, which will apply during Exit Management period. The parties shall ensure that their respective associated entities carry out their respective obligation set out in this Exit Management Clause.

30.1.2 The exit management period starts, in case of expiry of contract, at least 03 months prior to the date when the contract comes to an end or in case of termination contract, on the date when the notice of termination is sent to the CSP. The exit management period ends on the date agreed upon by RailTel or Three (03) months after the beginning of the exit management period, whichever is earlier.

30.2 Confidential Information, Security and Data:

CSP will promptly, on the commencement of the exit management period, supply to RailTel or its nominated agencies the following (if asked by RailTel in writing):

30.2.1 Information relating to the current services rendered and performance data relating to the performance of the services; documentation relating to the project, project's customized source code (if any); any other data and confidential information created as part of or is related to this contract;

30.2.2 All other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable RailTel and its nominated agencies, or its replacing vendor to carry out due diligence in order to transition the provision of the services to RailTel or its nominated agencies, or its replacing vendor (as the case may be).

30.3 Employees : Promptly on reasonable request at any time during the exit management period, the CSP shall, subject to applicable laws, restraints and regulations (including in particular those relating to privacy) provide RailTel a list of all employees (with job titles and communication address), dedicated to providing the services at the commencement of the exit management period; To the extent that any Transfer Regulation does not apply to any employee of the CSP, RailTel or the replacing vendor may make an offer of contract for services to such employees of the CSP and the CSP shall not enforce or impose any contractual provision that would prevent any such employee from being hired by RailTel or any replacing vendor.

30.4 Rights of Access to Information: Besides during the contract period, during the exit management period also, if asked by RailTel in writing, the CSP shall be obliged to provide an access of information to RailTel and / or any Replacing Vendor in order to make an inventory of the Assets (including hard software / active / passive), documentations, manuals, catalogues, archive data, Live data, policy documents or any other related material.

Note: RailTel at its sole discern may not enforce any or all clauses / sub-clauses under the

'Exit Management' clause due to administrative convenience or any other reasons as deemed fit.

31 Waiver

31.1. Except as otherwise specifically provided in the contract, no failure to exercise or delay in exercising, any right, power or privilege set forth in the contract will operate as a waiver of any right, power or privilege.

32 Changes in Contract Agreement

No modification of the terms and conditions of the Contract Agreement shall be made except by written amendments signed by the both CSP and RailTel.

ANNEXURES

32.1 ANNEXURE 1

FORMAT FOR PROJECT EXPERIENCE CITATIONS

Sl. No.	Item	Bidder's Response
1	Name of Bidder entity	
2	Assignment Name	
3	Name & Address of Client	
4	Approximate Value of the Contract (in INR Crores)	
5	Duration of Assignment (months)	
6	Start Date (month/year)	
7	Completion Date (month/year)	
8	Narrative description of the project	
9	Details of Work that defines the scope relevant to the	
10	Documentary Evidence attached	

Signature of Bidder ……..
Name: ……
Designation …….. Seal of BA Organization
Place: ……
Date: ……..

32.2 ANNEXURE 2

EOI COVER LETTER

(On Organization Letter Head)

EOI Ref No: Date:

To,

The Joint General Manager (ERS)

RailTel Corporation India Limited,

Kerala Territory Office,

1st Floor, Eastern Entry Tower

Ernakulam South Railway Station

Ernakulam – 682016

Ref. No.: Ref. No.: CEIT/ITCSD/16/2024-25 dated 30.12.2024; latest amendment/ Corrigendum / clarifications.
Floated on etender Kerala Portal (https://etenders.kerala.gov.in/)

Dear Sir/ Madam

1. I, the undersigned, on behalf of M/s ....., having carefully examined the referred EOI offer to participate in the same, in full conformity with the said EOI and all the terms and conditions thereof, including corrigendum issued till last date of submission of EOI. It is also undertaken and submitted that we are in abidance of Clause 4 of EOI.
2. I agree to abide by this Proposal, consisting of this letter, our Pre-qualification, Technical and Commercial Proposals, for a period of 210 days from the date fixed for submission of Proposals as stipulated in the EOI and modifications resulting from contract negotiations, and it shall remain binding upon us and maybe accepted by you at any time before the expiration of that period.
3. I acknowledge that the Authority will be relying on the information provided in the Proposal and the documents accompanying the Proposal for selection of the Commercially Suitable Partner (CSP) for there for said Service, and we certify that all information provided therein is true and correct; nothing has been omitted which renders such information misleading; and all documents accompanying the Proposal are true copies of their respective originals.
4. I undertake, if our Bid is accepted, to commence our services as per scope of work as specified in the contract document.
5. Until a formal Purchase Order or Contract is prepared and executed, this Bid and supplement / additional documents submitted (if any), together with your written acceptance thereof in your notification of award shall constitute a binding contract between us.

6. I hereby undertake and give unconditional acceptance for compliance of all terms & conditions **Ref. No.: CEIT/ITCSD/16/2024-25 dated 30.12.2024**; latest amendment/ Corrigendum / clarifications. Floated on etender Kerala Portal (https://etenders.kerala.gov.in/) against this EOI based customer's requirement.
7. I hereby undertake that there will be no deviation from the Terms and Conditions of EOI and **Ref. No.: CEIT/ITCSD/16/2024-25 dated 30.12.2024**; latest amendment/ Corrigendum / clarifications. Floated on etender Kerala Portal (https://etenders.kerala.gov.in/)

Signature of Bidder …….
Name: ……
Designation ……..... Seal of BA Organization
Place: ……
Date: ……..

32.3 ANNEXURE 3

(Local Content Compliance)

EOI Ref. No: Date:

To,

The Joint General Manager (ERS)

RailTel Corporation India Limited,

Kerala Territory Office,

1st Floor, Eastern Entry Tower

Ernakulam South Railway Station

Ernakulam – 682016

Ref. No.: CEIT/ITCSD/16/2024-25 dated 30.12.2024; latest amendment/ Corrigendum / clarifications. **Floated on etender Kerala Portal (https://etenders.kerala.gov.in/)**

Dear Sir / Madam

I, the undersigned, on behalf of M/s ....., hereby submits that our technical solution for the 'Scope of Work' mentioned under the EoI document is in compliance of local content requirement and makes us equivalent to 'Class-I local supplier' / 'Class-II local supplier' (mention whichever is applicable) for the EoI under reference, as defined under the order No. P-45021/2/2017-PP(BE-II) dt. 04-June-2020 issued by Ministry of Commerce and Industry, Govt. of India.

I hereby certify that M/s .....fulfils all requirements in this regard and is eligible to be considered and for the submitted bid Local Content Percentage is % (write in figures as well as in words).

I hereby acknowledge that in the event of acceptance of bid on above certificate and if the certificate is found to be false at any stage, the false certificate would be a ground for immediate termination of contract and further legal action in accordance with the Law, including but not limited to the encashment of Bank Guarantee related to Empanelment and Performance Bank Guarantee (PBG) and Security deposit (SD), as available with RailTel, related to this EoI. Signature of Authorized Signatory.

Signature of Bidder …….
Name: ……
Designation ……. Seal of BA Organization
Place: ……
Date: ……..

32.4 ANNEXURE 4

CHECKLIST OF DOCUMENTS FOR BID SUBMISSION

KSEBL Tender **Ref. No.: CEIT/ITCSD/16/2024-25 dated 30.12.2024**; latest amendment/ Corrigendum / clarifications. Floated on etender Kerala Portal (https://etenders.kerala.gov.in/)

Sl. No.	Document
1	EOI Cover Letter (Annexure-02)
2	Technical compliance sheet
3	Price bid
4	Local Content Compliance & Percentage Amount (annexure-03)
5	**TECHNICAL BID COVER LETTER**
6	**COMMERCIAL BID COVER LETTER**
7	EMD as per EOI document
8	This EOI copy duly Signed and Stamped by the Authorized Signatory Of Bidder
9	All Annexure/ Appendices/Formats/ Declarations as **per KSEBL Ref. No.: CEIT/ITCSD/16/2024-25 dated 30.12.2024**; addressing to RailTel.
10	Compliance of eligibility criteria related documents as per Clause 3
11	Any relevant document found suitable by bidder

Note:

1. The technical bid should have a 'Index' at the starting and all pages of bid should be serially numbered and should be traceable as per the 'Index'.
2. All the submitted documents should be duly stamped and signed by the Authorized Signatory at each page.
3. The above checklist is indicative only. RailTel may ask for additional documents from the bidders, as per the requirement

Signature of Bidder …….
Name: ……
Designation ……..... Seal of BA Organization
Place: ……
Date: ……..

32.5 ANNEXURE 5

FORMAT FOR TECHNICAL BID COVER LETTER

(On Company Letter Head)

To,

The Joint General Manager (ERS)

RailTel Corporation India Limited,

Kerala Territory Office,

1st Floor, Eastern Entry Tower

Ernakulam South Railway Station

Ernakulam – 682016

Sub: Submission of the response to the Tender No. <<tender id>>Request for Proposal for the **Setting up Security Operations Centre (SOC) as part of KSEBL Data Centre under RDSS Scheme**.We, the undersigned, offer to provide services for **Setting up Security Operations Centre (SOC) as part of KSEBL Data Centre under RDSS Scheme** in response to the request for proposal dated <insert date> and tender reference no <> "**Setting up Security Operations Centre (SOC) as part of KSEBL Data Centre under RDSS Scheme**" by KSEBL. We are hereby submitting our proposal online, which includes the pre-qualification, technical bid, and commercial bid.

We hereby declare that all the information and statements made in this technical bid are true and accept that any misinterpretation contained in it may lead to our disqualification.

We undertake, if our proposal is accepted, to initiate the implementation services related to the assignment not later than the date indicated in this tender.

We agree to abide by all the terms and conditions of the RFP and related corrigendum(s)/ addendum(s). We would hold the terms of our bid valid for 210 days from the date of opening of the commercial bid as stipulated in the RFP. We hereby declare that as per RFP requirement, we have not been black listed/ debarred by any Central/ State Government and we are not the subject of legal proceedings for any of the foregoing.

We understand you are not bound to accept any proposal you receive.

Signature of Bidder …….
Name: ……
Designation ……..... Seal of BA Organization
Place: ……
Date: ……..

32.6 ANNEXURE 6

FORMAT FOR COMMERCIAL BID COVER LETTER

To,

The Joint General Manager (ERS)

RailTel Corporation India Limited,

Kerala Territory Office,

1st Floor, Eastern Entry Tower

Ernakulam South Railway Station

Ernakulam – 682016

Dear Sir,

We, the undersigned Bidder, having read and examined in detail all the tender documents with respect to **Setting up Security Operations Centre (SOC) as part of KSEBL Data Centre under RDSS Scheme**, do hereby propose to provide services as specified in the tender reference No. **CEIT/ITCSD/16/2024-25 dated 30.12.2024** Price and Validity

a) All the prices mentioned in our bid are in accordance with the terms & conditions as specified in the RFP. The validity of bid is 8 months from the date of opening of the commercial bid.
b) We are an Indian firm and do hereby confirm that our prices are inclusive of all duties, levies etc., excluding GST.
c) We have studied the clause relating to Indian Income Tax and hereby declare that if any income tax, surcharge on income tax, professional and any other corporate tax is altercated under the law, we shall pay the same.

Unit rates: We have indicated in the relevant schedules enclosed, the unit monthly rates for the purpose of accounting of payments as well as for price adjustment in case of any increase / decrease from the scope of work under the contract.

Deviations:

We declare that all the services shall be performed strictly in accordance with the RFP irrespective of whatever has been stated to the contrary anywhere else in our bid. Further, we agree that additional conditions, if any, found in our bid documents, shall not be given effect to. We had remitted an EMD as specified in the tender document terms.

Tender pricing: we further confirm that the prices stated in our bid are in accordance with your instruction to bidders included in tender documents.

Qualifying data: we confirm having submitted the information as required by you in your instruction to bidders. In case you require any other further information/ documentary proof in this regard before evaluation of our tender, we agree to furnish the same in time to your satisfaction.

Bid price: we declare that our bid price is for the entire scope of the work as specified in the RFP. These prices are indicated in annexure-commercial bid format attached with our tender as part of the tender.

Performance bank guarantee and Security Deposit: we hereby declare that in case the contract is awarded to us, we shall submit the performance bank guarantee. We hereby declare that our tender is made in good faith, without collusion or fraud and the information contained in the tender is true and correct to the best of our knowledge and belief. We understand that our tender is binding on us and that you are not bound to accept a tender you receive.

Signature of Bidder …….
Name: ……
Designation ……..... Seal of BA Organization
Place: ……
Date: ……..

32.7ANNEXURE 7

TECHNICAL COMPLIANCE SHEET

TECHNICAL SPECIFICATION

The Service/OEM/MAKE specified are based on the existing network requirement for the present scope of work. This shall be followed as per the special condition of contract as per the relevant conditions of special conditions of contract as appended as per RFP back to basis.

Item No. 1 of BoQ

NextGen SOC with SIEM, SOAR, UEBA, NDR and TIP
(To be provided in HA mode)

Sl.No	Functional Requirements	Compliance Yes or No	Comments
Security Incident and Event Management (SIEM)			
1	SIEM solutions must be dedicated on premise solution. The Bidder should propose the necessary hardware along with any additional software licences (Database, Virtualization etc.) as part of the proposal.		
2	The solution must provide the ability to encrypt communications on the network between SIEM components and SIEM		
3	The solution must ensure all distributed system components continue to operate when few parts of the NG-SOC solution fails or loses connectivity (i.e. management engine goes off-line; all separate collectors continue to capture logs).		
4	The solution should allow a wizard-based interface for rule creation. The solution should support logical operations and nested rules for creation of complex rules		
5	Collection, Correlation and Console layer should be logically separate.		
6	The Proposed solution must offer all the below built-in threat detection techniques out of the box: 1. Detect Web Application Threats. 2.Detect APT Threats. 3.Integrate with leading HoneyPot solutions. 4.Integrate with leading NBAD, NDR tools. 5.Give visibility of endpoints also by integrating with EDR, DLP, HIPS, Antivirus etc. for endpoint analytics. 6.Integrate with SOAR tools for automation. 7.Integrate with leading Threat intelligence Platform (TIP).		

	Log Management		
7	The proposed solution should be sized for sustained data of 12,000 EPS or equivalent Gb/day or equivalent CPU - capacity based at all layers but should be able to handle peak of 20,000 EPS or equivalent GB/day or equivalent CPU - capacity based at all layers without dropping events or queuing events and must take burst of 30000 EPS or equivalent GB/Day. There		
	should be no limitation on the number of servers, devices, users or log sources integrated with the solution and it should not have an impact on the license in case servers, users, or data source count changes, till the time data ingestion size remains as per specifications		
8	Raw and normalized Logs should be handled and stored in tamper proof way across SIEM solution. alter/modify tamper rights w.r.t Raw logs. The solution must provide capabilities for time stamping, efficient storage and compression (minimum 20%) of collected data.		
9	The proposed solution should be able to pull the logs through JDBC / ODBC connectors out of the box		
10	The solution should have customizable parsers to accept and process unknown log formats. Raw logs should be visible to the user in one single click. Raw log data from the solution shall be made downloadable without the need of OEM dependent tools.		
11	The solution shall allow creation of unlimited user licences with RBAC Controls in place		
12	The solution should have live visualization of logs received from each source		

13	Log Search Interface: The proposed solution must provide a simple, intuitive search interface using following search methodologies: a) Search Templates b) Search Patterns c) Search Operators d) Search Export e) Search Criteria f) Search Time Range g) Search Results View		
14	The solution must have the capability of Multi tenancy and should support a minimum of 10 tenants in the same system. The solution should have RBACs in place to limit the tenant level visibility.		
15	Log Management Automation: The proposed solution must provide a log management solution and must retain a minimum of 180 days retention (RAW + Normalized). And these logs should be readily accessible		
16	Universal Log Analysis: The proposed solution must contain system content that can be used for cyber-security, compliance, application and IT & OT operations monitoring and must support additional content specific to regulations like ISO 27001, IT-Act etc..		
17	Log Data Integrity: The proposed solution must provide audit trail of all the administration activities such as login, logout, new user creations, etc		
18	The proposed solution search performance must be capable of searching through millions of structured (indexed) events and unstructured (raw) log messages.		
19	Retention Policy Suspension: The proposed solution must provide the ability to suspend the retention configurations manually and allow administrators to increase the retention period.		
20	The solution should be able to conduct agentless collection of logs except for those which cannot publish native audit logs. System should not leverage any open source agents, instead the agents should be from the same OEM.		

21	Log Archival: The proposed solution must provide a log archival solution and must retain the logs for a minimum of 3 years period. And these logs should be accessible through a suitable mechanism		
	Event & Log Collection		
22	The solution should be able to collect and process raw logs in real- time from any IP Device including Networking devices (router/switches/SDWAN devices/voice gateways), Security devices (IDS/IPS, AV, Patch Mgmt, Firewall/DB Security solutions), Operating systems (Windows (all flavors), Unix, LINUX (all flavors), AIX etc), Virtualization platforms, Databases (Oracle, PostGre SQL, DB2 etc.), Storage systems, and Enterprise Management systems etc. The list of supported systems with which SIEM can INTEGRATE in each category viz. Network, Security, OS, Databases, Servers, Anti-malware system, Storage, Backup system, Hypervisors.		
23	The system should support, not restricted to, the following log and event collection methods: ▪ Syslog ▪ Flat file logs such as from DNS, DHCP, Mail servers, web servers etc. ▪ Linux and Windows events logs – Agent-based or agent-less. ▪ FTP, S/FTP, SNMP, ODBC, SDEE, WMI, JDBC, etc.		
24	Categorized Event Data: The proposed solution must categorize log data into an easy-to-understand humanly-readable format that does not require knowledge of OEM- specific event IDs to conduct investigation, define new correlation rules, and/or create new reports/dashboards.		
25	Reliable Transport: Log Transmission should use reliable TCP protocol that will ensure retransmission in the event of protocol failure to ensure that no log data is lost in transit.		
26	Collection Health Monitoring: Any failures of the log forwarding must be detected immediately and operations personnel must be notified via communication mediums such as e -mail.		
27	Caching & Batching: The proposed solution must support local caching and batching at collection level in case of connectivity failures.		

28	Time Correction: The proposed solution must be capable of collecting event time for systems along with collection time and alerting time. This allows integrity for forensic analysis to determine the original time of the event source and what the system time was for each system component processing the event.		
29	Centralized Incident Management: The proposed solution must provide an interface to view the incidents and alerts generated. The solution should have integrated Incident review frameworks such as MITRE ATT&CK and Attack Kill Chain integrated.		
	Correlation		
30	Correlation Rules: The proposed solution must provide correlations rules out-of-the-box.		
31	Cross-Device Correlation: The proposed solution must be capable of correlating activity across multiple devices out-of- the-box to detect authentication failures, perimeter security and operational events in real -time without the need to specify particular device types		
32	The solution must monitor and alert when there is a disruption in log collection from a device. In other words, if logs are not seen from a server in five minutes then send a notification.		
33	The solution must support correlated incidents for applications, databases, servers, networks etc. based on feed from other solutions like PAM, WAF, NBAD, TIP, Threat hunting Centre and UEBA		
34	The solution must provide many correlations rules out-of-the- box. Again, the option of creating/configuring new rules must be available.		
35	Solution should be able to perform the following correlations (but not limited to) based on analysis rules mapped to various threat categories and provided with criticality information. The various threat categories to be covered include: 1) Vulnerability based 2) Statistical based 3) Signature Based 4) Event Based 5) Unauthorized Access 6) Denial of Service 7) Service Unavailable 8) Whitelist/Blacklist/Reference List		

36	The solution should have intelligence to extract Information from leading global intelligence sources, proposed threat intelligence platform and use it for valid correlation.		
37	The solution should be able to collect and store data from various devices as text/csv files and use it for analysis.		
38	The system should provide adequate categorization and prioritization of the collected and aggregated events from the monitored log sources. This entails a deep understanding of the event types and criticality associated with the events for the supported log sources. The categorization may by be HIGH, MEDIUM, LOW or color coding. The dashboard should visualize individual log source wise dashboards.		
39	The system/solution should have the ability to correlate all the fields in a log.		
40	Events should not be dropped if it exceeds the EPS limitation for a period of 48 Hrs.		
41	The solution must provide a mechanism to capture all relevant aspects of a security incident in a single logical view. This view should include relevant events, network activity data,correlated alerts, vulnerability data, etc.		
42	Custom Dashboards: The proposed solution must provide the framework to create custom visual displays to support security operations.		
43	Dashboard Drill-Down: The proposed solution must provide the ability to allow analysts to drill -down from graphical dashboards to the underlying event data.		
44	All the latest updates and patches for the solution should be updated to the NG-SOC without any additional cost		
45	All the Event, Alerts and other information pertaining to Data Centre's NG-SOC must remain within Data Centre premises only. Any information moving out of Data Centre premises		
	shall be reviewed and approved by the Data Centre on need basis.		
46	Reusable Content: The solution must allow users to create objects such as filters or search queries that are reusable for the ease of operations		
	Alerting		

47	The solution must provide real time alerting based on observed security threats. The critical alerts should be transmitted using multiple protocols and mechanisms such as email,sms etc. based on agreed policies.		
48	Solution must be capable of monitoring attack/incident history against critical assets or by particular users.		
49	Alert Filters: The proposed solution must provide pre - defined alerts and provide the ability to re-use predefined filters and own created filters as alert criteria		
	Reporting		
50	The centralized web based/console user interface should drill down on reports and incident alerts on real time basis with full filtering capabilities		
51	The solution must provide reporting engine for out-of-box reports, customized reports, ability to schedule reports, compliance reports with the following options: 1. Detailed reports of non-compliant activities and policy violations in the network. 2. The solution must provide a reporting engine for out-of-box reports, customized reports, ability to schedule reports, compliance reports etc. 3. The solution should provide out of box templates for reports on ISO, PCI, SOX and other standards. 4. The system should allow scheduling reports. 5. Reports should be available in pdf and csv format.		
	Dashboard		
52	The SIEM solution must provide central management of all components and administrative functions from a single web based / console user interface.		
53	Customizable Dashboards: The proposed solution should provide dashboards specific to each user and should be user configurable. The dashboards must be capable of displaying multiple daily reports specific to each user's job function.		
54	SIEM solution should be able to map correlation rules/use cases with MITRE ATT&CK Framework and Cyber Kill Chain for tactics and techniques to get better visibility of incidents and shall be a part of the proposed solution.		
55	The system should be able to support integration with the proposed threat hunting Centre and other Security Analytics tools.		

56	In case the connectivity with the SIEM management system is lost, the collector should be able to store the data in its own repository. The retention, deletion, synchronization with SIEM database should be automatic but it should be possible to control the same manually.		
57	The solution should allow creation of custom reporting dashboards from forensics search conducted on the system		
58	Solution should have an OOTB bidirectional integration with Threat Intel Platform.		
59	The system should be capable of consuming Threat Intelligence from Third Party sources as well.		
	Administration		
60	The Solution should provide a web-based administration user interface for device management and monitoring.		
61	Administration Dashboard: The proposed solution must provide a single administrative dashboard to analyze the system load, resource utilization and storage performance trends.		
62	System Process Status: The proposed solution must provide an administration page that allows viewing underlying system process status and resetting application components without having to restart the entire system. This should be provided through the same web interface along with all other administrative tasks.		
63	The solution should be multi-tenant with RBAC and should provide dedicated dashboards for the officials		
	Threat Hunting Features:		
64	The solution should have out of the box capability to integrate with CERT-In CMTX threat feeds.		
65	The solution should give ability to perform open searches with simple and complex queries and enable threat hunting		
66	The solution should give the ability to store queries and execute queries on a periodic basis/as per the requirement.		
No	Functional Requirements	Compliance Yes or No	Comments
Security Orchestration Automation and Response (SOAR)			
Dashboard			

1	Solution Should have a configurable Dashboard dependent on the role of the user		
2	alerts reaching the SLA time period should be configured to show up in some manner		
3	Dashboard should display alerts, Analyst Task		
4	ROI should be configurable.		
5	Alerts should be sorted by Severity		
6	Each analyst must see his own workload		
7	Dashboard should support import, Export		
8	Dashboard should auto-refresh		
9	Role wise dashboard view - T1, T2 or level 1, level 2 analysts		
10	Solution must be able display mean time for identification, confirmation, containment, eradication, recovery, or aftermath for incident management		
11	Solution must have dedicated dashboard to monitor health status / availability of each integration		
Reporting			
12	Report should be Customizable using UI		
13	Report should allow Scheduling		
14	admin should be able to export report to the below Format: PDF, CVS		
15	Report must be sent by Email		
16	Access to reports be role dependent and controlled through RBAC		
17	Solution must support recoding of audit logs for all the downloaded reports		
18	Reports must have Metrics		
Alerts Incidents/Case Management			
19	Alerts and incidents should be handled separately		
20	Alerts fields should be automatically changed to the relevant type of attack		
21	Alerts should correlate with one another if they share the same type of attack, asset, or another applicable component		
22	Audit trail (un-editable) should be available for each case		
23	Interfaces must be customizable		
24	Admin must be able to view raw logs from parsed/normalized data queries		
25	Workflows/playbooks must establish what remediation actions an investigator can take and prevent actions that would unnecessarily make changes or cause evidence loss		

26	User must be able to add new artifacts or IOCs upon investigation completion		
27	User must be able to search for keywords across all fields of data		
28	all updates, notes or actions must be able to be pushed from the investigation to a ticketing platform		
29	Analyst should have the ability to request a new ticket be created in the ticketing platform with relevant information included		
30	Ticket must have the ability to automatic enrichment available for data like host, IP, file reputation, etc.		
31	Admin must have the ability to Manage the comments (add, edit/delete/remove) or attachment (add, edit/delete/remove, search)		
32	Ticket Metadata must offer various information on a selected ticket (who/when, ID, status, priority, queue)		
33	Case management must support Role Based Access (RBAC)		
34	Tickets escalation based on: Priority, Risk, Impact, Age		
35	Solution should be able of performing Root Cause Analysis (RCA – related to break-in cause)		
36	Solution should be capable of performing Post Incident Analysis (PIA – related to incident handling)		
37	Solution must have Customizable Playbooks/Workflows on how to handle an incident in different incidents (Email, web, endpoint infection)		
38	Solution must support global search across all incidents for Notes & Description or other keywords in the incidents		
39	Solution must support Incident Response Lifecycle (assignment/mapping/escalation)		
40	Solution must support Mapping/Tagging tickets/ incident to Cyber Kill Chain phases		
41	Solution must support SLA Tracking and alerting (Service Level Agreements of Incident Tracking)		
42	Solution must manage the attachment as part of alert / incident management (add, edit/delete/remove, search)		
43	Solution must provide detailed chain of custody for events viewed and data collected		
44	Solution must support Threat Hunting / Track Campaigns		
45	Solution must support search for the added IOCs in Log Management system		
46	Solution must Provide the required logs related to specific IOCs in the tickets (Network logs/Endpoint Systems)		
Playbooks			

47	Solution must have at least 40 playbooks out of the box		
48	reporting metrics of playbooks must be available (runtime, point of failure, etc.)		
49	Playbook execution must create an audit trail in the case		
50	Solution must have the ability to send update to the ticketing system from playbook steps and outcomes		
51	Admin must have the ability to export Playbook		
52	Solution must support running multiple playbooks at same time		
53	Debugging tools must be available out of box with the tool		
54	Solution must support creating playbooks with a visual interface		
55	Playbook must support: manual actions and tasks, Decision making, Nested playbook concepts, Python execution for custom scripts, Rich text Emails		
56	Tool must have at least 6 playbook initiation types		
57	Analyst must have the ability a playbook and tag playbooks\Folders		
58	Solution must have the ability to: • data ingestion playbooks • trigger reports from playbooks • capture errors and failure reasons • schedule playbooks • have looping conditions and step • add conditions to steps • add mock output to steps • ignore errors • clone steps in and across playbooks • align playbook steps automatically • mark playbooks as private or public		
59	Solution must control playbooks through RBAC		
60	Solution must read PDF and data can be extracted to indicators		
61	Solution must support playbook initiation on data update or delete		
62	Solution must support versioning of the playbook		
63	Solution must support export of single playbook / export linked playbook		
64	Solution must support restarting the playbook from failed step		
Connectors			
65	vendor must provide consistent update and support to supplied connectors		

66	vendor provide new connectors on future releases that are created by them		
67	Vendor must provide documentation to setup integration with the supported connectors		
68	Solution must have at least 250+ integration		
69	Solution must send a notification about new update		
70	Vendor must provide connector SDK without additional cost		
71	Solution must have data ingestion wizard for SIEM, Exchange,TIP and related platforms		
72	Solution must show integration/connector health status		
IOCs Artifacts			
73	Solution must have dedicated Indicators, Hunts and Complains module		
74	IOCs must correlation across different incidents/tickets		
75	Analyst can ingest bulk IOCs		
76	Analyst can add, edit, delete, remove, search IOC		
77	IOC can be grouped by Event, Campaign, Attacker, Vector, Sector Grouping		
78	Analyst must be able to tag IOCs to the Cyber Kill Chain phases		
Audit			
79	Solution must record audit trail of all manual and automated steps, actions during execution of a playbook		
80	Solution must be able to auto-document the entire incident workflow manual as well automated steps for all incidents timestamp of all actions taken in an incident.		
81	Solution must monitor its usage to maintain a complete audit trail of system access, system modifications, any configuration are changed etc. Granular audit logs with details of “Who, What, When, Where" with success/fail result for each and every activity of users.		
User Management & RBAC			
82	Solution must support role-based access control for segregation of alert/incident type to a role		
83	Solution must support an easy menu for administrators/managers to add, modify, and delete users then provision access		
84	Admin should be able to limit access to specific components (search, reports, run playbooks, etc.)		

85	The SOAR solution must support 2 active analyst users and total 10 users from day one		
86	Solution must support Single sign on and two factor authentications		
Deployment			
87	Solution must have the ability to fully deployed on-prem with HA		
88	Solution must be provided and deployed on Virtual or physical infrastructure		
89	Solution must easily transfer settings to an updated version		
User and Entity Behaviour Analytics (UEBA)			
1	Supply, Install, Configure, troubleshoot, customise, operate and maintain the User and Entity Behavior Analytics Platform.		
2	Enable monitoring and alerting for increased frequency in accessing high-value assets. Detect changes in user behavior over time, such as sudden spikes or gradual deviations from normal activity.		
3	Allow users to define custom peer groups and analyze behavior patterns effectively.		
4	Provide a single-pane-of-glass view into high-risk users/entities, showcasing their behavior patterns with respect to activities.		
5	Implement anomaly detection for sequences of actions not typical of user behavior.		
6	Implement measures to detect application misuse by malware or bots, especially regarding sensitive data access.		
7	The solution should be able to administer from a web browser without the requirement of any custom application.		
8	Solution should ensure the detection of behaviour anomalies of both Users and Entities in a log.		
9	Said UEBA tool should be from the same SIEM OEM for monitoring user endpoints and reporting anomalies		
10	The solution should be able to highlight risky and potentially abnormal user		
11	Should be able to show us RAW and Normalized data, or relevant data basis on which anomalous behaviour was observed		
12	Integration with enterprise authentication or SSO platform for simplified access		
13	Availability of out-of-the-box administrative dashboards and reports		

14	Ability to monitor, report and alert on the data streaming in and out of the system		
15	Proactive and actionable alerting for anomalous behaviour and risk scores		
16	High privilege access anomaly detection for misuse, sharing, or takeover		
17	Identifying suspicious activities of users.		
18	The solution should consist of a powerful visualization that enables threats being analyzed and investigated intuitively		
19	Use of Machine Learning algorithms for finding abnormal activities		
20	Dashboards for different roles and access levels		
21	The UEBA solution should be able to detect and analyse the behaviour based on rolling time windows.		
22	Provide various visualization options for deep-dive investigation, compliance and reporting		
23	The solution should be able to automatically identify and classify users and entities (i.e. devices, applications, servers, data, or anything with an IP address)		
24	Availability of out of the box reports for analysts to make investigation decisions, administration and management, audit and compliance,		
25	Ability to create reports and schedule the same. Reports can be delivered as CSV, Email, PDF		
26	Change in account privileges: User attempts to change privileges on existing account or open new accounts on other systems		
27	UEBA should activate rules for a set of users until a specified condition or specified time window		
28	UEBA should monitor users data transfer : more data being transferred then a normal to and from servers and/ or external locations		
29	Should identify Account used for identify User involved in previously malicious or threatening behavior. Detect insider threats, account abuse & data exfiltration.		
Network Detection and Response (NDR) Specifications			
Functional Requirements			
1	The proposed solution shall have the ability to profile and benchmark traffic using ML to compare traffic and identify anomalies		
2	The solution should provide detection, analysis and remediation capability against APT & SSL based APT attacks.		
3	The solution must employ an on premise (not on cloud) analysis engine using advance feature extraction techniques.Solution must not be signature based.		

4	The proposed solution shall be able to work on an Air-gapped basis without need to connect to internet and shall have the ability to provide ofline updates		
5	The proposed solution should perform sub second Malware Analysis of advanced malware to confirm true zero-day and targeted attacks. No file should be sent to third party systems or cloud infrastructure system for analysis and detection of Malware		
6	Mature AI that applies malware features to achieve sub-second verdicts for day-one deployment with the capability to learn new features		
7	Scientifically analyze zero days including fileless threats and classifies them into 20+ malware attack scenarios Ex.Ransomware, Downloader, Password Stealer etc		
8	Solution must detect “fileless” malware as a category. Fileless is defined as no files planted on infected hosts, purely operate in memory/CPU instructions level.		
9	Solution shall provide Forensic Analysis capabilities for Forensic Investigation		
10	The proposed solution should have the ability to display the geo-location of the remote command and control server(s) when possible.		
11	The proposed solution should have the ability to be deployed in out-of-band mode (also SPAN/TAP). Should be able to act as a ICAP Server to integrate with well known Secure Web Gateway &		
12	The proposed solution shall have the capability to detect network intrusions		
13	The proposed solution should support SMB / CIFS / NFS protocol or suitable mechanism for sharing and transferring files		
14	The proposed solution should be able to analyze saved email (.eml) files for malicious attachments.		
15	The solution should protect the endpoints against advanced threats including zero-day attacks, which target application vulnerabilities that have yet to be discovered or patched.		
16	The proposed solution shall provide attack timeline to locate patient zero		
17	The proposed solution shall support common protocols such as TCP, UDP, ICMP, ICMP6, TLS, HTTP, SMB, SMTP, SSH, FTP, POP3, DNS, IRC, IMAP, RTSP, RPC, SIP, RDP, SNMP, MYSQL, MSSQL, PGSQL		
18	The proposed solution shall detect vulnerable protocols in the network and alert		

19	The solution shall be available as a Dedicated Appliance or a software running on Server/VM		
Administration, Management Dashboard and Reporting			
20	The solution should provide reports in (but not limited to) PDF/CSV formats.		
21	The proposed solution should have the ability to report the Source IP, Destination IP, C&C Servers, URL, BOT name, Malware class, executable run, used protocols and infection severity of the attack.		
22	Solution must provide MITRE ATT&CK view of attacks		
23	The proposed solution should provide visibility into scan histories of each file scanned that are aborted, completed, or in progress.		
24	The solution should be able to schedule reports and also provide the flexibility to generate on-demand reports like daily/weekly/monthly/ yearly/specific range (day and time) etc.		
25	The proposed solution should be able to send both summary notifications and detailed per-event notifications utilizing the protocols (SMTP, or SNMP).		
26	The proposed solution shall have the ability to classify malicious web campaigns by name		
27	The proposed solution shall support 2FA for Administrative Logon		
28	The solution shall provide Role based access control capabilities		
29	The solution shall support LDAP & RADIUS for remote logon		
Lateral Movement Detection			
30	On-premise Learning to reduce false positives by analyzing an organization's specific traffic and adapting to newly disguised threats		
31	Traffic Learning to be based full packet analysis		
32	The proposed solution shall have the ability to detect Network Anomalies as follows: o Encrypted attacks (TLS), Weak Cipher and vulnerable protocol detections, Malicious web campaign detection, Network Attacks (intrusions), Botnet Attacks (both DNS and IP based), Malware sub-second verdict		
33	Solution shall be able to Trace Source of Malware/worm Attack by providing a 'attack timeline', showing where the infection is from and possible sources (e.g. Downloader downloads worm, worm spreads over to other IPs i.e.		

	lateral movement)		
34	In event of Outbreak the solution should provide threat hunting on		
	o. Similarity Based :- Show all detections which has similar features more than 75%		
	o. Hash Based :- Show all Detections matching exact Hash value		
	o. Detection Based :- Show all detections of similar name/category. There may be no similarity in samples, neither hash be same, but all may be falling in same Detection type. Ex. Ransomware, Downloader etc		
Incident Response & Prevention			
35	Mimic experienced security analyst for outbreak, anomalies, and malware detection, processing large volume of network data		
36	Integrate with various third party (via API) to provide inline blocking		
37	The proposed solution shall support the following file types but not limited to: EXE, PDF, Office, HTML, ZIP, VBA, TAR, GZIP, XML, PowerShell, PERL Script, Active MIME, Unicode, DMG, Python, JPEG, TIFF, BMP, MPEG, MP3, MOV, WMA, WAV, AVI, RTF, OpenOffice, DLL		
Integration			
38	The proposed solution must support REST API		
39	The proposed solution shall support malware Indicator of Compromise (IOC) exports as CSV, PDF and STIXv2 format, to be consumed by 3rd party Threat intel platforms		
40	The proposed solution shall have the capability to integrate with proposed SIEM and SOAR solution		

Item No. 2 of BoQ

Threat Intelligence Feed Service

S/N	Threat Intelligence Requirements	Compliance (Y/N/)	Remarks
1	**Scope**		
1.1	The proposed Vendor solution shall provide cyber threat intelligence and attribution information in the area cyber-crime, cyber-espionage, hacktivism, and enterprise security		
1.2	The proposed Vendor solution shall provide strategic, operational / tactical, and technical threat intelligence.		
1.3	The proposed Vendor solution shall provide cyber threat intelligence that is relevant to the below DC entities based on their business sectors and geographical locations: KSEB Data Centre, WAN		

1.4	The proposed Vendor solution shall identify and track cyber threat actors that are relevant to SOC. The proposed Vendor solution shall provide a summary of the cyber threat actors as part of the submission		
1.5	The proposed Vendor solution shall identify and track the tactics, techniques and procedures (“TTPs”) used by cyber threat actors that is relevant to SOC. The proposed Vendor solution shall provide a brief summary of the TTPs as part of the submission		
1.6	The proposed Vendor solution shall identify and track attack campaigns by the cyber threat actors that is relevant to SOC. The proposed Vendor solution shall provide a brief summary for the campaigns, as part of the submission		
1.7	The proposed Vendor solution shall maintain a mapping of the cyber threat actors (alias) to those actors tracked by other reputable proposed Vendor solutions. The proposed Vendor solution shall provide the mapping of the cyber threat actors as part of the proposal submission.		
1.8	The proposed Vendor solution must have capabilities to generate a risk score or other quantitative risk assessments of the feeds at least in 2 categories - Reliability & Credibility		
1.9	The proposed Vendor solution must support monitoring of Dark Web forums for information related to KSEB DC or SOC and provide searching of live raw feeds from these Forums.		
1.10	The proposed Vendor solution must support proactive monitoring of Threat Actor infrastructures such as C&C servers, Telegram/IRC channels, forums, OSINT, Card shops etc.		
1.11	The proposed Vendor solution must provide compromised information related to KSEB DC such as credentials, latest exposed credit cards (masked & unmasked both), Mule Accounts, Files, Mobile Devices etc by proactively monitoring Threat Actor infrastructures.		
1.12	The proposed Vendor solution must support monitoring of common OSINT platforms for information related to KSEB DC/SOC		
1.13	The proposed Vendor solution must provide list of all release vulnerabilities from different vendors both CVE and Non-CVE along with list of known exploits in the wild for the relevant vulnerabilities.		
1.14	The proposed Vendor solution must provide suspicious and malicious list of IPs in the categories of CnC server, DDoS, TOR nodes, BoT and Open Proxies etc		
1.15	The proposed Vendor solution must provide access to a central database of publicly leaked email credentials for easy search & alert if any of the DC accounts are leaked in public dumps.		
1.16	The proposed Vendor solution must provide detection of Phishing attempts, Domains, Phishing pages hidden inside and defacements by proactively monitoring Threat Actor infrastructures.		
1.17	The proposed Vendor solution should provide Cloud based sandbox or on-premise sandbox for KSEB Data Centre to submit files for detonation and inspection of unknown as well-known malware behaviour		
1.18	The proposed Vendor solution must provide Network Analytic Graph for Threat Hunting and attribution purposes for DC Threat Analysts. This linkage graph should act as a single lookup		

	functionality for multiple types of IOCs		
1.19	The proposed Vendor solution must provide detailed analysis of latest Threats by Cyber Criminal and Nation state Groups including but not limited to IOCs, MITRE ATT&CK mapping, tools used etc. These threat analysis reports should also include but not limited - - Malware - Campaign - Threat Actor profiles - TTP's - IOCs per threat - Monitoring of APT-related activity The Vendor must submit an example of such report as part of submission.		
2	Quality		
2.1	The proposed Vendor solution shall have a robust process in identifying, collecting, analysing, producing, reviewing, and tracking cyber threat information to produce threat intelligence that are relevant to KSEB DC/SOC. The proposed Vendor solution shall provide the process stated above as part of the submission		
2.2	The proposed Vendor solution shall categorize the cyber threat intelligence for easy searching and reporting by category. The proposed Vendor solution shall state its categorization supported in the submission		
2.3	The proposed Vendor solution shall enrich the cyber threat intelligence by adding context (Summary Report). The proposed Vendor solution shall state what enrichment is provided in the submission.		
3	Accuracy		
3.1	The proposed Vendor solution shall provide cyber threat intelligence that is accurate and relevant. The proposed Vendor solution shall provide information on accuracy and relevancy in the submission		
3.2	The proposed Vendor solution shall provide a confidence level for cyber threat information provided. The proposed Vendor solution shall provide information on the confidence level in the submission		
3.3	The proposed Vendor solution shall fine-tune the accuracy of the collection based on feedback from customer		
4	Timeline		
4.1	The proposed Vendor solution shall provide cyber threat intelligence in a timely manner. The proposed Vendor solution shall provide the tailored intelligence within 24 hours of first exposure to the public		
4.2	The proposed Vendor solution shall provide email alerts when new threat intelligence is available, based on rules configured		
4.3	The proposed Vendor solution should provide multiple different attacks performed by a Cybercriminal or Nation-State group in single place for easy searching and IOCs consumption.		
5	Research Analyst Access		
5.1	The proposed Vendor solution shall be supported by a research team with good track records with at least 5+ years of experience. The proposed Vendor solution shall demonstrate its track record as part of submission		

5.2	The proposed Vendor solution shall be able to provide threat information (sanitized) from its incident response engagements (e.g.,victim intelligence)		
5.3	The proposed Vendor solution shall provide analyst access to DC SOC, for the purpose of additional information request relating to cyber threats, such as threat actor, profiles, tactics, targets etc		
6	Machine Readable Technical Threat Intelligence (Feed)		
6.1	The proposed Vendor solution shall provide Indicator of Compromise (IoC) information in machine readable format. IoCs shall include both network and host-based indicators. The proposed Vendor solution shall provide the types of IoCs provided in the submission		
6.2	The proposed Vendor solution shall support STIX (Structured Threat Information Expression), TAXII (Trusted Automated Exchange of Indicator Information) and CSV format. The proposed Vendor solution shall state other formats supported in the submission		
6.3	The proposed Vendor solution shall maintain and update the list of IoCs provided to SOC		
6.4	The proposed Vendor solution shall provide IoC machine readable format that is supportable by the DC's SIEM platform. The proposed Vendor solution shall support DC in configuring the DC's SIEM platform to pull down IoC information automatically as part of the onboarding		
6.5	The proposed Vendor solution shall provide option to access the cyber threat intelligence via REST API. The proposed Vendor solution shall state if the information provided via the REST API is structured or unstructured		
6.6	The proposed Vendor solution shall state out-of-box support for Cyber Threat Intelligence Platform ("TIP") from reputable proposed Vendor solutions. The proposed Vendor solution shall state what TIP platform it supports out-of-box as part of the quotation submission		
7	Portal		
7.1	The proposed Vendor solution shall provide a portal for SOC to view and access the threat information knowledge base.		
7.2	The proposed Vendor solution portal shall provide search features for DC to search based on keywords, IP addresses, file hashes, threat actors, malware names, CVE et cetera. The search should preferably support complex searches such as AND, OR search expressions. The proposed Vendor solution shall state the search capabilities as part of quotation submission		
7.3	The proposed Vendor solution portal shall provide capabilities to alert DC for any new relevant content made available. The proposed Vendor solution shall state the different customizations supported to configure the alerting feature		
7.4	The proposed Vendor solution portal shall provide periodic summary via email. The proposed Vendor solution shall state what are the regular finished threat intelligence products included as part of the proposal.		
8	Threat Briefing		

8.1	The proposed Vendor solution shall provide regular threat calls to brief its customers on strategic cyber threat outlook and round-up. The proposed Vendor solution shall state the format and structure of such threat calls in the submission on request		
8.2	The proposed Vendor solution shall provide periodic threat landscape briefing to its customers. The proposed Vendor solution shall state the format and structure of such threat landscape briefings in the quotation submission		
9	Post Implementation Support		
9.1	The proposed Vendor solution shall provide First Level Support for post implementation		
9.2	The proposed vendor must provide 24x7 access to analyst team via portal to provide support on various types of RFIs such as - Phishing Take down, Threat Actor Profiling, IOCs enrichment, Malware reverse engineering, email and APK analysis etc		
9.3	The proposed Vendor solution must maintain history of all the requests or tickets on the portal for search and follow ups.		
9.4	Provide DC SOC with regular updates of its key innovations and capabilities, as well as market intelligence on related products and services that the proposed Vendor solution is providing SOC, and providing business or technical consultancy service to DC as appropriate		
9.5	Proposed Vendor solution is to provide an individual who will be the primary contact for DC SOC at the regional and local country level. This representative will:		
9.6	Have overall responsibility for managing and coordinating the proposed Vendor solution's services		
9.7	Meet regularly with DC SOC representative and our appointed third- party proposed Vendor solutions if required		
9.8	Have the authority to make decisions with respect to actions to be taken by proposed Vendor solution in the ordinary course of day-to-day management of DC SOC's account		
9.9	Ensuring internal compliance to DC's stated process and procedures		
10	Service Provider Credibility		
10.1	Service provider must have at least 10 years of experience in Cyber Threat Intelligence and forensic investigations related to cyber security across various countries (at least 5 countries)		
10.2	Service provider must have deep knowledge of attack methodologies, background, objectives, target countries/verticals categorised by specific APT groups.		
10.3	Service provider must release at least 5 reports publicly in a year covering High-tech crimes by different Threat Actor groups providing technical details of attacks and TTPs.		
10.4	The service provider must have their own Computer Security Incident Response Teams (CSIRTs) accredited by an external agency.		
10.5	The service provider must have been recognised by reputed industry experts/analysts for their Cyber Threat Intelligence services for APAC region.		
10.6	Service provider must have in-house capabilities to engage with law enforcement agencies and CERTs of different countries to provide assistance in investigations. Please provide public		

	reference case studies of your engagement with law enforcement agencies.		

Item No. 6 of BoQ

75" Professional LED Display

S/N	Specifications	Complied Yes or No	Remarks
1	Panel Type: IPS / VA		
2	Size: 75 inch		
3	Type: Led Backlight		
4	Resolution: 3,840 x 2,160 (UHD)		
5	Brightness: 500 nits or Higher		
6	Contrast ratio: 1100:1 or Higher		
7	Refresh Rate: 60Hz or higher		
8	Min Input ports: HDMIx3, USBx2 or higher, WiFi		
9	Min Output Ports: Audiox1		
10	Storage: 8GB or higher		
11	24x7 operation		
11	Product Quality Certifications: UL, BIS, FCC		

Item No. 7 of BoQ

Workstation with dual monitors

S.No	Specifications	Compliance (Yes/No)	Remarks
1	Processor : Latest generation i5 or Higher		
2	Motherboard : OEM Motherboard		
S.No	**Specifications**	**Compliance (Yes/No)**	**Remarks**
3	RAM : Minimum 16 GB DDR5 RAM expendable to 32 GB		
4	Dedicated Graphics card with Minimum 2 GB video memory (non- shared)		
5	Monitor: Dual Monitors of 24" TFT LED monitor, with Minimum 1920 x1080 resolution, Minimum input of 1xDP, 1x HDMI, 1xDVI, Energy star 5.0/BEE star certified		
6	Min. 500 GB NVMe SSD Drive		
7	Other Accessories : Line/Mic IN, Line- out/Spr Out, Minimum 6 USB ports (out of that 2 in front), 104 keys minimum OEM keyboard, USB Optical OEM mouse		
9	Operating System : Windows 11 Professional		

Signature of Bidder ……

Name: ……

Designation …….. Seal of BA Organization

Place: ……

Date: ……..

ANNEXURE 8

PRICE BID

To be uploaded as pdf (On Organization Letter Head)

EOI NO. RCIL/SR/ERS/2025-26/EOI/03 DTD. 27-05-2025

To,

The Joint General Manager (ERS)

RailTel Corporation India Limited,

Kerala Territory Office,

1st Floor, Eastern Entry Tower

Ernakulam South Railway Station

Ernakulam – 682016

TENDER NO: **CEIT/ITCSD/16/2024-25 dated 30.12.2024**

The RFP published by KSEBL for the work vide **CEIT/ITCSD/16/2024-25 dated 30.12.2024** as circulated March please be referred for any clarifications. **The submission of EMD, PBG, SD and Agreement with RCIL Non-Judicial paper by the selected Bidder will be sacrosanct selected Bidder**.

BOQ 1

Sl. No.	Item Description	Quantity	Units	BASIC RATE In Figures To be entered by the Bidder in Rs. P	GST in Rs. P	Other Taxes in Rs. P	All inclusive Rate/unit in Rs Rs. P	TOTAL AMOUNT With Taxes in Rs. P	TOTAL AMOUNT In Words
1	2	4	5	13	14	15	53	54	55
1	SOC services with SIEM,SOAR, UEBA and NDR	1.000	Set				0	0	
2	Threat Intelligence Platform Service	1.000	Set				0	0	
3	Central Log Collection Services	1.000	Set				0	0	
4	Log Archival Services	1.000	Set				0	0	

5	Indexed Log Services	1.000	Set				0	0	
6	75" Professional Displays	2.000	Nos				0	0	
7	Professional Workstations with dual monitors	7.000	Nos				0	0	
8	Installation,integration, testing and commissioning	1.000	No				0	0	
9	Manpower charges for L1 Resource (24X7x365 basis) for 5 years	1.000	No				0	0	
10	Manpower charges L2/L3 Resource (8X6 basis) for 5 years	1.000	No				0	0	
Total in Figures							0	0	
Quoted Rate in Words									

BOQ 2

Sl. No.	Item Description	Quantity	Units	BASIC RATE in Figures for 6th & 7th years to be entered by the Bidder in Rs. P	GST for the 6th & 7th years in Rs. P	Other Taxes for 6th & 7th years in Rs. P	Unit All inclusive Rate for 6th & 7th years in Rs. P	TOTAL AMOUNT With Taxes in Rs. P
1	2	4	5	13	14	15	53	54
1	**Extended Warranty /Support and Manpower charges for the 6th and 7th year**							
1.1	SOC services with SIEM,SOAR, UEBA and NDR	1.000	Set				0	0
1.2	Threat Intelligence Platform Service	1.000	Set				0	0

1.3	Central Log Collection Services	1.000	Set				0	0
1.4	Log Archival Services	1.000	Set				0	0
1.5	Indexed Log Services	1.000	Set				0	0
1.6	75" Professional Displays	2.000	Nos				0	0
1.7	Professional Workstations with dual monitors	7.000	Nos				0	0
1.8	Manpower charges L1 Resource (24X7X365 basis) for 6th and 7th year	1.000	No				0	0
1.9	Manpower charges L2/L3 Resource (8X6 basis) for 6th and 7th year	1.000	No				0	0
Total in Figures							0	0
Quoted Rate in Words								

BOQ 3

Sl. No.	Item Description	Quantity	Units	BASIC RATE In Figures To be entered by the Bidder in Rs. P	GST in Rs. P	Other Taxes in Rs. P	Unit All inclusive Rate in Rs Rs. P	TOTAL AMOUNT With Taxes in Rs. P	TOTAL AMOUNT In Words
1	2	4	5	13	14	15	53	54	55
1	Additional License for SOC solution for 1000 EPS (1Unit)	5.000	Nos	0					
Total in Figures							0	0	
Quoted Rate in Words									

BOQ 4

Sl. No	Item Description	Total Amount of BOQ in Figures To be entered by the Bidder in Rs. P	TOTAL AMOUNT With Taxes in Rs. P	TOTAL AMOUNT In Words
1	2	13	54	55
1	Total of BOQ 1		0	
2	Total of BOQ 2		0	
3	Total of BOQ 3		0	
Total in Figures				
Quoted Rate in Words				

Signature of Bidder …….
Name: ……
Designation ……. Seal of BA Organization
Place: ……
Date: ……..

32.8 ANNEXURE 9

PROFORMA FOR PERFORMANCE BANK GUARANTEE

(On Stamp Paper of ₹ Two Hundred/requisite value)

To,

The Joint General Manager (ERS)

RailTel Corporation India Limited,

Kerala Territory Office,

1st Floor, Eastern Entry Tower

Ernakulam South Railway Station

Ernakulam – 682016

Ref. No.: **CEIT/ITCSD/16/2024-25 dated 30.12.2024**; latest amendment/ Corrigendum clarifications. Floated on etender Kerala Portal (https://etenders.kerala.gov.in/)

In consideration of the RailTel Corporation of India Limited (CIN: L64202DL2000GOI107905), having its registered office at Plate-A, 6th Floor, Office Block Tower-2, East Kidwai Nagar, New Delhi–110023 (herein after called "RailTel") having agreed to exempt ..... (CIN: .....) having its registered office at..... (Herein after called "the said Contractor") from the demand, under the terms and conditions of Purchase Order No ..... dated..... made between RailTel and.....for (hereinafter called "the said Agreement") of security deposit for the due fulfilment by the said Contractor of the terms and condition contained in the said Agreement, or production of a Bank Guarantee for Rs. ..... (Rs..... Only). We ..... (Indicate the name and address and other particulars of the Bank) (hereinafter referred to as 'the Bank') at the request of .....contractor do hereby undertake to pay RailTel an amount not exceeding Rs. ..... (Rs ..... Only) against any loss or damage caused to or suffered or would be caused to or suffered by the RailTel by reason of any breach by the said Contractor of any of the terms or conditions contained in the said Agreement.

1. We, ...the Bank do hereby undertake to pay the amounts due and payable under this Guarantee without any demur, merely on demand from the RailTel stating that the amount is claimed is due by way of loss or damage by the said Contractor of any of terms or conditions contained in the said Agreement by reason of the Contractor's failure to perform the said Agreement. 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 ..... (Rs.....Only).

2. We, ... the Bank undertake to pay the RailTel any money so demanded notwithstanding any dispute or disputes raised by the Contractor in any suit or proceedings pending before any court or Tribunal relating thereto our liability under this present being, absolute and unequivocal. The payment so made by us under this Bond shall be a valid discharge of our liability for payment there under and the Contractor shall have no claim against us for making such payment.

3. 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 Agreement and that it shall continue to be enforceable till all the dues of the RailTel under or by virtue of the said

   Agreement have been fully paid an its claims satisfied or discharged or till RailTel certifies that the terms and conditions of the said Agreement have been fully and properly carried out by the said contractor and accordingly discharges this Guarantee. Unless a demand or claim under the Guarantee is made on us in writing on or before .....We shall be discharged from all liability under this Guarantee thereafter.

4. We, ……. the Bank further agree with the RailTel that the RailTel shall have fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the Agreement or to extend time of to postpone for anytime or from time to time any of the powers exercisable by the RailTel against the said Contractor and to forbear or enforce any of the terms and conditions relating to the said Agreement and we shall not be relieved from our liability by reason of any such variation, or extension to the said Contractor or for any forbearance, act or omission on the part of RailTel or any indulgence by the RailTel to the said Contractor 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.

This Guarantee will not be discharge due to the change in the constitution of the Bank or the Contract or (..... indicate the name of Bank ……) lastly undertake not to revoke this Guarantee during its currency except with the previous consent of RailTel in writing.

Dated the …… Day of …… 2025 for .....(Name of Bank) In the presence of Witnesses:

1.Signature with Date & Name

2. Signature With Date & Name

Signature of Bidder …….
Name: ……
Designation …..
Place: ……
Date: ……..

Seal of BA Organization

32.9ANNEXURE 10

NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement (this "Agreement") is made and entered into on this____day of, 2021 (the "Effective Date") at by and between RailTel Corporation of India Limited, (CIN: L64202DL2000GOI107905), a Public Sector Undertaking under Ministry of Railways, Govt. of India, having its registered and corporate office at Plate-A, 6th Floor, ~~Office Block, Tower -2, East Kidwai Nagar, New Delhi-110023 & Southern Region~~ office at 1-10-39 to 44, 6A, 6th Floor, Gumidelli Towers, Begumpet Airport Road, Opp. Shoppers Stop, Hyderabad- 500016, (hereinafter referred to as 'RailTel'), which expression shall unless repugnant to the context or meaning thereof, deem to mean and include its successors and its permitted assignees of the ONE PART, and) (CIN:_____), a company duly incorporated under the provisions of Companies Act, having its registered office at , (hereinafter referred to as ' '), which expression shall unless repugnant to the context or meaning thereof, deem to mean and include its successors and its permitted assignees of OTHER PART RailTel and_____shall be individually referred to as "Party" and jointly as "Parties" WHEREAS, RailTel and_____ , each possesses confidential and proprietary information related to its business activities, including, but not limited to, that information designated as confidential or proprietary under Section 2 of this Agreement, as well as technical and non- technical information, patents, copyrights, trade secrets, know-how, financial data, design details and specifications, engineering, business and marketing strategies and plans, forecasts or plans, pricing strategies, formulas, procurement requirements, vendor and customer lists, inventions, techniques, sketches, drawings, models, processes, apparatus, equipment, algorithms, software programs, software source documents, product designs and the like, and third party confidential information (collectively, the "Information"); WHEREAS, the Parties have initiated discussions regarding a possible business relationship for WHEREAS, each Party accordingly desires to disclose certain Information (each Party, in such disclosing capacity, the "Disclosing Party") to the other Party (each Party, in such receiving capacity, the "Receiving Party") subject to the terms and conditions of this Agreement.

NOW THEREFORE, in consideration of the receipt of certain Information, and the mutual promises made in this Agreement, the Parties, intending to be legally bound, hereby agree as follows:

1. Permitted Use.

(a) Receiving Party shall:

(i) hold all Information received from Disclosing Party in confidence;

(ii) use such Information for the purpose of evaluating the possibility of entering into a commercial arrangement between the Parties concerning such Information; and

(iii) restrict disclosure of such Information to those of Receiving Party's officers, directors, employees, affiliates, advisors, agents and consultants (collectively, the "Representatives") who the Receiving Party, in its reasonable discretion, deems need to know such Information, and are bound by the terms and conditions of (1) this Agreement, or (2) an agreement with terms and conditions substantially similar to those set forth in this Agreement.

(b) The restrictions on Receiving Party's use and disclosure of Information as set forth above shall not apply to any Information that Receiving Party can demonstrate:

(i) is wholly and independently developed by Receiving Party without the use of Information of Disclosing Party;

(ii) at the time of disclosure to Receiving Party, was either (A) in the public domain, or (B)known to Receiving Party;

(iii) is approved for release by written authorization of Disclosing Party; or

(iv) is disclosed in response to a valid order of a court or other governmental body in the India or any political subdivision thereof, but only to the extent of, and for the purposes set forth in, such order; provided, however, that Receiving Party shall first and immediately notify Disclosing Party in writing of the order and permit Disclosing Party to seek an appropriate protective order.

(c) Both parties further agree to exercise the same degree of care that it exercises to protect its own Confidential Information of a like nature from unauthorized disclosure, but in no event shall a less than reasonable degree of care be exercised by either party.

2. Designation.

(a) Information shall be deemed confidential and proprietary and subject to the restrictions of this Agreement if, when provided in:

(i) written or other tangible form, such Information is clearly marked as proprietary or confidential when disclosed to Receiving Party; or

(ii) oral or other intangible form, such Information is identified as confidential or proprietary at the time of disclosure.

3. Cooperation. Receiving Party will immediately give notice to Disclosing Party of any unauthorized use or disclosure of the Information of Disclosing Party.

4. Ownership of Information. All Information remains the property of Disclosing Party and no license or other rights to such Information is granted or implied hereby. Notwithstanding the foregoing, Disclosing Party understands that Receiving Party may currently or in the future be developing information internally, or receiving information from other parties that may be similar to Information of the Disclosing Party. Notwithstanding anything to the contrary, nothing in this Agreement will be construed as a representation or inference that Receiving Party will not develop products, or have products developed for it, that, without violation of this Agreement, compete with the products or systems contemplated by Disclosing Party's Information.

5. No Obligation. Neither this Agreement nor the disclosure or receipt of Information hereunder shall be construed as creating any obligation of a Party to furnish Information to the other Party or to enter into any agreement, venture or relationship with the other Party.

6. Return or Destruction of Information.

(a) All Information shall remain the sole property of Disclosing Party and all materials containing any such Information (including all copies made by Receiving Party) and its Representatives shall be returned or destroyed by Receiving Party immediately upon the earlier of:

(i) termination of this Agreement;
(ii) expiration of this Agreement; or
(iii) Receiving Party's determination that it no longer has a need for such Information.

(b) Upon request of Disclosing Party, Receiving Party shall certify in writing that all Information received by Receiving Party (including all copies thereof) and all materials containing such Information (including all copies thereof have been destroyed.

7. Injunctive Relief: Without prejudice to any other rights or remedies that a party may have, each party acknowledges and agrees that damages alone may not be an adequate remedy for any breach of this Agreement,

and that a party shall be entitled to seek the remedies of injunction, specific performance and/or any other equitable relief for any threatened or actual breach of this Agreement.

8. Notice.

(a) Any notice required or permitted by this Agreement shall be in writing and shall be delivered as follows, with notice deemed given as indicated:

(i) by personal delivery, when delivered personally;

(ii) by overnight courier, upon written verification of receipt; or

(iii) by certified or registered mail with return receipt requested, upon verification of receipt.

(b) Notice shall be sent to the following addresses or such other address as either Party specifies in writing.

RailTel Corporation of India limited:

Attn:

Address:

Phone:

Email:

9. Term, Termination and Survivability.

(a) Unless terminated earlier in accordance with the provisions of this agreement, this Agreement shall be in full force and effect for a period of years from the effective date hereof.

(b) Each party reserves the right in its sole and absolute discretion to terminate this Agreement by giving the other party not less than 30 days' written notice of such termination.

(c) Notwithstanding the foregoing clause 9(a) and 9 (b), Receiving Party agrees that its obligations, shall:

(i) In respect to Information provided to it during the Term of this agreement, shall survive and continue even after the expiry of the term or termination of this agreement; and

(ii) not apply to any materials or information disclosed to it thereafter.

10. Governing Law and Jurisdiction. This Agreement shall be governed in all respects solely and exclusively by the laws of India without regard to its conflicts of law principles. The Parties hereto expressly consent and submit themselves to the jurisdiction of the courts of New Delhi.

11. Counterparts. This agreement is executed in duplicate, each of which shall be deemed to be the original and both when taken together shall be deemed to form a single agreement

12. No Definitive Transaction. The Parties hereto understand and agree that no contractor agreement with respect to any aspect of a potential transaction between the Parties shall be deemed to exist unless and until a definitive written agreement providing for such aspect of the transaction has been executed by a duly authorized representative of each Party and duly delivered to the other Party (a "Final Agreement"), and the

Parties hereby waive, in advance, any claims in connection with a possible transaction unless and until the Parties have entered into a Final Agreement.

13. Settlement of Disputes:

(a) The parties shall, at the first instance, attempt to resolve through good faith negotiation and consultation, any difference, conflict or question arising between the parties hereto relating to or concerning or arising out of or in connection with this agreement, and such negotiation or consultation shall begin promptly after a Party has delivered to another Party a written request for such consultation.

b) In the event of any dispute, difference, conflict or question arising between the parties hereto, relating to or concerning or arising out of or in connection with this agreement, is not settled through good faith negotiation or consultation, the same shall be referred to arbitration by a sole arbitrator

14. The sole arbitrator shall be appointed by CIAL/RailTel out of the panel of independent arbitrators maintained by RailTel, having expertise in their respective domains. The seat and the venue of arbitration shall be New Delhi. The arbitration proceedings shall be in accordance with the provision of the Arbitration and Conciliation Act 1996 and any other statutory amendments or modifications thereof. The decision of arbitrator shall be final and binding on both parties. The arbitration proceedings shall be conducted in English Language. The fees and cost of arbitration shall be borne equally between the part.

15.CONFIDENTIALITY OF NEGOTIATIONS

Without the Disclosing Party's prior written consent, the Receiving Party shall not disclose to any Person who is not a Representative of the Receiving Party the fact that Confidential Information has been made available to the Receiving Party or that it has inspected any portion of the Confidential Information or that discussions between the Parties may be taking place.

16. REPRESENTATION

The Receiving Party acknowledges that the Disclosing Party makes no representation or warranty as to the accuracy or completeness of any of the Confidential Information furnished by or on its behalf. Nothing in this clause operates to limit or exclude any liability for fraudulent misrepresentation.

17. ASSIGNMENT

Neither this Agreement nor any of the rights, interests or obligations under this Agreement shall be assigned, in whole or in part, by operation of law or otherwise by any of the Parties without the prior written consent of each of the other Parties. Any purported assignment without such consent shall be void. Subject to the preceding sentences, this Agreement will be binding upon, inure to the benefit of, and be enforceable by, the Parties and their respective successors and assigns.

18. EMPLOYEES AND OTHERS

Each Party shall advise its Representatives, contractors, subcontractors and licensees, and shall require its Affiliates to advise their Representatives, contractors, subcontractors and licensees, of the obligations of confidentiality and non-use under this Agreement, and shall be responsible for ensuring compliance by its and its Affiliates' Representatives, contractors, subcontractors and licensees with such obligations. In addition, each Party shall require all persons and entities who are not employees of a Party and who are provided access to the Confidential Information, to execute confidentiality or non- disclosure agreements containing provisions no less stringent than those set forth in this

Agreement. Each Party shall promptly notify the other Party in writing upon learning of any unauthorized disclosure or use of the Confidential Information by such persons or entities.

19. NO LICENSE

Nothing in this Agreement is intended to grant any rights to under any patent, copyright, or other intellectual property right of the Disclosing Party, nor will this Agreement grant the Receiving Party any rights in or to the Confidential Information of the Disclosing Party, except as expressly set forth in this Agreement.

20. RELATIONSHIP BETWEEN PARTIES:

Nothing in this Agreement or in any matter or any arrangement contemplated by it is intended to constitute a partnership, association, joint venture, fiduciary relationship or other cooperative entity between the parties for any purpose whatsoever. Neither party has any power or authority to bind the other party or impose any obligations on it and neither party shall purport to do so or hold itself out as capable of doing so.

21. UNPULISHED PRICE SENSITIVE INFORMATION (UPSI)

agrees and acknowledges that_____, its Partners, employees, representatives etc.,by virtue of being associated with RailTel and being in frequent communication with RailTel and its employees, shall be deemed to be "Connected Persons" within the meaning of SEBI (Prohibition of Insider Trading) Regulations, 2015 and shall be bound by the said regulations while dealing with any confidential and/ or price sensitive information of RailTel. shall always and at all times comply with the obligations and restrictions contained in the said regulations. In terms of the said regulations_____shall abide by the restriction on communication, providing or allowing access to any Unpublished Price Sensitive Information (UPSI) relating to RailTel as well as restriction on trading of its stock while holding such Unpublished Price Sensitive Information relating to RailTel

22. MISCELLANEOUS.

This Agreement constitutes the entire understanding among the Parties as to the Information and supersedes all prior discussions between them relating thereto. No amendment or modification of this Agreement shall be valid or binding on the Parties unless made in writing and signed on behalf of each Party by its authorized representative. The failure or delay of any Party to enforce at any time any provision of this Agreement shall not constitute a waiver of such Party's right thereafter to enforce each and every provision of this Agreement. In the event that any of the terms, conditions or provisions of this Agreement are held to be illegal, unenforceable or invalid by any court of competent jurisdiction, the remaining terms, conditions or provisions hereof shall remain in full force and effect. The rights, remedies and obligations set forth herein are in addition to, and not in substitution of, any rights, remedies or obligations which may be granted or imposed under law or in equity.

IN WITNESS WHEREOF, the Parties have executed this Agreement on the date set forth above.

By Name:	RailTel Corporation India Limited:
Title:	By Name :
Witnesses:	Title:

32.10ANNEXURE 11

PRE -BID AGREEMENT

(To be executed in presence of public notary on non-judicial stamp paper of the value of Rs. 200/-. The stamp paper has to be in the name of the BA)

This Pre-Bid Agreement (the "**Agreement**") is made at New Delhi on this_____Day of (month) 2022.

BETWEEN

M/s. RailTel Corporation Of India Limited, (CIN: L64202DL2000GOI107905) a company registered under the Companies Act 1956, having its registered and corporate office at Plate-A, 6th Floor, Office Block, Tower-2, East Kidwai Nagar, New Delhi India – 110 023 and Southern Regional office at 1-10-39 to 44, 6A, 6th Floor, Gumidelli Towers, Begumpet Airport Road, Opp. Shoppers Stop, Hyderabad-500 016 (hereinafter referred to as **"RailTel"** which expression shall, unless repugnant to the context or meaning thereof, be deemed to include its successors and permitted assigns) of the **FIRSTPART. AND M/s. _XXXX_**, (CIN:_____) a company registered under the Companies Act 1956, having its registered office at and its Corporate Office located at_____(hereinafter referred to as **"_XXXX_"** which expression shall, unless repugnant to the context or meaning thereof, be deemed to include its successors and permitted assigns) of the **SECOND PART.**

RailTel and_____shall be hereinafter individually referred to as "**Party**" And collectively as "**Parties**. "**Whereas**,

A) RailTel is a "Mini Ratna (Category-I)" CPSU of Ministry of Railways, having exclusive right of way along Indian Railways and has created an OFC backbone and associated transport and network infrastructure to provide carrier class telecom services. RailTel has Unified License issued by DoT to provide a range of telecom services. RailTel also has two tier III certified data centres at Secunderabad and Gurugram. RailTel has created a slew of digital services like cloud, hosting, hosted Video Conferencing service, Aadhar Services, Content delivery platform, WIFI as a service etc. RailTel has strong capabilities in managing telecom infrastructure, MPLS network infrastructure, data centre services like as (Infrastructure as a Service) and PaaS (Platform as a Service).

B) _____(DETAILS OF SECOND PART)

C) RailTel had floated an **EOI No: _ dated_____pursuant to the RFP floated by End Customer for"__ for End Customer Organization for agreed Scope of Work"(hereinafter referred as "The said work/project/tender"),** and subsequently, based on the offer submitted by M/s XXXX towards the RailTel's EOI, M/s XXXX has been selected by RailTel as Business Associate for the said Project.

D) RailTel is in the process of participating in the tender issued by end customer, complete details of which have deliberately not been shared with XXXX and XXXX has waived its right to get the RFP document of end customer owing to confidentiality concern raised by the end customer. However, a limited scope of work on 'need to know basis and as detailed in clause 1.7 below, which will be carried out by XXXX has been shared with XXXX and based on the representation of "XXXX" that "XXXX" has read the said limited Scope of Work and has understood the contents thereof and that "XXXX" has sufficient experience to execute the said limited and defined scope of work, the Parties have mutually decided to form a " Business association" wherein RailTel shall act as the "Bidder" and "XXXX" shall act as the "business associate" in terms of the said Tender and in accordance to the terms agreed hereunder;

E) RailTel shall submit Rupees YYYY as BG against pre integrity pact at the time of submission of bid as an Integrity Pact bank guarantee to end customer and accordingly "XXXX" shall submit Rupees ZZZZ as BG of pre integrity pact on back-to-back basis to RailTel before final submission of the said bid to end customer. **(This is applicable on cases to case basis as per CIAL requirement. May please read in conjunction of the current RFP.)**

F) Party hereby acknowledges that RailTel has received Rs. /- (Rs._____) from M/s XXXX as per the Terms and conditions of EOI no. dated_____.

G) The Parties are thus entering into this Agreement to record the terms and conditions of their understanding and the matters connected therewith.

RailTel has agreed to extend all the necessary and required support to "XXXX" during the entire contract period.

NOW, THEREFORE, in consideration of the mutual covenants set forth herein it is hereby agreed by and between the Parties hereto as under:

1. SCOPE OF CO-OPERATION

1.1. Parties have agreed to form a "business association" to co-operate with each other on an exclusive basis with respect to execution of the said Project.

1.2. It has been further agreed between the Parties that Parties shall not bid individually for the said Project nor shall they enter into any arrangement with other parties for the purpose of bidding for the said Project during the validity of this Agreement.

1.3. The Parties also agree that the terms of the said EOI for limited and defined scope of work along with the Corrigendum's issued thereafter shall apply mutatis-mutandis to this Agreement.

1.4. The Parties further agree that they shall, enter into a 'Definitive Agreement' containing elaborate terms and conditions, role and responsibilities and respective scope of work of this Agreement after declaration of RailTel as the successful bidder of the said Project.

1.5. RailTel shall submit the PBG amounting Rs. XXXXX, earnest money deposit / EMD declaration (whichever is applicable) and performance bank guarantee to **End customer** and accordingly "XXXX" shall submit to RailTel, BG amounting to Rs._____as the earnest money deposit. Further, XXXX shall also pay the performance bank guarantee in proportionate to the extent of its defined scope of work.

1.6. RailTel may further retain some portion of the work mentioned in the end organization's RFP, where RailTel has competence so that overall proposal becomes most winnable proposal.

XXXX agrees, undertakes and acknowledges that following shall be Scope of Work of XXXX out of the total project work.:

2. Technical Terms – As per CIAL/RCIL document

3. TERM AND TERMINATION

3.1. This Agreement shall come into force as of the date of signing and shall continue to be in full force and effect till the complete discharge of all obligations, concerning the carrying out of the said Project, except terminated earlier by the Parties in terms of this Agreement or in terms of the said project, whichever is applicable.

3.2. This Agreement can be terminated by either Parties forthwith in the event of happening of the following events:

(a) End customer announces or notifies the cancellation of the said Project and / or withdrawing the said RFP.

(b) The receipt of an official communication that End customer chooses not to proceed with RailTel for the said Project or RailTel is not short listed by End customer.

(c) Material breach of any of the terms and conditions of this Agreement by either of the Parties and the same is not rectified by the defaulting Party beyond 15 (fifteen) days (ora reasonable time period as mentioned under the notice issued by the other Party) from the date of receipt of notice from the other Party to cure the said breach.

3.3. Parties agree and understand that as of the execution of this Agreement they are contractually bound and obligated to perform the services, obligations and the scope of work entrusted, should RailTel be declared as the successful bidder of the said Project. Any Party shall not withdraw its participation subsequent to execution of this Agreement, at any point in time except in case of material breach of any of the terms of the Agreement.

3.4. In case "XXXX" breach the terms of Agreement i.e. defaulting party in such case the balance unsupplied quantity or service shall be completed by RailTel i.e. non-defaulting party and cost for completion of that balance unsupplied quantity or service of such defaulting party shall be executed by RailTel at the risk and cost of such defaulting party.

4. Liability:

It is understood that the parties are entering into this pre-bid teaming agreement for requirement of submission of bid against the RFP floated by end customer for Implementation of Network Security System and Integration for end Customer Organization. Parties acknowledge and agree that "XXXX" shall be completely liable for the successful execution of this project, in relation to its defined scope of work (as detailed in clause 1.7 above), fully complying the end customer requirements. Accordingly, it is agreed that notwithstanding anything contained in the RFP document, "XXXX" shall be liable to RailTel with regard to its obligations and liability to complete the agreed and defined scope of work as detailed in clause 1.7 above.

5. EXCLUSIVITY

Parties agree to co-operate with each other for the purpose of the said Project on an exclusive basis with respect to applying for, submitting and execution of the said Project including providing of technical demo, proof of concept for the agreed and defined scope of work.

6. PAYMENT TERMS

The payment terms between the parties shall be only on receipt of payment from end customer.

7. TAXES

Parties agrees that they will comply with the Indian Income Tax Act in force from time to time and pay Indian Income Tax, as may be imposed / levied on them by the Indian - Income Tax Authorities, for the payments received by them for the Project under this agreement and any other taxes, cess, surcharge, etc. for their respective scope of works;

8. INDEMNIFICATION

8.1 Parties agree to and undertake to indemnify and hold each other, its officers, directors, agents and employees harmless, from and against any and all claims, demands, causes of action, losses, damages, costs and expenses (including attorney's reasonable fees, costs of investigation and defence) arising out of or resulting from any claim, action or other proceeding (including any proceeding by any of the indemnifying party's employees, agents or contractors) based upon:

i. any breach or contravention of any of the terms, conditions, covenants of this Agreement by the Party;

ii. Unethical business practices;

iii. any acts or omission of the Party and/ or any of its employees, agents or contractors, and the liability for damages to property arising from or out of party operations in connection with the performance of this agreement;

iv. any claim for taxes that might arise or be imposed due to this performance of Services hereunder;

v. any representation or warranty or information furnished by the Party being found to be false;

vi. Parties failure to pay all applicable compensation to its respective personnel;

vii. death or personal injury to any person;

viii. destruction or damage to any property by acts or omissions of either Party, its representatives or personnel;

ix. any violation/non-compliance by the Party with any applicable laws governmental regulations or orders;

x. any third-party liability;

xi improper handling or misuse of the Confidential Information of the Party(ies) by the Party

8.2 XXXX shall be liable to all risks and consequences (including the risk of payments) suffered in the performance of services under the Project and undertakes to indemnify RailTel from and against any non-payments (of RailTel's share payable to RailTel), recoveries and claim from End Customer or any other cost or losses incurred due to default/non-performance on part of XXXX.

9. COMPLIANCES TO STATUTORY OBLIGATIONS

9.1. Parties shall also obtain and keep in place necessary insurance policies, Mediclaim policies, group insurance schemes of adequate value to cover their workmen, supervisors, etc. with regard to any accidents, injury or the liability under the Employee Compensation Act.

9.2. Parties shall observe and be responsible for the compliance of all labour laws (including labour cess) as per government notifications and shall maintain necessary records for the same and shall submit the same to RailTel when so required.

9.3. Parties shall duly maintain all records / registers required to be maintained by them under various labour laws mentioned above and shall produce the same before the concerned Statutory Authorities whenever required and called upon to do so.

10. LEGAL STATUS

This Agreement constitutes a contractual relationship and shall relate solely to the Project and shall not extend to other activities or be construed to create a corporation, body corporate, partnership or any other form of legal entity.

11. REPRESENTATIONS AND COVENANTS

11.1. Each Party represents and warrants to the other Party as follows:

11.1.1. That it has full capacity, power and authority and has obtained all requisite consents and approvals to, enter into and to observe and perform this Agreement and to consummate the transactions contemplated hereunder. Each of the Persons / personnel executing this Agreement on behalf of the each of the Parties have full capacity and authority to sign and execute this Agreement on behalf of the respective Parties;

11.1.2. The execution, delivery and consummation of, and the performance by it, of this Agreement shall not conflict with, violate, result in or constitute a breach of or a default under, (a) any contract by which it or any of its assets or properties, are bound or affected, and/or (b) its constitutional documents;

11.1.3. This Agreement constitutes its legal, valid and binding obligations, enforceable against it, in accordance with their terms under Applicable Statutory Law(s);

11.1.4. It has the right, authority and title to execute this Agreement;

12. SUBCONTRACTING BETWEEN PARTIES

If a Party subcontracts certain supplies or services pertaining to its scope of work to the other party, then the resulting relationship between such parties shall be governed by a separate subcontract. This Agreement shall not in any way be affected thereby except as stated otherwise in this Agreement

13. GOVERNING LAW AND JURISDICTION

The construction, validity and performance of this Agreement shall be governed in all respects by the Laws of India. The Parties hereby submit to the exclusive jurisdiction of the Indian courts at Delhi only.

14. GOOD FAITH NEGOTIATION AND DISPUTE RESOLUTION

The parties shall, at the first instance, attempt to resolve through good faith negotiation and consultation, any difference, conflict or question arising between the parties hereto relating to or concerning or arising out of or in connection with this agreement, and such negotiation or consultation shall begin promptly after a Party has delivered to another Party a written request for such consultation.

In the event of any dispute, difference, conflict or question arising between the parties here to, relating to or concerning or arising out of or in connection with this agreement, is not settled through good faith negotiation or consultation, the same shall be referred to arbitration by a sole arbitrator.

The sole arbitrator shall be appointed by CIAL/RailTel out of the panel of independent arbitrators maintained by RailTel, having expertise in their respective domains. The seat and the venue of arbitration shall be New Delhi. The arbitration proceedings shall be in accordance with the provision of the Arbitration and Conciliation Act 1996 and any other statutory amendments or modifications thereof. The decision of arbitrator shall be final and binding on both parties. The arbitration proceedings shall be conducted in English Language. The fees and cost of arbitration shall be borne equally between the parties.

15. FORCE MAJEURE

“Force Majeure Event” shall mean any event beyond the reasonable control of the affected Party including acts of God, fires, earthquakes, strikes, pandemic, epidemics, lock down, and labour disputes, acts of war or terrorism, civil unrest, economic and financial sanctions, or acts or omissions of any Governmental Authority occurring on or after the Signature Date.

No Party shall be liable to the other if, and to the extent, that the performance or delay in performance of any of its obligations under this Agreement is prevented, restricted, delayed or interfered with, due to a Force Majeure Event. The Party affected by Force Majeure Event shall promptly inform the other Party in writing and shall furnish within 30 (thirty) days thereafter, sufficient proof of the occurrence and expected duration of such Force Majeure Event. The Party affected by Force Majeure Event shall also use all reasonable endeavours to mitigate the negative effects of such Force Majeure Event on such Party’s ability to perform its contractual obligations. In the event of a Force Majeure Event, the Parties shall immediately consult with each other in order to find an equitable solution and shall use all reasonable endeavours to minimise the consequences of such Force Majeure Event. The occurrence of a Force Majeure Event shall however, not relieve a Party of any obligation to pay any sum due under this Agreement prior to the occurrence of the Force Majeure Event. If the Force Majeure lasts for more than 6 (six) months, the Parties may mutually decide in writing on the future course of action with respect to this Agreement.

16. INTELLECTUAL PROPERTY RIGHTS

16.1. Each Party shall remain the sole owner of all industrial or intellectual property rights, Technical Data, Know-How, designs, specifications and the like, generated or acquired before the signature, or beyond the scope of this agreement.

16.2. Each Party shall remain the sole owner of all industrial or intellectual property rights, technical data, know-how, design specifications and the like generated solely by that Party during the course of the performance of this agreement and shall not be free to used it by the other party and if the other party uses that intellectual property rights prior permission shall be taken with paying necessary fees for such rights.

16.3. In case of joint development, the work-share and associated ownership of intellectual property of each Party shall be mutually agreed upon and defined in advance in the definitive agreement for the specific program. However, should any invention be jointly made by the Parties in the performance of this agreement, without neither Party being in a position to reasonably claim the ownership of said intellectual property right, the said right shall be jointly owned by the Parties and the corresponding measures of protection for both Parties of the said right as may be practicable shall be mutually agreed by both Parties and cost for such registration of such right shall be borne by the parties proportionately as per the ownership of the rights.

16.4 As on date, Parties confirms that there are no infringements of any Intellectual Property Rights of the products contemplated under this agreement, in accordance with the laws prevailing in the country.

16.5. The Parties undertake and confirm that the Technology / Knowhow / Design owned by each of them and intended to be put into use for execution of various Projects pursuant to this agreement has been originally developed by each of such Parties. The Parties are entitled to all the Intellectual Property Rights in Technology / Knowhow / Design intended to be put into use for execution of various Projects and no third-party Intellectual Property Rights have been put in to use either in their original or modified form without proper authorisation of such third party. The Parties further vouchsafes that the foregoing undertaking is actuated by truth and accuracy and no misrepresentation is being put into use for inducing each other to enter into this agreement.

17. CONFIDENTIALITY

17.1. During the term of this agreement, either party may receive or have access to technical information, as well as information about product plans and strategies, promotions, customers and related non-technical business in formation which the disclosing party considers to be confidential ("Confidential Information as per RFP tender document"). In the event Confidential Information is to be disclosed, the Confidential Information must be marked as confidential at the time of disclosure, or if disclosed orally but stated to be confidential, and be designated as confidential in writing by the disclosing party summarizing the Confidential Information disclosed and sent to the receiving party within thirty (30) days after such oral disclosure.

17.2. Confidential Information may be used by the receiving party only with respect to the performance of its obligations under this Agreement, and only by those employees of the receiving party and its subcontractors who have a need to know such information for purposes related to this Agreement, provided that such subcontractors have signed separate agreements containing substantially similar confidentiality provisions. The receiving party must protect the Confidential Information of the disclosing party by using the same degree of care to prevent the unauthorized use, dissemination or publication of such Confidential Information, as the receiving party uses to protect its own confidential information of like nature.

17.3. The obligations is not applicable to any information which is:

17.3.1. Already known by the receiving party prior to disclosure;

17.3.2. Publicly available through no fault of the receiving party;

17.3.3. Rightfully received from a third party without being responsible for its confidentiality;

17.3.4. Disclosed by the disclosing party to a third party without being responsible for its Confidentiality on such third party;

17.3.5. Independently developed by the receiving party prior to or independent of the disclosure;

17.3.6. Disclosed under operation of law;

17.3.7. Disclosed by the receiving party with the disclosing party's prior written approval.

17.4. XXXX agrees and acknowledges that XXXX, its Partners, employees, representatives etc. by virtue of being associated with RailTel and being in frequent communication with RailTel and its employees, shall be deemed to be "Connected Persons" within the meaning of SEBI (Prohibition of Insider Trading) Regulations, 2015 and shall be bound by the said regulations while dealing with any confidential and/ or price sensitive information of RailTel. XXXX shall always and at all times comply with the obligations and restrictions contained in the said regulations. In terms of the said regulations, XXXX shall abide by the restriction on communication, providing or allowing access to any Unpublished Price Sensitive Information (UPSI)relating to RailTel as well as restriction on trading of its stock while holding such Unpublished Price Sensitive Information relating to RailTel

17.5 Notwithstanding anything contained in this agreement, XXXX undertakes, agrees and acknowledges that being RailTel's Business Associate, XXXX shall maintain utmost confidentiality in relation to said Project. XXXX further, undertakes that any information relating to said Project which is or will be disclosed/ divulged by RailTel on need to know basis, will be received and treated by XXXX as strictly confidential and XXXX shall not, without the prior written consent of the RailTel or as expressly permitted herein, disclose or make available to any other person such information.

18. NOTICES

Notices, writings and other communications under this Agreement may be delivered by hand, by registered mail, by courier services or facsimile to the addresses as set out below:

To RailTel Corporation Of India Limited

To: RailTel Corporation of India Ltd

Attn: Executive Director / Southern Region

Address:1-10-39 to 44, 6A, 6th Floor, Gumidelli Towers, Begumpet Airport Road, Opp. Shoppers Stop, Hyderabad-500016 No.: +91-40-27788000

To XXXX

To: XXXX

Kind Attn: _____Address: _____ Mob. No.: Email:

19. AMENDMENT

No amendment or modification or waiver of any provision of these presents, nor consent to any departure from the performance of any obligations contained herein, by any of the Parties hereto, shall in any event be valid and effective unless the same is in writing and signed by the Parties or their duly authorized representative especially empowered in this behalf and the same shall be effective only in respect of the specific instance and for the specific purpose for which it is given.

20. PRIOR UNDERSTANDING

This Agreement contains the entire Agreement between the Parties to this Agreement with respect to the subject matter of the Agreement, is intended as a final expression of such Parties' agreement with respect to such terms as are included in this Agreement is intended as a complete and exclusive statement of the terms of such agreement, and supersedes all negotiations, stipulations, understanding, Agreements, representations and warranties if any, with respect to such subject matter, which precede or accompany the execution of this Agreement.

21. GENERAL

21.1. Binding Effect:

This Agreement shall be binding upon and inure to the benefit of the Parties here to and their respective legal successors.

21.2. Counterpart:

This Agreement may be executed simultaneously in 2 (two) counterparts, each of which shall be deemed to be original and all of which together shall constitute the same Agreement.

21.3. Non-Partnership:

-

21.3.1. This Agreement shall be on a principal-to-principal basis and shall not create any principal- agent relationship between the Parties.

21.3.2. Nothing in this Agreement shall be deemed to constitute a partnership or joint venture between the Parties or otherwise entitle either Party to have an authority to bind the other Party for any purpose.

21.4. Severability:

In the event any provision of this agreement is held invalid or un-enforceable by a court of competent jurisdiction, such provision shall be considered separately and such determination shall not invalidate the other provisions of this agreement and annexure/s which will be in full force and effect.

21.5. Waiver:

A failure by any Party to exercise or enforce any rights conferred upon it by this Agreement shall not be deemed to be a waiver of any such rights or operate so as to bar the exercise or enforcement thereof at any subsequent time.

21.6. Time is of essence:

Time is the essence of this agreement and the Parties herein agree and acknowledge to abide by the same.

22. Miscellaneous

22.1. No Party to this agreement will have any rights or obligations arising from or in relation to this agreement in excess of those rights and obligations expressly declared herein.

22.2. No Party to this agreement is entitled to sell, assign or otherwise transfer any of its rights and/or obligations arising from or in relation to this agreement to any third party, without the prior written consent of the other Party of this agreement.

22.3. Each Party shall be solely responsible for its own actions or failures to act and for its own commitments and undertakings. Neither Party shall present itself as the representative or agent of the other Party, nor shall it

have the power or the authority to commit the other Party, unless it receives the other Party's prior written consent.

22.4. No release shall be made by any Party to the news media or the general public relating to this agreement and/or the subject matter thereof without prior written approval of the other Party.

22.5. During the term of this agreement, each party shall refrain from taking any action or attempt to take any action with the intent of impairing or causing prejudice to the business relationship, whether existing or prospective that subsists between the other party and its customers and business partners. Each party shall also desist from inducing or influencing or attempting to induce or influence any customer or business partner, whether existing or prospective of the other party, resulting into prejudice or detriment to business prospects of the other party.

Furthermore, Parties shall not compete with or cause detriment to the business prospects of each other by making use of confidential information, whether in its embodied or disembodied form, shared pursuant to this agreement.

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement as of the day and year first above written.

For RailTel Corporation Of India Limited	For XXXX
Authorised Signatory	Authorized Signatory
Name:	Name
Designation:	Designation:
In Presence of witness	
Signature:	Signature:
Name:	Name:
Address:	Address:

32.11 ANNEXURE 12

FORMAT FOR AFFIDAVIT TO BE UPLOADED BY BA ALONGWITH THE EOI

DOCUMENTS

(To be executed in presence of Public notary on non-judicial stamp paper of the value of Rs. 200/-The paper has to be in the name of the BA) **

I_____ (Name and designation) ** appointed as the attorney/authorized signatory of the BA (including its constituents), M/s (hereinafter called the BA) for the purpose of the EOI documents for the work of _____ as per the EOI No.

of (RailTel Corporation of India Limited), do hereby solemnly affirm and state on the behalf of the BA

including its constituents as under:

1. I/we the BA (s), am/are signing this document after carefully reading the contents.

2. I/we the BA(s) also accept all the conditions of the EOI and have signed all the pages in confirmation thereof.

3. I/we hereby declare that I/we have downloaded the EOI documents from RailTel website www.railtelindia.com. I/we have verified the content of the document from the website and there is no addition, no deletion or no alternation to be content of the EOI document. In case of any discrepancy noticed at any stage i.e., evaluation of EOI, execution of work or final payment of the contract, the master copy available with the RailTel Administration shall be final and binding upon me/us.

4. I/we declare and certify that I/we have not made any misleading or false representation in the forms, statements and attachments in proof of the qualification requirements.

5. I/we also understand that my/our offer will be evaluated based on the documents/credentials submitted along with the offer and same shall be binding upon me/us.

6. I/we declare that the information and documents submitted along with the EOI by me/us are correct and I/we are fully responsible for the correctness of the information and documents, submitted by us.

7. I/we undersigned that if the certificates regarding eligibility criteria submitted by us are found to be forged/false or incorrect at any time during process for evaluation of EOI, it shall lead to forfeiture of the EOI EMD besides banning of business for five years on entire RailTel. Further, I/we (insert name of the BA) ** and all my/our constituents understand that my/our constituents understand that my/our offer shall be EMD rejected.

8. I/we also understand that if the certificates submitted by us are found to be false/forged or incorrect at any time after the award of the contract, it will lead to termination of the contract, along with forfeiture of EMD/SD and Performance guarantee besides any other action provided in the contract including banning of business for five years on entire RailTel.

VERIFICATION

SEAL AND SIGNATURE OF THE

DEPONENT

I/We above named EOI do hereby solemnly affirm and verify that the contents of my/our above affidavit are true and correct. Nothing has been concealed and no part of it is false.

DEPONENT

Place:

Dated:

SEAL AND SIGNAURE OF THE BA

**The contents in Italics are only for guidance purpose. Details as appropriate, are to be filled in suitably by BA. Attestation before Magistrate/Notary Public.

Signature of Bidder …….
Name: ……
Designation ……..... Seal of BA Organization
Place: ……
Date: ……..