Date: September 30, 2024

CORRIGENDUM No. 2: RESPONSE TO PRE-BID MEETING QUERIES FOR GeM TENDER ON "UPGRADATION OF CYBER SOC (REF.NO: GEM/2024/B/5393842)".

Please refer to the E-Tender reference no. GEM/2024/B/5393842 for Upgradation of Cyber SOC for Export-Import Bank of India. The pre-bid meeting was conducted on September 25, 2024, at 11 a.m. "The bidders are advised to consider the following amendments and corrigenda subsequent to the pre-bid meeting discussion before submitting their bids against this tender."

The details are as follows:

SrNo	Page No	Existing Clause	Revised Clause / Clarification
1	1	**GeM Bid Document:** Bid End Date/Time: 03-10-2024 15:00:00	**GeM Bid Document:** Bid End Date/Time: 11-10-2024 15:00:00
2	3	**Background and Purpose of the Project:** In addition, the partner will provide an onsite L2 engineer at EXIM Bank, Mumbai office. The detailed requirements are outlined in subsequent sections.	**Background and Purpose of the Project:** In addition, the partner will provide a dedicated onsite L2 engineer at EXIM Bank, Mumbai Head Office during business hours, Monday to Friday 0930 Hrs. to 1800 Hrs. following EXIM Bank calendar for leaves including bank holidays and 12 Annual leaves and 6 sick leaves. If the L2 resource is required to take continuous leaves for a period exceeding four days, including bank holidays and public holidays, the bidder must provide a substitute/backup resource at Exim Bank.
3	3	**Scope of Work:** Reporting and logging of information security incidents *using appropriate ticketing tools*.	**Scope of Work:** **Clarification:** Bidder to provide ITSM tool as a service dedicated to SOC operations for 10 user accounts.

4	20	**Bill of Material:** **1. MSSP License Cost**: - SIEM as a service for on-premises set-up ***For 5,000 EPS and 50,000 Flows*** IBM QRadar SIEM components: - a) Collectors, Processor, console for monitoring DC, DR and Cloud Environments. b) SIEM Set-up in DC and DR (Currently Bank has only DC set-up) c) UEBA/UBA d) ***Network Behaviour Analysis-50,000 Flows***	**Bill of Material:** **1. MSSP License Cost**: - SIEM as a service for on-premises set-up **For 2,500 EPS** IBM QRadar SIEM components: - a) Collectors, Processor, console for monitoring DC, DR and Cloud Environments. b) SIEM Set-up in DC and DR (Currently Bank has only DC set-up) c) UEBA/UBA d) Network Behaviour Anomaly Detection supporting deep packet inspection (IBM-QRadar Insights-QNI) at EXIM Bank DC & DR supporting 1 mirror port of 1 Gbps.
5	20	**Bill of Material:** **7. Threat Intelligence Including** 1) Brand Protection Services - Website URL or link Anti Phishing & Anti Malware. 2) Brand Protection Services -Rogue of Mobile Applications. 3) Brand Protection Services - Social Media handles of Top-level business executives 4) Brand Protection Services- Social Media Monitoring under Brand defacement Keywords related to Exim Bank. 5) Brand Protection Services - Social Media Monitoring under Brand defacement Dark web and domain names	**Bill of Material:** **7. Threat Intelligence Including** 1) Brand Protection Services - Website URL or link Anti Phishing & Anti Malware **for 10 URLs** 2) Brand Protection Services -Rogue of Mobile Applications **for 2 Mobile applications**. 3) Brand Protection Services - Social Media handles of Top-level business executives **for 5 users**. 4) No Change. 5) Brand Protection Services - Social Media Monitoring under Brand defacement Dark web and domain names **for 3 domains.**
6	18	**Payment Terms:** Define Payment Terms under the contract.	**Payment Terms:** **1)** The AMC payment will be made in half yearly advance basis within 15

			working days from original hardcopy invoice submission date. 2) Onsite L2 Resource payment will be made in quarterly basis within 15 working days from original hardcopy invoice submission date.
7	3	**Clarification Sought:** What is the current Storage and Sizing which Bank is using to maintains online data retention period of 180 days within the QRadar environment?	**Response:** Exim Bank will provide Server with sufficient Storage to retain 180 days logs.
8	3	**Clarification Sought:** Will bank extend its existing FMS/IT Service Team to support the installation activity?	**Response:** FMS/IT Service Team support will be provided.
9	3	**Clarification Sought:** Job Role for Onsite L2 engineer	**Response:** Onsite L2 engineer shall do following activities. 1. Coordination among SOC team, Exim IT team and Exim Information Security Unit [ISU]. 2. Analyze and categorize alerts generated by security tools, prioritize based on severity, and escalate issues. 3. Develop and implement strategies for containing security incidents, working with IT teams and ISU to remediate vulnerabilities. 4. Ticket creation on behalf of Exim Bank on the bidder's ISMS ticketing tool, follow-up, closing, and reporting to Exim Bank ISU. 5. Monitoring SIEM Tool, SOC and escalate the issues to SOC team and Exim ISU. **6.** Attending meeting with Exim IT and ISU team, prepare and follow up of actions points. Arrange monthly review meeting with SOC teams.

10	5	**Scope of Work:** **A. Next-Gen Managed Detection and Response (MDR)** **Point No. 21: Clarification Sought:** Bidder should develop custom plug-ins/ connectors / agents for business application monitoring wherever required. What is the total number of applications required custom plug-ins /connectors /agents.	**Scope of Work:** **A. Next-Gen Managed Detection and Response (MDR)** **Point No. 21: Response** Up to 15 custom plug-ins/ connectors / agents are required. The bidder has to provide additional plug-ins/ connectors / agents on a need basis for three years contract period for any new business applications.
11	5	**Scope of Work:** **B. Next-Gen Managed Detection and Response (MDR)** **Point No. 23: Clarification Sought:** Operation team should send alerts with details to designate personnel and systems upon detection of anomalies. Alert types at least should be, **SMS**, emails, phone calls, escalate the incident. Describe your capabilities and strategy for reporting and alerting incidents and findings along with the supported communication channels. **Request to remove SMS option.**	**Scope of Work:** **C. Next-Gen Managed Detection and Response (MDR)** **Point No. 23: Clarification Sought:** **Agreed. Revised clause as:** Operation team should send alerts with details to designate personnel and systems upon detection of anomalies. Alert types at least should be, emails, phone calls, escalate the incident. Describe your capabilities and strategy for reporting and alerting incidents and findings along with the supported communication channels.
12	8	**Scope of Work:** **D. Next-Gen SOAR Platform** **Point No. 3 Clarification Sought:** **Playbook Development and Management:** The service provider should possess expertise in developing and managing playbooks to automate routine security tasks and improve response efficiency. **How many Playbooks required.**	**Scope of Work:** **A. Next-Gen SOAR Platform** **Point No. 3 Response:** Maximum 5 Playbooks.
13	10	**F. Threat Intelligence Services** **Point No. 1: Clarification Sought:**	**F. Threat Intelligence Services** **Point No. 1:** Response:

		24x7 scanning of critical websites (identified by the Bank) for anti-phishing, anti-Trojan, and anti-malware service. How many websites needs to be considered for deep-web solution?	Total 10 web applications to be considered.
14	11	G. Attack Surface Management Clarification Sought: Please confirm is this external or Internal surface monitoring ?	G. Attack Surface Management **Response:** It is External Attack Surface Monitoring.
15	-	The Bank may consider "**Make in India**" Products for SIEM, SOAR, ASM and Threat Intelligence as per guidelines set forth by the Ministry of Electronics and Information Technology.	For the past five years, the Bank has utilized IBM QRadar as part of its Security Operations Center (SOC) infrastructure. These tender aims to upgrade the existing SOC by continuing with IBM QRadar as the SIEM solution while integrating additional technologies such as Security Orchestration, Automation, and Response (SOAR), Attack Surface Management (ASM), and Threat Intelligence. Accordingly, the Bank is open to considering 'Make in India' products for all newly proposed technologies, including SOAR, ASM, and Threat Intelligence.
16	12	G. Attack Surface Management Point No. 5: Clarification Sought The Bidder shall possess and demonstrate expertise in Breach and Attack Simulation (BAS) to proactively identify vulnerabilities and weaknesses within the Bank's IT infrastructure. Request to remove this clause.	G. Attack Surface Management Point No. 5: Response. Agreed to remove this clause.
17	8	Security Information & Event Management - IBM-QRadar (SIEM) Point No. 15 Assisting Banks team for Cyber Drill activity.	Security Information & Event Management - IBM-QRadar (SIEM) Point No. 15 Assisting Banks team for cyber drill activities and conducting tabletop exercises on a half-yearly basis.

18	20	Bill of Material Point No. 3 SOAR Platform License Cost – *Unlimited Licenses*	Bill of Material Point No. 3 SOAR Platform License Cost – *25 User licenses.*

All other terms and conditions of the tender document will remain unchanged. The tender document and corrigendum are available on our website https://www.eximbankindia.in/ tenders-and-notices

Sd/-
Madheshwaran G
DGM & CISO