EXIM BANK
EXPORT-IMPORT BANK OF INDIA

E-Tender for

Setting up of Security Operations Centre (SOC)

Head Office:

Center One Building, 21st Floor, World Trade Centre Complex, Cuffe Parade, Mumbai – 400 005

GENERAL TENDER DETAILS

Tender Document for	Setting up of Security Operations Centre (SOC)
Tender Reference No.	IT/EXIM/RFP/2018-19/039
Tender Document Cost	₹5,000/- (Non-refundable) (DD in favour of "Export-Import Bank of India" payable at Mumbai)
EMD Amount	₹5,00,000/-(DD in favour of "Export-Import Bank of India" payable at Mumbai)
Last date for acceptance of Tender document cost, EMD Amount and Integrity Pact Agreement (IPA)	12-Feb-2019 04:00 PM -DD and IPA to be submitted at **EXIM Bank Head Office:** **IT Group- IT/EXIM/RFP/2018-19/038** **Center One Building, 21st Floor, World Trade Centre Complex, Cuffe Parade,** **Mumbai – 400 005**
Date of Online Notice	21-Jan-2019 02:00 PM
Pre bid meeting date and time	30-Jan-2019----From 3.00 PM to 6.00 PM (No other way of bidding queries are entertained. Pre-bid meeting place at "EXIM Bank, Head Office, Mumbai")
Document Downloading Start Date	21-Jan-2019 05:00 PM
Document Downloading End Date	12-Feb-2019 02:00 PM
Last Date and Time For Submission	12-Feb-2019 04:00 PM
Opening Of Tender for Technical Evaluation	12-Feb-2019 04:30 PM
Address for communication	As above Ph. 022-22172600, Ext:- 2410 E-Mail: dharmendra@eximbankindia.in;
Place of Receipt of Tender	**https://eximbankindiatenders.procuretiger.com**

Note: Technical and Commercial bids will be opened online only. E-Tendering is the simulation of the manual tendering process on the internet. I.e. the eligible bidders / Tenders can log on to the internet site specified using a unique username and password and place their Technical & Commercial bids.

The eligible bidders will be trained by M/s e-Procurement Technologies Ltd. (Abc Procure) personnel on the methodology of submitting the bids online using a special digital signature / electronic key / password at the date and time specified. The bids placed by the tenderers are confidential and will be opened by the authorized EXIM Bank officials. No other person can gain access to the information regarding the bids, which is confidential in nature.

Minimum requirement for e-tender participation:

1. Computer / Laptop with internet connection.
2. Operating system – Windows XP Service pack 3 / Windows 7/ Windows 10.
3. Digital certificate - Class II or III, Signing + Encryption, and it should be organizational certificate.
4. Vendor registration can be done online by opening Website:

https://eximbankindiatenders.procuretiger.com Click on "New Bidder Registration" link, create User Id and Password and attach your Digital certificate. For any clarification kindly contact -

E-Procurement Technologies Limited
801 – Wall Street – II
Opposite Orient Club near Gujarat College, Ellis
Bridge Ahmedabad – 380 006 Gujarat, India
Phone: +91 (79) 40230 813/14/16/18/03
Fax: +91 (79) 40230847

Mandatory information required for pre-qualification of the Tenderer

I/We confirm that to the best of our knowledge this information is authentic **and accept that any deliberate concealment will amount to disqualification at any stage.**

Sr. No.		Particulars	Details
1. Name of theFirm			
2.Name of theProprietor,			
Partners/Directors			
A (Mobile No.)			
B (Mobile No.)			
3. Office TelephoneNos.			
a.			
b.			
c.			
4. Head Office Address			
5. Email Address a.			
b.			
6. Year of Establishment			
7. Registration No. and Date of Registration			
8. Status OfFirm. (Proprietor/Partnership/Co. etc)			
9. Name ofBankers	a.		
	b.		
10. PAN Card No.			
11. GSTNo.			

Seal and Signature of the Bidder/s not required since the document is digitally signed.

Date:
Place:
Note:

Please upload scanned copies ofCertificates for S.No.7,8,10,11

Introduction

Export-Import Bank of India (EXIM Bank) is the premier export finance institution of the country that seeks to build value by integrating foreign trade and investment with the economic rise of India. The Bank has been guided by expertise at the Board level, by senior policy makers, expert bankers, leading players in industry and international trade as well as professionals in exports, imports or financing. With offices spread across India and in select locations of the world, the bank aspires to boost the businesses of industries and SMEs.

Established by the Government of India, we commenced operations in 1982 under the Export-Import Bank of India Act, 1981 as a purveyor of export credit, mirroring global Export Credit Agencies. With our rich pedigree, today we serve as a growth engine for industries and SMEs through a wide range of products and services. This includes import of technology and export product development, export production, export marketing, pre-shipment and post-shipment and overseas investment. In a rapidly shifting financial landscape, we are a catalyst and key player in the promotion of cross border trade and investment. By instilling a powerful culture of innovation and foresight, we help India maximize its potential and meet and exceed its vision.

Export-Import Bank of India has taken many IT initiatives. Bank has Computerized 100% of its branches and has implemented a Centralized Banking Solution (CBS) with Data Centre at Mumbai and Disaster Recovery Site at Bengaluru. The centralized Banking Solution covers all 11 Domestic offices which are connected to the Data Centre through an Enterprise Wide Network (MPLS).

EXIM Bank is having Office 365 for e-mail infrastructure and Sharepoint framework for intranet application and other internal workflow automations. Applications from multiple vendors for different internal requirements of Bank are also in use. The Operating Systems used in Different applications include different flavors of UNIX like AIX, Linux etc., and flavors of Windows. The Data bases include Oracle, MySQL, Microsoft SQL Server, Access etc. The Enterprise Wide Network is maintained by Bank's Network Integrator and the security measures are already enforced at various levels (Application Security, Network Security, Database Security, OS Security, Access Controls, and Physical Security etc.). All these security measures are in place in congruence with the Bank's Information Security Policy, Business Continuity & Disaster Recovery Plans & various other regulatory compliances.

Background and Purpose of the Project

Bank has its data centre at Mumbai Head office. At present we have approximately 50 servers, 100 network devices, In-row Cooling solution, on-line UPSs etc. Presently the system generates system / security /event logs on the respective devices and the log analysis is being done on need basis. To automate the process, the Bank is interested to implement a Centralized Log Management system. The logging of events should be on real time basis at the Data Centre and on batch mode for the other offices.

The Bidder shall setup an onsite SOC at the bank's 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, mitigate and report incidents as they occur along with 24*7 offsite monitoring. SIEM Solution to be deployed in Banks premises.

Supply, install, implement, integrate, customize, manage and maintain Security Information & Event Management (SIEM) and associated Tools, Technologies and Resource to meet Bank's Requirements.

Vulnerability management tool to be implemented for performing VA and configuration management activities as per the defined Secure Configuration Document (SCD).

Provide services like Log analysis & Monitoring, Vulnerability Management, Application Security, Penetration Testing, Incident Management, Anti Phishing, Anti Malware, Phishing Site take down, SCD etc. as elaborated in this tender document.

The vendor shall also provide the SCDs (Hardening documents) to secure the OS / Database pertaining to servers / devices with different flavors and different versions of the operating systems (like Windows, Linux, Unix, AIX, etc.), databases (like Oracle, SQL, etc.), webservers (like Windows IIS, Apache Tomcat for Windows and Linux, etc.), routers, switches, etc. The list of OS / Database are only indicative not exhaustive. The vendor shall review and provide updated checklist documents quarterly with proper version control. The vendor has to implement all the SCD at least once in the live environment successfully.

Scope of Work

- Identification & Prevention of Information Security Vulnerabilities: The SOC should be able to identify information security vulnerabilities in the bank's environment and prevent these vulnerabilities through implementation of adequate security solutions.

- Incident Management: Reporting and logging of information security incidents using appropriate ticketing tools. Track and monitor the closure of these information security incidents and Escalation of these incidents to appropriate teams/ individuals in the bank if required.

- Continuously improve SOC operations.

- The solutions deployed should be modular, scalable and should be able to address the Bank's requirements during contract period, with the deployed hardware.

- The solutions should not have any significant impact on the existing infrastructure of the Bank either during installation/ implementation or during operation of SOC.

- Putting in place an adaptive Incident Response, Management and Recovery framework to deal with adverse incidents/disruptions.

- Performing Risk Assessment Activity in line with cyber security framework defined by regulators.

- Development and implementation of minimum Baseline Cyber Security and Resilience Framework.

- The SOC to be implemented should fully comply with the banks configuration guidelines as to ensure continuous surveillance.

- Development of Cyber security preparedness indicators.

- Implementation of Cyber Crisis Management Plan (CCMP) in line with Cyber Security Policy of the Bank.

Security Information & Event Management (SIEM):

- Implement the SIEM tool to collect logs from the identified devices, applications, databases, end points, network devices, applications in cloud etc.

- Ensure that the SIEM/ security monitoring and analytics tool & other solutions used in the SOC are up to date in terms of product releases, version upgrades, patches and other service packs.

- The selected Bidder shall supply, install, customize, integrate, migrate, test, and troubleshoot the SIEM to run SOC.

- The SIEM product must enable BANK to collect, correlate, analyse, derive logical conclusion from logs, events, information received by it from heterogeneous systems including Networking and Security systems, OS, Web servers, Applications, databases, other infrastructure etc.

- Bidder must ensure that once the logs are written to the disk/ database no one including SIEM or database / system administrator should be able to modify or delete the stored raw logs.

- Implement correlation rules based on out-of-box functionality of the SIEM solution and based on the use-cases defined.

- Design and implement threat modelling

- Apply machine learning, AI based models to detect and mitigate advance threats on real time basis.

- Integrate SIEM with other security solutions and build use cases, threat modelling using those tools.
- Integrate SIEM with security analytics.
- The SIEM tool should be integrated to VAPT Tool to provide a comprehensive dashboard for VAPT reports.
- Rapid real-time response to incidents.
- Monitor the SIEM alerts and suggest/ take appropriate action.
- Perform on-going optimization, performance tuning, and maintenance, configure additional use cases, and suggest improvements as a continuous improvement process.
- Perform log backup and archival as per Bank's policy requirements, and applicable legal/statutory requirements.
- Assisting Banks team for Cyber Drill activity.
- The SIEM tool should be integrated with incident management tool to generate automated tickets for the alert events generated by the SIEM tool. All the security devices and solutions being proposed as part of the current RFP need to be included for monitoring by SIEM solution.
- Manage and carry out rule-based Audit using automated tools of Security Devices/solutions viz., Firewalls (at least once in six months for 5 sets of firewalls), other security devices (Windows AD, Antivirus, Office365 etc., at least once in a year) Reports should at a minimum provide the following

    a) Recommendation on cleanup and optimizing rulesets

    b) Discover and Recommend mitigation for risky rules

SOC Operations:

- Bidder shall conduct the monitoring of various types of operating systems, web servers, application servers, databases, servers, storage, Network & security devices and solutions etc. Bidder will also be responsible for any escalation or trouble- shooting requirements.
- The Bidder shall monitor an onsite SOC at the bank's premises during working hours and offsite SOC by accessing Onsite SOC application hosted in Banks 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, mitigate and report incidents as they occur. One resource to be deployed onsite.
- Bidder shall monitor security devices/security logs to detect malicious or abnormal events and raise the alerts for any suspicious events that may lead to security breach in BANK's environment.
- The SIEM product must enable BANK to collect, correlate, analyse, derive logical conclusion from logs, events, information received by it from heterogeneous systems including

Networking and Security systems, OS, Web servers, Applications, databases, other infrastructure etc.

- Bidder shall do pro-active and continuous monitoring of security events throughout the network by co-relation and analysis of logs from servers, network devices, security devices and application systems (Layer7).
- log and availability monitoring for infrastructure and business applications.
- Bidder should provide consolidated security status reporting through centralized and automated application.
- Provide centralized security dashboard with integrated reporting of all systems and services.
- Bidder must follow the best practices for all compliances related to data and its security.
- Bidder shall propose solution that should can retrieve the archived logs for analysis, correlation, reporting and forensic purposes.
- Bidder must ensure that for each security incidents, solution should provide online and real time remediation guidance.
- Bidder must provide threat intelligence feed (free and commercial) for identifying new global threats around the globe like DDoS (Slowloris or LOIC etc.), Malicious IP Addresses, Domain, URL, Filename ,File hash, Email address, Known C&C (Command and Control) hosts, Geolocation feeds like latlong, ASNumber, ISP, Country, etc.
- Proactively inform about potential security threats/vulnerabilities, new global security threats/ zero day attacks in circulation and suggest and implement suitable countermeasures to safeguard BANK‘s IT assets and data against such evolving threats / attacks along with the analysis.
- Bidder should develop custom plug-ins / connectors / agents for business application monitoring wherever required.
- Describe the level of customization you provide for Custom connectors, log parsers mainly, reports, dashboards, etc.
- Operation team should send alerts with details to designate personnel and systems upon detection of anomalies. Alerts 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.
- Bidder should be adopting a variety of correlation methodologies that may include: a) Rule based Correlation b) Statistical Based c) Historical Based d) Heuristic Based e) Human Based Correlation.
- Bidder must be able to correlate logs based on threat intelligence feeds for botnet C&C servers, malware domains, proxy networks, known bad IP’s and hosts, traffic to APT domains.
- Bidder must monitor interruption or gaps in both generation and reception of logs, includes missing logs, log disabled, log setting changes, time gap between log events.

- Provide live dashboards with capability to browse and drill down to the actual data or other data transformations.
- Bidder must provide capability to authorize IT staff to perform investigative advanced searches with rules and correlations over real-time and historical data.
- Integrate with HR systems and Active directory data to extract metadata on the users and assets to enrich the correlation. Such data would be department, previous department, employee type, membership to groups, access to assets or criticality of the user, VLAN etc.
- The Bidder should integrate with popular vulnerability assessment tools to extract vulnerability results and correlate activities on the network based on the risk level of the asset.
- Bidder must ensure the integrity and confidentiality of the logs in transfer or at storage.
- It should include the trend analysis comparing the present reporting cycle data with the previous reporting cycle data (Weekly, Monthly, Quarterly and annually as what may be applicable).
- Bidder should develop a Standard Operating Procedure (SOP) for all the products /solutions /services provided including alert management, incident management, forensics, report management, log storage and archiving, Business Continuity.
- Monitor events from WAF and suggest/ take appropriate action on an on-going basis.
- Develop new policies and improve the policies configured on an on-going basis to reduce the occurrence of false positives.
- Provide single integrated and consolidated enterprise view of security and compliance

Management and Monitoring

- Bidder shall provide 24x7x365 management & monitoring of security devices which includes proposed devices. It is to be noted that bidder shall have separate dedicated of 50 members each for monitoring and management of SOC components.
- Automated vulnerability and patch management should be integrated with the framework.
- Before updating critical systems and application, the criticality of the patch and the compatibility should be checked and the same must Management and maintenance of security devices / solutions/ technologies to ensure compliance with internal policies, regulatory & legal requirements be informed with corrective measures.
- Conduct risk assessment activity for the security devices under the scope of SOC.
- Reporting/escalations and closure of alerts
- Crisis Management

Integration with Privilege Identity Management (PIM)

- Integrate the existing PIM with SIEM to generate alerts for any PIM violations.
- Monitor events from PIM and suggest/ take appropriate action on an on-going basis.
- Develop new policies and improve the policies configured on an on-going basis to reduce the occurrence of false positives.

Incident Response and Problem Management

- The bidder will also provide a detailed process for managing incidents - describing each phases of the process – prepare, identify, contain, eradicate, recover and learn from the incidents responded to.
- Develop response plan/ strategy which will describe the prioritization of incidents based on the organizational impact.
- The incident management solution should be able to register any security event and generate alerts. The solution should provide complete life cycle management of alerts from incident generation till closure of the incident. The solution should have capability to structure rule based work flow and calendar/ event based alerting capability.
- Establishing process for identifying, preventing, detecting, analyzing & reporting all Information Security incidents as per the best practices, this may revise time to time as per the requirements.
- Incident and problem Management, resolution, root cause analysis, and reporting within time limit as per the requirement.
- Describe the incident response process including the roles and responsibilities and scope of action.
- Incidence Response to comply with international standards. ISO/IEC 27035-1 Security incident management NIST.SP.800-61 Computer Security Incident Handling Guide, CSIRT, Computer Security Incident Response Team.
- Bidder should do root cause analysis for security incidents and recommend implementation of controls to prevent reoccurrence.
- Bidder must provide on demand timely support by performing investigation and forensic analysis on the logs by doing the necessary analysis on the logs by doing the necessary analysis and log review and providing required data on a timely fashion.
- Faster incident response by replacing purely ad-hoc activities with Advanced playbooks, analytical tools, incident management tools and reporting, which liberates security analysts to spend less time doing research and more time doing analysis.

Anti-Phishing, Anti-Trojan, Anti-Malware, and Anti-Rouge Services

- 24x7 scanning of critical websites (identified by the Bank) for anti-phishing, anti-Trojan, and anti-malware service.
- Takedown of websites and Mobile App as per Bank's request.
- A dashboard view of the risks and threats to the bank initiated in deep web and dark web and threat intelligence report regarding the same is presented to the Bank. The Bank should be provided with online access to the dashboards.
- To protect Websites from "Phishing" and alert the Bank authorities' concerned, immediately if Bank's Brand/ logo is targeted in Phishing attacks. Upon detection, the bidder shall work to shut down the phishing site and submit the report.
- Rapid response to phishing attacks
- Track hosting of phishing websites through digital watermark.
- Tracking new Domain Name Registrations to detect any spoofed or similar site being registered, this will include brand abuses too.
- Providing alerts on detection of phishing sites, daily status report on the phishing site detected and the action taken.
- Report on phishing trend in India and across the globe.
- Monitor events from anti-APT and suggest & take appropriate action on an on-going basis.
- Anti-Phishing framework should be integrated part and should be automated. The framework should have minimal impact on traffic and network.
- Framework should have Real-time instant alerting upon detection of malicious behavior.
- Detailed remediation recommendation guidance including step by step instructions on how to address the threats captured.
- Framework should be able to perform authenticated and unauthenticated scans.
- Identify email addresses that are being used for sending spoofed emails.
- The bidder should monitor networks known to be source of attacks and/or points of collection of compromised data, compromised devices, Malicious URLs, malicious command and control sites.
- The Bidder should maintain or have direct access to data from Honey-pots or network of sensors to collect data on Trojans.

Security Intelligent Services

- Continuous feed from the deep web and dark web about the risks and threat to the organization.

- Incorporate managed detection response using security analytics on end points and network devices for deeper detection.
- The Bidder shall regularly track and advise the Bank about new global security threats and Vulnerabilities.
- The Bidder shall ensure adequacy, appropriateness and concurrency of various policies and guidelines in place in the Bank and shall provide Information Security consultancy for newer technology deployment for new and existing applications and products.
- The Bidder shall have access to and track leading security databases such as- NIST, OEM sites, CERT-IN, OWASP, OVAL, CVE, Anti-virus vendors, National Vulnerability Database, and SANS etc.
- Bidder should provide alerts on critical outbreaks, global risks, critical patches released applicable on the systems and technologies.

Storage:

- The SIEM should be able to maintain 3 months of logs. In addition, the bidder should provide for near line secondary storage for archiving logs for up to 1 years.
- The solution should be capable of automatically moving the logs from device to archival storage based on the ageing of the logs. The logs should also be available online to the device for easy correlation and auditing should provide detailed auditing to easily detect files deletes, add changes as and when asked by Bank.
- The complete SIEM Storage Solution should have Write Once Read Many (WORM), Encryption, Advance Indexing and Searching, Retention and Disposal capabilities in Online, Near Line and External Storage Types.
- The solution should provide Compression and De-duplication functionalities on archival system.
- The solution should provide data replication over IP to a different site for disaster recovery and data protection with support for Unidirectional, Bi-directional, one-to-many and many-to-one replication topologies, Retention and Disposal functionality, and no single point of failure in the solution.

PENETRATION TESTING/BLACK BOX TESTING [PT]) and VULNERABILITY ASSESSMENT

- ✓ The Bidder shall carry out PT for minimum 5 EXIM websites on a half yearly basis.
- ✓ Vulnerability assessment has to be carried out for all the applications/critical devices of the Bank on half yearly basis.

- ✓ The Bidder shall conduct scheduled penetration testing for identified devices / networks to identify security issues/vulnerabilities that could be exploited by remote attackers. The penetration testing exercise must give the Bank a picture of overall security of the infrastructure as seen from the Internet.

- ✓ The penetration testing should include testing for information pilferage, denial of service, password cracking, brute force attack etc.
- ✓ The SOC shall Generate Executive Reports in graphical format and Technical Reports in text format for all penetration tests conducted.
- ✓ Assessment document should necessarily contain proof/evidence of the vulnerabilities identified.

- ✓ The Bidder shall provide a comprehensive report for Vulnerability Assessment and Penetration Testing activity. Vulnerability reporting must be concise and understandable. The Bidder shall provide / offer technical consulting services to mitigate the reported vulnerabilities. Once the Bank initiates the corrective measures to mitigate the risk, a re-check shall be done by the vendor to ascertain / ensure the security of the organization.

Eligibility and Technical Evaluation Criteria

S.No.	Evaluation Parameter	Minimum Requirement	Maximum Marks	Details	Attachments/Necessary documentary evidence/ proofs
1	The bidder submitting the offer should have minimum average turnover of Rupees 50 Crores for the last three financial years i.e. 2015-16, 2016-17 & 2017-18. This must be the individual company turnover and not of any group of companies. The bidder should have positive net worth for past three years.	50 Crores	20	Rs.50 Crores = 15 marks Rs.50-100 Crores = 18 Marks >100 Crores = 20 marks	Chartered Accountant /Auditor certificate is required mentioning the turnover and net worth details of the company for past three years. Along with Chartered Accountant/auditor certificate, the balance sheets have to be uploaded.
2	No. of SOC projects above Rs. 100 lakhs globally.	2 Projects	5	2 Projects = 2 Marks 3 Projects = 3 Marks 4+ Projects = 5 Marks	PO/Invoice Copy/Work Order/Self Declaration for projects under NDA

3	Company should have established SOC internally/on Premise	1 soc	5	1 soc=5 Marks	Self-Declaration for SOC set up
4	Quality Certificates: ISO 9001:2015 ISO 27001:2013	Minimum One Certificate is required.	5	3 Marks for one valid certificate and 5 Marks for both the certificates.	Scan Copy of certificates
5	SOC Team Size of the Company	15 Members	10	Qualified SOC Team Members 15 =6 Marks 25 = 8 Marks >25= 10 Marks	Self-certificate
6	Proposed Solution/SI should be in Gartner's leader/challenger quadrant for SIEM Or Strong Performer/Leaders quadrant in Forrester Wave For MSSP	SIEM product Should be in Gartner's leader or challenger quadrant.	20	Only Gartner challenger/Leader quadrant for SIEM = 10 Marks. Gartner challenger/Leader and Forrester Wave Strong Performer/Leaders quadrant =20 Marks	Copy of latest Gartner report and Forrester Wave For MSSP. MAF to be uploaded as per annexure-I for SIEM.

7	Project Manager & Proposed Team for EXIM Bank	Project Manager: CISSP/CISA/CISM/CEH With 10 years of proven experience in Incident Handling in a Major Corporation/ Government Organization Tentative list of proposed team member to be provided	10	1 Certified Manager = 6 Marks 5 SOC Staff = 8 Marks 5+ Certified Staff = 10 Marks	Resume and Certification copies.
8	AI enabled Chabot, Web based ticketing system	Web based ticketing system	5	AI enabled chatbot and Web Based Ticketing system=5 Marks, Only Web based ticketing system=3 Marks	Self-certificate.
9	Approach, Methodology & Expertise (Presentation would be held if required) Sample reports to be submitted which would be evaluated.		20	Based on data submitted including (1) Project plan and Product details for all products/technology that will be used in EXIM Bank Environment. 2) People to be deployed in the environment and 3) Proposed process) and formal presentation on	Project Report

				the architecture for 1 hour	
10	The bidder should not figure in the negative / black list of any public sector undertaking / bank /Government organization for breach of applicable laws or violation of regulatory prescriptions or breach of agreement for providing the SOC services.				Self-Certificate
11	Integrity Pact has to be executed as per Annexure	Mandatory			Download the IPA (attached as Annexure) and sign on Rs.500 stamp paper. Scanned copy to be uploaded on the E-tender portal. Original document to be handed over to Exim Bank, Head Office, Mumbai on or before Last date and time of tender submission. If the bank is not receiving the Physical IPA as per requirement then the bidding is invalid.

Bidders who score marks greater than or equal to 70 will qualify for participation in the Commercial Bid. The evaluation of the response to this E-TENDER will be done on a 70-30 Techno-commercial Evaluation method. This evaluation will be conducted only for Bidders scoring 70 marks or above in the technical evaluation. A comprehensive "Score (S)" will be arrived at after considering the commercial quote and the marks obtained by the eligible bidders in technical evaluation with relative weights of 30% for commercials and 70% for technical. The

Bidder with the highest score will be declared successful. **Bids received from a consortium of bidders will be summarily rejected. Bidding in consortium is not allowed for this procurement.**

Computation Methodology for arriving at "successful Quote":

- The evaluation criteria will be based on Quality and Cost Based Selection (QCBS) on 70:30 valuation. The Bidder must score a minimum of 70 marks in the Technical evaluation criteria to be qualified for commercial evaluation.
- For Quality and Cost based Evaluation (QCBS), the following formula will be used for the evaluation of the bids. The scores will be calculated as:

A "Score (S)" will be calculated for all qualified bidders using the following formula:

$$\text{Commercial score (CS)} = \frac{C_{low}}{C} \times 30$$

$$\text{Technical score (TS)} = T \times 0.7$$

$$\text{Final score (S)} = CS + TS$$

C_{low} - The lowest commercial bid.

C - Commercial quote of the bidder.

T - The marks obtained by the bidder as per the technical evaluation.

- The bidder achieving the highest overall score will be invited for negotiations for awarding the contract. In case of a tie where two or more bidders achieve the same highest overall score, the bidder with the higher technical score will be invited first for negotiations for awarding the contract.
- Bank reserves the right to negotiate the price with the finally successful bidder before awarding the contract.
- The Bank's decision in respect to evaluation methodology will be final and binding and no claims whatsoever in this respect will be entertained.
- The Bank also reserves the right to re-issue / re-commence / cancel the Bid/Bid process. Any decision in this regard by the Bank shall be final, conclusive and binding on the Bidders.

ANNEXURE - 1

Manufacturer Authorization Format (On OEM's letter head)

Ref: Date:

To

GM
Export-Import Bank of India
Head Office, Mumbai

Dear Sir,

Sub: Manufacturer Authorization for RFP No._____ dated xx/xx/xxxx

We <OEM Name> having our registered office at <OEM Address> are an established and reputed manufacturer of <hardware details> do hereby authorize M/s_____ (Name and address of the Partner) to offer their quotation, negotiate and conclude the contract with you against the above invitation for tender offer.

We hereby extend our full guarantee and warranty as per terms and conditions of the tender and the contract for the solution, products/equipment and services offered against this invitation for tender offer by the above firm and will extend technical support and updates / upgrades if contracted by the bidder.

We also confirm that we will ensure all product upgrades (including management software upgrades and new product feature releases) are provided by M/s ……..for all the products quoted for and supplied to the Bank.

<OEM Name>
<Authorized Signatory>

Name:

Designation:

ANNEXURE - 2

E-Tendering Process Compliance Statement

The following terms and conditions are deemed as accepted by you for participation in the bid event:

1. The price once submitted cannot be changed.

2. Technical and other non-commercial queries (not impacting price) can be routed to the respective contact personnel of EXIM Bank indicated in the tender document. Bidding process related queries could be addressed to M/s e Procurement Technologies Ltd personnel indicated in the tender document.

3. Inability to bid due to glitch in telephone lines, Internet response issues, software or hardware hangs will not be the responsibility of M/s E-Procurement Technologies Ltd or the EXIM Bank. However M/s E-Procurement Technologies Ltd, shall make every effort to ensure availability of technology resources to enable continuous bidding.

4. M/s E-Procurement Technologies Ltd does not take responsibility beyond the bid event. Order finalization and post order activities would be transacted directly between bidder and the EXIM bank.

5. Bids once made cannot be withdrawn or modified under any circumstances.

6. EXIM Bank can decide to extend or reschedule or cancel an e-tendering.

7. The bidders are advised to visit https://eximbankindiatenders.procuretiger.com for any corrigendum etc.

I / We have read, understood and agree to abide by the e-tendering process compliance statement.

Date:-

Organization Name:-

Designation:-

ANNEXURE – 3

UNDERTAKING FROM THE BIDDER

Mr. Dharmendra Sachan, General Manager,

Export- Import Bank of India, 21st Floor, Centre One,

World Trade Centre,

Cuffe Parade, Mumbai 400 005

Dear Sirs,

Ref: **Setting up of Security Operation Centre (SOC)**

Ref. No: **IT/EXIM/RFP/2018-19/039**

I / we further agree to execute and complete the work within the time frame stipulated in the tender scope of document. I / we agree not to employ Sub-Service Providers without the prior approval of the EXIM Bank. I / We agree to pay Sales Tax, Works Contract Tax, Excise Tax, Octroi, LBT, VAT, Duties, all Royalties and all other applicable taxes prevailing and be levied from time to time on such items for which the same are liable and the rates quoted by me/us are Exclusive of the same.

I / we understand that you are not bound to accept the lowest tender or bound to assign any reasons for rejecting our tender. We unconditionally agree Exim Bank's preconditions as stipulated in the tender documents and empanelment process.

I / We agree that in case of my/our failure to execute work in accordance with the specifications and instructions received from the Exim Bank, during the course of the work, Exim Bank reserves the right to terminate my contract.

Yours truly,

Seal and Signature of the Bidder/s not required since the document is digitally signed.

Place: Name:

Date: Designation:

Seal:

INSTRUCTIONS TO TENDERERS

1.0 Location:

Export-Import Bank of India, 21st Floor, Centre One Building, World Trade Center, Cuffe Parade, Mumbai 400 005 and regional offices in pan India.

a. Tenderers must get acquainted with the proposed work, specifications, conditions of contract and other conditions carefully before tendering. No request of any change in rates or conditions for want of information on any particular point shall be entertained after receipt of the tenders.

2.0 Submission of Tender:

Refer to E-Tendering Process Compliance Statement .No queries will be entertained on last day of tender submission.

3.0 Any **printing or typographical errors /omission** in tender document shall be referred to EXIM Bank and their interpretation regarding correction shall be final and binding on Service Provider.

4.0 Transfer of Tender Documents:

Transfer of tender documents purchased by one intending Tenderer to another is not permitted.

5.0 Validity:

Tenders submitted by Tenderers shall remain valid for acceptance for a period **up to 30 days from the date of opening of Bid/tender**. The Tenderers shall not be entitled during the period of validity, without the consent in writing of EXIM Bank to revoke or cancel his tender or to vary the tender given or any terms thereof.

6.0 Right to accept or reject tender:

The acceptance of a tender will rest with the EXIM Bank who does not bind themselves to accept lowest tender and reserve to themselves the authority to reject any or all the tenders received. They also reserve the right of accepting the whole or any part of the tender and the Tenderers shall be bound to perform the same at the rates quoted. All tenders in which any of the prescribed conditions are not fulfilled or are incomplete in any respect or there is any correction notduly signed and dated by the Tenderer are liable to be rejected. For this purpose, Tenderer shall quote rates for various items which will be self-sufficient to meet their whole costs for executing any / every item. No demand for variations in rates for items executed shall be entertained on the plea of the EXIM Bank deciding to delete, alter or reduce the quantities specified in respect of the any item.

7.0 Rates:

EXIM Bank is not concerned with any rise or fall in the prices of materials, Parts and Labour during 30 days' pricevalidity.

8.0 Payments: The AMC payment will be made in half yearly advance basis within 15 working days from original hardcopy invoice submission date. Any delay in technical service as per the tender scope of work will attract penalty of 1% of the AMC cost on per day basis.

9.0 Signing of the contract:

a) The successful Tenderer may be required to execute a non-disclosure agreement (**NDA**) and Service Level Agreement (**SLA**) with Exim Bank within 30 days from the date of receipt of the notice of acceptance of tender. In the event of failure on the part of the successful Tenderer to sign the agreement in the above- stipulated period. EXIM Bank may cancel the order.

b) Until the Agreement is formally signed, the Work Order / Letter of Acceptance of Tender issued to the successful tenderer and accepted by him shall be operative and binding on the EXIM Bank of India and the Service Provider.

10.0 On acceptance of the tender, the name of the accredited representatives of the Tenderer who would be responsible for taking instructions from EXIM Bank shall be mentioned by the Tenderer.

11.0 If so decided EXIM Bank reserves the right to appoint PMC (Project Management Consultant) or any other agency to get the quality of works checked, measurements recorded, including certification of bills etc.

12.0 EXIM Bank has the right to delete items, reduce or increase the scope of work with mutually agreed terms and condition.

13.0 Notices to local bodies:

The Service Provider shall comply with and give all notices required under any law, rule, regulations or bye laws of parliament, state legislature or local authority relating to works.

14.0 I / We hereby declare that I / We have read and understood the above instructions for the guidance of the Tenderers. Seal and Signature of the Bidder/s not required since the document is digitally signed.

Bill of Material

S.No	Service	Cost Type	Quantity	Cost for 1st Year (INR)	Cost for 2nd Year (INR)	Cost for 3rd Year (INR)	Cost for 4th Year (INR)	Cost for 5th Year (INR)	Remarks
1	SOC preparedness, Gap Analysis and SIEM implementation cost	One time	1		NA	NA	NA	NA	
2	SIEM Tool License cost and SOC Operation and Monitoring (Offsite) 24x7. (The solution has to be deployed in banks premises).	Yearly (Opex Model)	1						
3	One L 2 Resource deployed onsite	Yearly	1						
4	VAPT Charges	Yearly	1						
5	Anti-Phishing , Anti-Trojan, Anti-malware and Anti-Rouge services (For 5 websites)	Yearly	1						
6	Security Intelligence services	Yearly	1						
		Total Cost							

Notes: -

a) Hardware will be provided by the Bank.

b) The rates quoted in commercial bid should be exclusive of all taxes.

c) For One L2 Resource, the payment will be released on monthly basis.

d) The Bank is having a right to terminate contract with one month notice period. Similarly, the vendor has to give one month notice period in case the vendor would like to terminate the contract.

e) No Advance payment will be made on any services.

ANNEXURE

PRE CONTRACT INTEGRITY PACT

General

This pre-bid pre-contract Agreement (hereinafter called the Integrity Pact) is made on _____day of the _____month of 2019, between, on one hand, the President of India acting through Shri Dharmendra Sachan (General Manager), Export-Import Bank of India, Ministry of Finance, Government of India (hereinafter called the "BUYER", which expression shall mean and include, unless the context otherwise requires, his successors in office and assigns) of the First Part and is represented by Shri_____ (hereinafter called the "Seller" which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

WHEREAS the **BUYER** proposes to procure (Name of the Stores/Equipment/Item) and the BIDDER/Seller is willing to offer/has offered the stores and

WHEREAS the **BIDDER(s)** is a private company/public company/Government undertaking/partnership/registered export agency, constituted in accordance with the relevant law in the matter and the BUYER is a General Manager, Export-Import Bank of India, Ministry of Finance performing its functions on behalf of the President of India.

NOW, THEREFORE,

To avoid all forms of corruption by following a system that is fair, transparent and free from any influence/prejudiced dealings prior to, during and subsequent to the currency of the contract to be entered into with a view to: -

Enabling the **BUYER** to obtain the desired said stores/equipment at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement, and

Enabling **BIDDER(s)** to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the BUYER will commit to prevent corruption, in any form, by its officials by following transparent procedures.

The parties hereto hereby agree to enter into this Integrity Pact and agree as follows:

1. Commitments of the BUYER:

1.1 The BUYER undertakes that no official of the BUYER, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favor or any material or immaterial benefit or any other advantage from the BIDDER, either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the contract.

1.2 The BUYER will, during the pre-contract stage, treat all BIDDER(s) alike, and will provide to all BIDDER(s) the same information and will not provide any such information to any particular BIDDER which could afford an advantage to that particular BIDDER in comparison to other BIDDERs.

1.3 All the officials of the BUYER will report to the appropriate Government office to avoid any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.

2. In case any such preceding misconduct on the part of such official(s) is to be reported by the BIDDER to the BUYER with full and verifiable facts and the same is prima facie found to be correct by the BUYER, necessary disciplinary proceedings, or any other action as deemed

fit, including criminal proceedings may be initiated by the BUYER and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the BUYER the proceedings under the contract would not be stalled.

3. Commitments of BIDDERS

The BIDDER commits himself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its bid or during any pre-contract or post-contract stage in order to secure the contract or in furtherance to secure it and in particular commit himself to the following: -

3.1 The BIDDER will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favor, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER, connected directly or indirectly with the bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

3.2 The BIDDER further undertakes that they have not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favor, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Government for showing or forbearing to show favor or disfavor to any person in relation to the contract or any other contract with the Government

3.3 BIDDERs shall disclose the name and address of agents and the representatives and Indian BIDDERs shall disclose their foreign principals or associates.

3.4 BIDDERs shall disclose the payments to be made by them to agents/brokers or any other intermediary, in connection with this bid/contract.

3.5 The BIDDER further confirms and declares to the BUYER that the BIDDER is the original manufacturer/integrator/authorized government sponsored export entity of the defense stores and has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or in any way to recommend to the BUYER or any of its functionaries, whether officially or unofficially to the award of the contract to the BIDDER, nor has any amount been paid, promised or intended to be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.

3.6 The BIDDER, either while presenting the bid or during pre-contract negotiations or before signing the contract, shall disclose any payments he has made, is committed to or intends to make to officials of the BUYER or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.

3.7 The BIDDER will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract.

3.8 The BIDDER will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

3.9 BIDDER shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the BUYER as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The BIDDER also undertakes to exercise due and adequate care lest any such information is divulged.

3.10 The BIDDER commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

3.11 The BIDDER shall not instigate or cause to instigate any third party/ person to commit any of the actions mentioned above.

3.12 If the BIDDER or any employee of the BIDDER or any person acting on behalf of the BIDDER, either directly or indirectly, is a relative of any of the officers of the BUYER, or alternatively, if any relative of an officer of the BUYER has financial interest/stake in the BIDDER's firm, the same shall be disclosed by the BIDDER at the time of filing of tender. The term 'relative' for this purpose would be as defined in Section 6 of the Companies Act 1956. The BIDDER shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the BUYER.

4. Previous Transgression

4.1 The BIDDER declares that no previous transgression occurred in the last three years immediately before signing of this Integrity Pact, with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Enterprise in India or any Government Department in India that could justify BIDDER's exclusion from the tender process.

4.2 The BIDDER agrees that if it makes incorrect statement on this subject, BIDDER can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reasons.

5. Earnest Money (Security Deposit)

5.1 While submitting commercial bid, the BIDDER shall deposit an amount as Earnest Money/Security Deposit, with the BUYER through any of the following instruments:

(i) Demand Draft or a Bankers' Cheque in favor of M/s. Export –Import Bank of India.

(ii) A confirmed guarantee by an Indian Nationalized Bank, promising payment of the guaranteed sum to the BUYER on demand within three working days without any demur whatsoever and without seeking any reasons whatsoever. The demand for payment by the BUYER shall be treated as conclusive proof of payment. No other mode or through any other instrument except mentioned here is accepted.

5.2 The Earnest Money/Security Deposit shall be valid up to a period of five years or the complete conclusion of the contractual obligations to the complete satisfaction of both the BIDDER and the BUYER, including warranty period, whichever is later.

5.3 In case of the successful BIDDER a clause would also be incorporated in the Article pertaining to Performance Bond in the Purchase Contract that the provisions of Sanctions for Violation shall be applicable for forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

5.4 No interest shall be payable by the BUYER to the BIDDER on Earnest Money/Security Deposit for the period of its currency.

6. Sanctions for Violations

6.1 Any breach of the aforesaid provisions by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER) shall entitle the BUYER to take all or any one of the following actions, wherever required: -

(i) To immediately call off the pre contract negotiations without assigning any reason or giving any compensation to the BIDDER. However, the proceedings with the other BIDDER(s) would continue.

(ii) The Earnest Money Deposit (in pre-contract stage) and/or Security Deposit/Performance Bond (after the contract is signed) shall stand forfeited either fully or partially, as decided by the BUYER and the BUYER shall not be required to assign any reason therefore.

(iii) To immediately cancel the contract, if already signed, without giving any

compensation to the BIDDER.

(iv) To recover all sums already paid by the BUYER, and in case of an Indian BIDDER with interest thereon at 2% higher than the prevailing Prime Lending Rate of State Bank of India, while in case of a BIDDER from a country other than India with interest thereon at 2% higher than the LIBOR. If any outstanding payment is due to the BIDDER from the BUYER in connection with any other contract for any other stores, such outstanding payment could also be utilized to recover the aforesaid sum and interest.

(v) To encash the advance bank guarantee and performance bond/warranty bond, if furnished by the BIDDER, in order to recover the payments; already made by the BUYER, along with interest.

(vi) To cancel all or any other Contracts with the BIDDER. The BIDDER shall be liable to pay compensation for any loss or damage to the BUYER resulting from such cancellation/rescission and the BUYER shall be entitled to deduct the amount so payable from the money(s) due to the BIDDER.

(vii) To debar the BIDDER from participating in future bidding processes of the Government of India for a minimum period of five years, which may be further extended at the discretion of the BUYER.

(viii) To recover all sums paid in violation of this Pact by BIDDER(s) to any middleman or agent or broker with a view to securing the contract.

(ix) In cases where irrevocable Letters of Credit have been received in respect of any contract signed by the BUYER with the BIDDER, the same shall not be opened.

(x) Forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

6.2 The BUYER will be entitled to take all or any of the actions mentioned at para 6.1(i) to (ix) of this Pact also on the Commission by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER), of an offence as defined in Chapter IX of the Indian Penal code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption.

6.3 The decision of the BUYER to the effect that a breach of the provisions of this Pact has been committed by the BIDDER shall be final and conclusive on the BIDDER. However, the BIDDER can approach the Independent Monitor(s) appointed for the purposes of this Pact.

7. Fall Clause

7.1 The BIDDER undertakes that it has not supplied/ is not supplying similar product/ systems or subsystems at a price lower than that offered in the present bid in respect of any other Ministry/Department of the Government of India or PSU and if it is found at any stage that similar product/ systems or sub systems was supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the BUYER, if the contract has already been concluded.

8. Independent Monitors

8.1 The BUYER has appointed Independent Monitors (hereinafter referred to as Monitors) for this Pact in consultation with the Central Vigilance Commission (Names and Addresses of the Monitors to be given).

8.2 The task of the Monitors shall be to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.

8.3 The Monitors shall not be subject to instructions by the representatives of the parties and perform their functions neutrally and independently.

8.4 Both the parties accept that the Monitors have the right to access all the documents

relating to the project/procurement, including minutes of meetings.

8.5 As soon as the Monitor notices, or has reason to believe, a violation of this Pact, he will so inform the Authority designated by the BUYER.

8.6 The BIDDER(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the BUYER including that provided by the BIDDER. The BIDDER will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractors. The Monitor shall be under contractual obligation to treat the information and documents of the BIDDER/Subcontractor(s) with confidentiality.

8.7 The BUYER will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the parties. The parties will offer to the Monitor the option to participate in such meetings.

8.8 The Monitor will submit a written report to the designated Authority of BUYER/Secretary in the Department within 8 to 10 weeks from the date of reference or intimation to him by the BUYER / BIDDER and, should the occasion arise, submit proposals for correcting problematic situations.

9. Facilitation of Investigation

In case of any allegation of violation of any provisions of this Pact or payment of commission, the BUYER or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER and the BIDDER shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

10. Law and Place of Jurisdiction

This Pact is subject to Indian Law. The place of performance and jurisdiction is the seat of the BUYER.

11. Other Legal Actions

The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

12. Validity

12.1 The validity of this Integrity Pact shall be from date of its signing and extended up to 5 years or the complete execution of the contract to the satisfaction of both the BUYER and the BIDDER/Seller, including warranty period, whichever is later. In case BIDQER is unsuccessful, this Integrity Pact shall expire after six months from the date of the signing of the contract.

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

The parties hereby sign this Integrity Pact at _____on _____

BUYER	**BIDDER**
Mr. Dharmendra Sachan	Mr./Ms._____
General Manager	Chief Executive Officer/ MD/ Director
Export-Import Bank of India	_____
Ministry of Finance	
Witness	Witness
1. _____	1. _____
2. _____	2. _____

- Provisions of these clauses would need to be amended/ deleted in line with the policy of the BUYER in regard to involvement of Indian agents of foreign suppliers.