EXIM BANK
EXPORT-IMPORT BANK OF INDIA

E-Tender for

PROCUREMENT OF PRIVILEGED IDENTITY MANAGEMENT (PIM) TOOL

Head Office:

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

GENERAL TENDER DETAILS

Tender Document for	Procurement Of Privileged Identity Management Tool
Tender Reference No.	IT/EXIM/RFP/2018-19/038
Tender Document Cost	₹5,000/- (Non-refundable) (DD in favour of "Export-Import Bank of India" payable at
EMD Amount	₹1,00,000/-(DD in favour of "Export-Import Bank of India" payable at Mumbai)
Last date for acceptance of Tender document cost and EMD Amount	25-Jan-2019 02:00 PM (DD to be submitted(Both Tender Fee and EMD) 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	04-Jan-2019 05:00 PM
Document Downloading Start Date	04-Jan-2019 05:00 PM
Document DownloadingEnd Date	25-Jan-2019 02:00 PM
Tender Clarification End Date	23-Jan-2019 06:00 PM
Last Date and Time For Submission	25-Jan-2019 04:00 PM
Opening Of Tender	25-Jan-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

The Bank has deployed various applications across its network for various usage. These applications along with database are being managed internally by Bank's own /Outsourced team. The administrator/Super user password is also maintained and changes as per Bank's guidelines. Bank is also following change management process for any change in server/application/database.

At present the password policy across all servers is not uniform and is being applied as per the administrator managing the server. Further, changes which require root/admin access, is being given to different users and the changes being performed by admin users are not being logged.

The purpose of this RFP is to procure a Privileged Identity Management (PIM)/ Privilege Access Management (PAM)/ Privilege User Management (PUM) Tool for automated monitoring of all User activities across EXIM Bank devices which would function as a Centralized authentication and authorization system with best security practices along with role based access control for all servers.

The tool will monitor the user activity in case any change is being done by super user/user and will store the super user logs for verifying the activities being carried out by them. It would ensure better user management across various servers by applying restrictions on user profile as per role which can be changed on immediate basis.

Scope of Work

The scope of work includes the following components

The solution will be installed at the Data Center with High Availability (HA) mode.

The policies if applied should get replicated immediately across all PIM servers and should have a feature to roll back the applied policy for group admins.

The solution should have capability of integrating all devices irrespective of their Hardware/OS/application/Database in Bank environment. Further, in case of any upgradation of current Hardware/OS/application/Database in Bank, the same should be integrated with PIM Solution within one month. No extra cost will be paid to vendor for any customization. Vendor should provide and implement all feature upgrades or version upgrades during contract period without any cost. There should be Maker-Checker feature available in case any configuration/policy change is being done by any user.

Vendor should provide support to plug out any vulnerability found in the PIM solution as and when identified by Bank, as well as by the OEM. Patches made available by the OEM should be applied immediately. All vulnerabilities should be closed immediately or within 15 days of reporting the same to vendor.

The successful bidder, in coordination with the OEM must make a detailed study of Bank infrastructure and requirements relating to the solution, prepare a detailed plan document/road map mentioning all the pre-requisites, timeframe of milestones/achievements within the Completion Period leading to the full

operationalization of the solution. The vendor will provide a detailed Business Requirement Document (BRD), Solution design and Project Plan. The implementation would start only after sign-off of the documents submitted by vendor/Go-ahead from the Bank.

During the requirement analysis phase, if the bidder expresses inability to integrate any system considered critical by Bank or the PIM solution does not support any requirement, Bank may reject the process at its sole discretion without assigning any reason and without incurring any liability towards the vendor.

Technical Specifications

	Description	**Compliance (Out-of-Box) Yes or No**	**Vendor Response/Detailed Comments**
A	**Single - Sign On and Authentication Models:**		
1	The solution should have a Generic Target System Connectors to enable one to uses this connector for non-standard devices etc.		
2	The solution should be agentless i.e. does not require to install any agent on target devices		
3	The solution should support transparent connection to the target device, without seeing the password or typing it in as part of the connection		
4	The solution should support direct connections to windows, ssh, databases and other managed devices without having to use a jump server.		
5	The solution should have an inbuilt dual factor authentication for soft token, mobile OTP etc. Also it should have an inbuilt authentication for Bio-Metrics without having to acquire another biometric authentication server.		
6	The solution should be able to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including LDAP, RADIUS and a built-in authentication mechanism		
7	The solution should also provide local authentication and all the security features as per best standards.		
8	The solution should provide flexibility **user/device wise** for local authentication or enterprise authentication		
9	The solution should support an application integration framework for web based as well as .exe based applications. There should be strong out of the box support including ease of integration with any third party connectors.		

10	The solution should provide multi-tenancy feature whereby the entire operations can be carried out within a tenant or line of business.		
11	The solution should provide multi-domain feature whereby the entire operations can operate in an distributed environment		
12	The solution can restrict end-user entitlements to target accounts by location; that is, allow access only from a specified PC or range or class of PCs.		
13	The solution should be able to handle multi-location architecture or distributed architecture with seamless integration at the User Level. For example: Multiple datacenter may have multiple secondary installations but the primary installation will also simultaneously work for all users and all locations		
B	**Shared Account Password Management**		
1	The solution shall perform password change options which is parameter driven		
2	The solution should set password options every x days, months, years and compliance options via the use of a policy		
3	Ability to create exception policies for selected systems, applications and devices		
4	The solution should enable an administrator to define different password formation rules for target accounts on different target systems and supports the full character set that can be used for passwords on each target system.		
5	The solution enables an administrator to change a target-account password to a random value based on a manual trigger or automatic schedule.		
6	Allow single baseline policy across all systems, applications and devices (e.g. one single update to enforce baseline policy		
7	The solution should support changing a password or group of passwords according to a policy (time based or 'on-demand')		
8	Ability to generate 'One-time' passwords as an optional workflow		
9	Ability to send notifications via email or other delivery methods triggered by any type of activity		
10	Ability to send notification via email to the user requesting the password that checkout is complete		
11	Flexibility that allows exclusivity for password retrieval or multiple users checking out the same password for the same device in the same time period.		
14	All locally stored target-account passwords should encrypted using AES or similar encryption with at least 256 bit keys.		
15	The solution should automatically reconcile passwords that are detected 'out of sync' or lost without using external restore utilities		

16	The solution should have the ability to reconcile passwords manually, upon demand		
17	The solution should automatically verify , notify and report all passwords which are not in sync with PIM		
18	The solution should have the ability to automatically "check-out" after a specific time and "check-in" within a specified time.		
19	The solution should set unique random value anytime a password is changed. The password generated should be strong and should not generate a similar value for a long iteration.		
20	The tool allows secure printing of passwords in Pin Mailers. Lifecycle of printing and labelling of envelopes should be part of the module.		
21	The solution should be able to control re-prints with adequate authorization		
22	Secured Vault platform - main password storage repository should be highly secured (built-in firewall, hardened machine, limited and controlled remote access etc.)		
23	The proposed solution should restrict the solution administrators from accessing or viewing passwords or approve password requests		
24	The solution should have the capability to seamlessly change the passwords for the large number of desktops. It should be able to handle floating IPs		
C	**Access Control**		
1	The solution should be able to restrict usage of critical commands over a SSH based console based on any combination of target account, group or target system and end-user.		
2	The solution should restrict privileged activities on a windows server (e.g. host to host jumps, cmd/telnet access, application access, tab restrictions) from session initiated with PIM		
3	The solution should be able to restrict usage of critical commands on command line through SSH clients on any combination of target account, group or target system and end-user.		
4	The solution should be able to restrict usage of critical commands on tables for database access through SSH, SQL+ (client/), front-end database utilities on any combination of target account, group or target system and end-user.		
5	The solution should provide for inbuilt database management utility to enable granular control on database access for Sql, my Sql, DB2, Oracle etc.		
6	The solution enables an administrator to restrict a group of commands using a library and define custom commands for any combination of target account, group or target system and end user.		

7	The solution should provide secure mechanism for blacklisting/whitelisting of commands for any combination of target account, group or target system and end user.		
8	The solution can restrict user-specific entitlements of administrators individually or by group or role.		
9	The solution should have workflow control built-in for critical administrative functions over SSH including databases (example user creation, password change etc.) and should be able to request for approval on the fly for those commands which are critical.		
10	The solution can restrict target-account-specific entitlements of end users individually or by group or role.		
11	The solution can restrict end-user entitlements to target accounts through a workflow by days and times of day including critical command that can be fired.		
12	The solution should provide for a script manager to help in access controlling scripts and allow to run the scripts on multiple devices at the same time.		
13	System should be able to define critical commands for alerting & monitoring purpose and also ensure user confirmation (YES or NO) for critical commands over SSH.		
D	**Privileged Session Management and Log Management**		
1	The solution should be able to support an session recording on any session initiated via PIM solution including servers, network devices, databases and virtualized environments.		
2	The solution should be able to **log commands** for all commands fired over SSH Session and for database access through ssh, sql+		
3	The solution should be able to log/search text commands for all sessions of database even through the third party utilities		
4	The solution should be able to log/search text commands for all sessions on RDP		
5	The solutions should support selective option for enabling session based recording on any combination of target account, group or target system and end-user.		
6	All logs created by the solution should be tamper proof and should have legal hold		
7	The solution logs all administrator and end-user activity, including successful and failed access attempts and associated session data (date, time, IP address. Machine address, BIOS No and so on). The tool can generate — on-demand or according to an administrator-defined schedule — reports showing user activity filtered by an administrator, end user or user group.		
8	The tool can restrict access to different reports by administrator, group or role.		
9	The tool generates reports in at least the following formats: HTML, CSV and PDF		

10	System should be able to define critical commands for alerting & monitoring purpose through SMS or Email alerts		
11	The solution should provide separate logs for commands and session recordings. Session recordings should be available in image/ video based formats		
12	The session recording should be SMART to help jump to the right session through the text logs		
13	Secure and tamper-proof storage for audit records, policies, entitlements, privileged credentials, recordings etc.		
14	The proposed solution shall cater for live monitoring of sessions and manual termination of sessions when necessary		
15	The proposed solution shall allow a blacklist of SQL commands that will be excluded from audit records during the session recording. All other commands will be included.		
16	The proposed solution shall enable users to connect securely to remote machines through the tool from their own workstations using all types of accounts, including accounts that are not managed by the privileged account management solution.		
17	The proposed solution shall allow configuration at platform level to allow selective recording of specific device.		
18	The proposed solution shall allow specific commands to be executed for RDP connections (e.g. Start the connection by launching a dedicated program on the target machine without exposing the desktop or any other executables).		
19	The proposed solution shall support correlated and unified auditing for shared and privileged account management and activity.		
21	The proposed system shall support full colour and resolution video recording.		
22	The proposed system shall support video session compression with no impact on video quality.		
E	**PIM Security**		
1	The solutions should use minimum FIPS 140-2 validated cryptography for all data encryption.		
	The Solution should be TLS 1.2 and SHA-2 compliant		
2	All communication between system components, including components residing on the same server should be encrypted.		
3	All communication between the client PC and the target server should be completely encrypted using secured gateway. (Example: a telnet session is encrypted from the client PC through the secured gateway)		
4	The Administrator user cannot see the data (passwords) that are controlled by the solution.		
5	Secured platform - main password storage repository/Vault should be highly secured (hardened machine, limited and controlled remote access etc.).		

6	The solution should secure master data, records, entitlement, policy data and other credentials in tamper proof storage container.		
F	**PIM Administration**		
1	The solution should have central administration web based console for unified administration.		
2	The tool uses Active Directory/LDAP as an identity store for administrators and end users.		
3	The tool enables an administrator to define groups (or similar container objects) of administrators and end users.		
4	The tool enables an administrator to add an administrator or end user to more than one group or to add a group to more than one super group.		
5	The tool enables an administrator to define a hierarchy of roles without limit.		
6	Administrative configurations (e.g. configuration of user matrix) shall be accessible via a separate client where client access is controlled by IP address.		
7	Important configuration changes in the solutions (example changes to masters) should be based on at least 5 level workflow approval process and logged accordingly		
8	Segregation of Duties - The Administrator user cannot view the data (passwords) that are controlled by other teams/working groups (UNIX, Oracle etc.).		
9	The solution should provide for self-service portal for users and devices for ease of on boarding both users and devices.		
10	All administrative task should be done LOB wise i.e. Line of Business Wise		
11	The solution should have Auto-Onboarding Feature for both User and Devices without having to do any manual activity.		
G	**System Architecture**		
1	The solution architecture should be highly scalable both vertically as well as horizontally.		
2	The proposed solution shall provide multi-tier architecture where the database and application level is separated.		
3	The solution should work at the network layer instead through a jump server. This will have achieve large number of sessions.		
4	The proposed solution shall provide scalability where it is not limited by the hardware. Also the solution shall provide modular design for capacity planning and scalability metrics.		
5	The proposed solution shall have the ability to support multiple mirrored systems at offsite Disaster Recovery Facilities across different data centre locations.		
6	The proposed solution shall have built-in options for backup or integration with existing backup solutions		

7	The proposed solution shall handle loss of connectivity to the centralized password management solution automatically.		
8	The proposed solution shall not require any network topology changes in order to ensure all privileged sessions are controlled by the solution.		
9	The proposed solution shall support distributed network architecture where different segments need to be supported from a central location.		
10	The proposed solution shall support both client based (in the case where browser is not available) as well as browser based administration		
11	The proposed solution should be 100% agentless that includes password storage, password management and session recording features.		
12	The solution must support parallel execution of password resets for multiple concurrent requests.		
13	The solution should provide fully failover from a single active instance to a backup/standby instance with a fully replicated repository		
14	The solution should support multiple active instances with load balancing and fully automatic failover to another active instance		
15	The solution if required should be available to install on a virtual sever		
16	The system should be highly available (24x7x365) and redundant from a hardware failure, application failure, data failure, and or catastrophic failure. Please elaborate		
17	The solution should have an ability to have direct connection to target device as well as using secured gateway channel.		
H	**Out of box Integration**		
1	Ability to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including AD, LDAP, Windows SSO, PKI, RADIUS and a built-in authentication mechanism.		
2	Ability to integrate with Bio-Metric Solutions		
3	Ability to integrate with Hard and Soft token solutions		
4	Ability to integrate with ticketing systems.		
5	Ability to integrate with Automation software for enhancing productivity in the data center		
6	The proposed solution supports integration with the Hardware Security Module (HSM) devices to store the encryption keys.		
I	**Ticketing System integration**		
1	The solution can force the requestor of password / session to provide a reason, including a service desk incident ticket number, for the request.		
2	The solution can communicate with a workflow engine to verify an incident ticket number cited in the end user's request.		

3	The solution provides the capability to enable end users to retrieve (or reset) a target-system password only after approval by a designated approver (to allow dual control). Approval criteria can be based on any combination of target account, group or target system and end-user identity, group or role, as well as contextual information such as day of the week or time of day.		
4	Ability to enforce ticketing integration as well as approval workflow for specific ticket types (e.g. change/incident ticket)		
5	Inbuilt ticketing system with 5 level workflow approval with ticket level validation, risk and impact assessments as per LOB wise, Service type and user type. This ticketing system to help in creating a work order on an executer, who will then request for the access through the request workflow with this valid ticket		
J	**SIEM Integration**		
1	The solution should be able to integrate with leading SIEM Solutions.		
2	The solution should be able to integrated with applications like VA Systems, performance monitoring applications to eliminate hard coded passwords		
K	**Application Password Management (Hard-Coded Password Management)**		
1	The solution should have an ability to eliminate, manage and protect privileged credentials in applications, scripts, configuration files etc.		
2	The solution should be able to authenticate and trust the application requesting the privileged password based on various authentication methods		
3	Application Servers Support - The product should support removing static hard coded passwords from Data Sources in Application Servers. Please elaborate.		
L	**Auto Discovery of Privileged Accounts**		
1	The solution should be able to perform auto discovery of privileged accounts on target systems and perform two way reconciliation.		
2	The solution should provide feature for user governance on the target devices i.e. auto detect users and schedule a governance workflow and user certification process with adequate review process.		
3	Map privileged and personal accounts on various target systems		
4	Ability to quickly identify all non-built-in local administrator accounts in your environment (flag possible 'backdoor' accounts)		

5	Ability to quickly identify private and public SSH keys, including orphaned SSH keys, on Unix/Linux machines, extracts key related data and ascertain the status of each key		
M	**Notification Engine**		
1	The solution should have capability to provide alerts and notification for critical PIM events over SMS & Email		
2	The solution should have capability to provide alerts and notification for all administration/configuration activities over SMS & Email		
3	Customizable notification for command executed on SSH and Telnet based devices		
4	Customizable notification for command/Process executed on Windows		
5	Notification on target being access on criteria like Line of Business or Groups		
N	**Solution Workflow**		
1	The solution should have inbuilt workflow to manage		
2	Electronic Approval based Password Retrieval		
3	Onetime access / Time Based / Permanent Access		
4	5 level approval workflow with E-mail and SMS notification with delegation rules		
5	Ability to provide for delegation at all levels in the workflow		
6	Mobile device support - ability to send a request to access a password, approve the request and retrieve the password, all from a hand-held mobile device e.g. smart phones		
7	Supports a workflow approval process that is flexible to assign multiple level of approvers based on product or model (i.e. require 2 or more approvals before access is allowed).		
8	Supports a workflow approval process that requires approvers to be in sequence before final approval is granted.		
9	Ability to log workflow processes and/or have the ability to be reported or audited.		
O	**Dashboard & Reporting**		
1	Dashboard Capabilities should include real-time view of activities performed by the administrators		
2	The system shall have the ability to run all reports by frequency, on-demand and schedule.		
3	The solution should provide detailed and scheduled reporting with the following basic report sets Entitlements Reports, User's activities, Privileged Accounts inventory and Activities log		

4	The solution should have ability to report on all system administrative changes performed by PIM Administrators with relevant auditable records		
5	The solution should be able to report password lockouts (failure logon attempts)		
6	Ability to report password checkouts on systems and users requesting passwords		
7	Ability to report password lockouts (failure logon attempts)		
8	Ability to report on password change following verification process		
9	Ability to report on password status		
10	Reports should be customizable		
11	Audit data can be exported for use for any BI Tool		
12	Reports shall be automatically distributed by email		
13	Access to audit reports (and report configuration) shall be restricted to "auditor" end-users		
14	Ability to replay actual session recordings for forensic analysis		
15	Dashboard - for at a glance critical events and password policies.		

ELIGIBILITY CRITERIA OF THE BIDDER

S.No.	ELIGIBILITY CRITERIA	SUPPORTING DOCUMENTS TO BE SUBMITTED	COMPLIANCE (YES/NO)
1	The bidder should be registered with Registrar of companies/firms in India for at least 3 years.	Certificate of incorporation or any other certificate of registration issued by competent authority from Government of India.	
3	Bidder must have ISO 9001: 2013 or higher certified company	ISO 9001: 2013 or higher certificate	
4	The solution should be successfully implemented in at least 5 PSU Banks in India.	P.O. or reference letter needed to submit as a reference.	
5	The bidder should have Support center/authorized office in Mumbai. The OEM should have office and direct support center in India.	Undertaking to be submitted	
6	The bidder should be the Original Equipment Manufacturer (OEM) or the authorized representative in India.	The bidder on their company's letter head shall provide self-declaration about OEM status. In case of authorized representative, MAF from OEM as per Annexure-1 in their letter Head needs to be provided.	

8	The bidder should have a minimum turnover of INR 10 crores (Rupees Ten crores) per annum for the past 3 financial years i.e. 2017-18, 2016-17, 2015-16 from their Indian operations. The bidder should have positive net worth during the last three financial years.	Provide CA Certificate. The CA certificate provided in this regard should be without any riders.	
9	The bidder should not be involved in any litigation which threatens solvency of company.	Certificate is to be provided by the chartered accountant/statutory auditor.	
10	Bidder shall execute E-Tendering Process Compliance Statement and Undertaking letter as per Annexure	Upload seal and signed copy of Annexure -2 and Annexure -3	
11	Integrity Pact Agreement (IPA) to be executed.	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 sent to Exim Bank, Head Office, Mumbai.	

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: **Procurement of Privileged Identity Management Tool**

Ref. No: **IT/EXIM/RFP/2018-19/038**

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 (Title No. 7) 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 not duly 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' price validity.

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**) with Exim Bank within 10 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 without the Service Provider claiming any compensation for the reduction in the scope of work.

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.	Items	Unit Cost (a)	Multiplication Factor (b)	Total Cost (c=a*b) (exclusive of all taxes)
A	License Cost for IP		**150**	
B	License Cost for User		**50**	
C	Implementation Cost (including Integration)			
D	ATS of solution per year applicable after expiry of warranty) (range Minimum 10%- Maximum 20% of (A+B)			
			Total	**A+B+C+D**

Notes: -

a) Hardware, Database and O/S will be provided by the Bank.

b) The rates quoted in commercial bid should be exclusive of all taxes. However, Taxes, if any including GST shall be paid to the bidder on actual basis at the rate applicable. The rate of applicable GST should be informed and charged separately in the invoice generated for supply of the product.

c) The vendor will provide services for implementation / rolling-out /support / maintenance of proposed solution for a minimum period of 5 years (3 years warranty + 2 years ATS) from Go Live date with option of further extension of contract for another 2 years at the same rate, provided services of the bidder is satisfactory and at Bank's sole discretion. Bank reserves right to cancel the contract at any time in case system fails to meet any of the requirements as mentioned in the e-tender.

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.