बैंक ऑफ महाराष्ट्र
Bank of Maharashtra
भारत सरकार का उद्यम
एक परिवार एक बैंक

CORRIGENDUM
Please refer to RFP 032021 published on **24.08.2021** inviting proposal from eligible bidders for **Supply, Installation, and Maintenance of Security Solutions.** The corrigendum for change in timelines of Technical Bid Submission and amendment in clauses are available on Bank's website https://www.bankofmaharashtra.in in the Tenders Section. **Deputy General Manager** **Information Technology Department**

बैंक ऑफ महाराष्ट्र
Bank of Maharashtra
भारत सरकार का उद्यम
एक परिवार एक बैंक

12.10.2021

CORRIGENDUM

Please refer to RFP 032021 published on **24.08.2021** inviting bids for **Supply, Installation, and Maintenance of Security Solutions.**

Following correction be read in the tender document.

1. Change in timelines for Bid submission enclosed in Annexure – I.
2. Amendment in clauses in RFP. The amendments are enclosed as Annexure-I.

The online bid submission will be through E-Procurement Technologies Ltd. (URL - https://eauction.auctiontiger.net/EPROC/). Bidder manual is also available on the same site.

(Shirish Salway)
Deputy General Manager
Information Technology Department

Annexure I

1. **Page No. 12: Invitation to the Tender :**

Important Information regarding Bid Submission

RFP Term/Clause no. Invitation of the Tender	As per previous Timelines	Revised Timelines
Last Date for Submission of Bid	20.10.2021 14:00 Hrs	26.10.2021 14:00 Hrs
Time and Date for Opening of Technical Bid	20.10.2021 16:00 Hrs	26.10.2021 16:00 Hrs

Note:- Except above clause, there is no other change in information regarding Bid submission date.

2. **Amendment in clauses in RFP:**

S. No.	Page	Point / Clause	Clarification point as stated in the tender document	Modified Clause
1	152	eligibility Criteria	The bidder should have experience of implementation of similar technology implemented on premises mode under RFP in at least 2 companies from BFSI Sector. In which one should be implemented with minimum Endpoints/Devices/ Database instances (DLP – 7500, DICT – 7500, DAM-100, EE-750, PMS-7500, EDR-7500, FRA – Minimum 4 Firewall, SSLO – No minimum count, but experience for implementation should be in line with technical specification.) In case Bidder is bidding for multiple solutions, the above clause would be separately applicable for each of the solution	Please read clause as " The bidder should have experience of implementation of similar technology implemented on premises mode under RFP in at least 2 companies from BFSI Sector. In which one should be implemented with minimum Endpoints/Devices/ Database instances (DLP – 4000, DICT – 4000(DLP experience will be considered) , DAM-60, EE-500, PMS- 4000, EDR-4000, FRA – Minimum 4 Firewall, SSLO –ADC Platform Experience will be considered.) In case Bidder is bidding for multiple solutions, the above clause would be separately applicable for each of the solution."
2	132	51	The solution should be integrated with Active Directory or LDAP to help manage and enforce user policies.	Please read the caluse as " The solution should provide integration with Active Directory or LDAP or should have built-in AAA for authentications to Management Console and to help enforce policies based on group.

S. No.	Page	Point / Clause	Clarification point as stated in the tender document	Modified Clause
3	154	Annexure 5: Eligibility Criteria Compliance	The OEM should have been in existence for a minimum period of 3 years in India as on 31-July-2021	Please read the clause as "The OEM should have been in existence for a minimum period of 3 years in India which will be validated at the time of awarding the contract."
4	120	10 /Architecture Requirements	The solution must support the following OS, However for OS like Unix /Solaris/HPUX/IBM AIX/VMware ESXI OS which are OEM dependent Patching, The solution should support custom patch deployment using agentless or Script Based patching and must provide centralized reporting with compliance.: Microsoft Windows i) Windows 7 / Windows 8 / Windows 8.1 / Windows 10 (All versions and x86 -x64 bit architecture) and latest Endpoint OS released by Microsoft time to time ii) Windows 2008 / 2012/ 2016 / 2019 (All Versions and x86 -x64 bit architecture) and latest server OS released by Microsoft time to time IBM AIX Linux - (x86 -x64 bit architecture) i) Red Hat (Desktop, Enterprise) ii) Fedora iii) SUSE iv) CentOS v) Ubuntu Virtualization i) Vmware and ESXI Server ii) Hyper-V	Please read the clause as "The solution must support the following OS: a. **Microsoft Windows** i) Windows 7 / Windows 8 / Windows 8.1 / Windows 10 (All versions and x86 -x64 bit architecture) and latest Endpoint OS released by Microsoft time to time ii) Windows 2008 / 2012/ 2016 / 2019 (All Versions and x86 -x64 bit architecture) and latest server OS released by Microsoft time to time b. **Linux - (x86 -x64 bit architecture)** i) Mandatory OS Support - Red Hat (Desktop, Enterprise) ii) Additional OS Support (Optional) - Fedora, SUSE, Cent OS, Ubuntu **Note :** For Out of support OS (like Windows 7, Windows Server 2008 and Older versions of RHEL OS) - Solution should support the deployment of Older patches released by OEM and custom package (MSI and EXE) package deployement through Solution."
5	104	192	The DLP solution should support as an API be able to provide the risk adaptive based protection by dynamically calling the action plan based on the Risk.	Clause is removed
6	87	14	The solution should Support PrtSc blocking on endpoint when configurable list of specific application are running, no matter it is in the foreground or background. The actual PrtSc capture will also be submitted to the DLP system as forensic evidence.	Please read the clause as " The proposed solution should be able to block PrtSC on sensitive data"

S. No.	Page	Point / Clause	Clarification point as stated in the tender document	Modified Clause
7	92	52	The DLP Solution must provide visibility into Broken Business process. For ex:-if unsecured sensitive content is sent daily from several users to a business partner, the users are probably not aware that they are doing something wrong	Please read the clause as "The Propsed solution should have capability to identify sensitive data shared on daily basis"
8	100	146	Proposed solution should inspect data leaks over HTTP , HTTPs and SMTP User client like Outlook and Lotus Notes. The solution should be able to inspect HTTP traffic and HTTPs traffic natively. Should provide support both build-in SSL decryption and destination awareness capability with integration with Network and Gateway DLP controls.	Please read the clause as "Proposed solution should inspect data leaks over HTTP , HTTPs and SMTP User client like Outlook, Lotus Domino etc. The solution should be able to inspect HTTP traffic and HTTPs traffic. "
9	100	138	Proposed Solution should be able to detect and protect for the low volume data leaks over the Network.	Please read the clause as " The proposed solution should be able to identify and prevent the sensitive data leakage over the network as per policy defined in DLP"
10	100	139	Proposed Solution should be able to do full binary fingerprint of files and also should be able to detect even if partial information gets leaks from fingerprinted files or folders	Please read the clause as " The proposed solution should be able to identify and prevent the sensitive data leakage from fingerprinting of file and data"
11	100	142	Proposed solution should enforce policies to detect low and slow volume data leaks over the period for max 7 days.	Please read the clause as " The proposed solution should be able to identify and prevent the sensitive data leakage over the network as per policy defined in DLP"
12	100	143	The solution should able to detect the data leaks over to competitors and the data sent and uploaded after the office hours predefined patterns.	Please read the clause as " The proposed solution should be able to identify and prevent the sensitive data leakage over the network as per policy defined in DLP"
13	100	144	Proposed Solution should have advanced Machine Learning – Ability to automatically learn sensitive information from copies of information that needs to be protected and automatically learn false positives.	Please read the clause as "Proposed solution should have advanced machine learning/Capture feature enables to learn and analyze sesitive information that needs to be protected and help to reduce false positive

S. No.	Page	Point / Clause	Clarification point as stated in the tender document	Modified Clause
14	98	122	Proposed Solution should have the ability to suggest or enforce classification and digital rights management protection for end users in real-time.	Clause is removed
15	86	4	Proposed solution should be able to monitor and protect data classifiers created in via the Fingerprinting of the structured and unstructured, it need to be synched to all the Network DLP channels and to Endpoint Channel.	Please read the clause as "Proposed solution should be able to monitor and protect data classifiers created in via the Fingerprinting of the structured and unstructured, it need to be synched to all the Network DLP channels and / or to Endpoint Channel."
16	93	59	Proposed solution should enforce fingerprinting policy on both network and endpoint channel, even when the endpoint is off network by custom data classifier where customer can use in compound with any existing data classifier to identify sensitive data which is unique to the Bank	Please read the clause as "The Proposed solution should enforce fingerprinting policy on network and / or endpoint channel, even when the endpoint is off network by custom data classifier where customer can use in compound with any existing data classifier to identify sensitive data which is unique to the Bank"
17	129	5	The proposed solution must be able to analyse and report all files using MD5, SHA1, and SHA 256 hash methods	Please read clause as " The proposed solution must be able to analyse and report all files using folowing methods : a) Mandatory Hash Methods - MD5 and SHA 256 b) Additional Hash Method (optional) - SHA1
18	130	26	The solution should support agent capping for CPU and memory utilization.	Please read clause as " The solution should support agent capping (CPU and memory utilization) or optimal resource utilization.
19	131	42	The solution must allow grouping of endpoints into host sets based on distinguishing attributes. It must also be able to identify and label high-value hosts.	Please read clause as " The solution must allow grouping of endpoints into host sets based on distinguishing attributes"
20	131	45	Solution should be able to detect , respond & block (Automatic & Manual) to malicious payload ,process identified based on behaviour analysis.	Please read clause as " Solution should be able to detect & respond to malicious payload identified based on behaviour analysis.Blocking fuctionality will be added advantage and accordingly preference will be given."

S. No.	Page	Point / Clause	Clarification point as stated in the tender document	Modified Clause
21	131	46	The solution must be able to automatically detect ,respond & block (Automatic & Manual) to exploited applications along with payload information .The same should also to be notified to user.	Please read clause as "The solution must be able to automatically detect & respond to exploited applications along with payload information .The same should also to be notified to user. pabilities to detect and respond to Zero-Day exploits & hash banning functionality.Blocking fuctionality will be added advantage and accordingly preference will be given."
22	134	68	Solution should have the capability to detect ,respond & block (Automatic & Manual) the Zero-day exploits.	Please read clause as "The solution should have built-in capabilities to detect and respond to Zero-Day exploits & hash banning functionality.Blocking fuctionality will be added advantage and accordingly preference will be given."
23	135	76	The solution should have built-in capabilities to detect,respond & & block (Automatic & Manual) to Zero-Day exploits & hash banning functionality	Please read clause as "The solution should have built-in capabilities to detect and respond to Zero-Day exploits & hash banning functionality.Blocking fuctionality will be added advantage and accordingly preference will be given."

Deputy General Manager
Information Technology Department