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

CORRIGENDUM

Please refer to RFP 102020 published on **30.07.2020** inviting proposal from eligible bidders for **Supply, Installation, and Maintenance of Information Security Solutions Endpoint Detection and Response (EDR), Firewall Rule Analyser(FRA), Web Application Firewall (WAF) & Deception Solutions.** The corrigendum & reply to pre-bid queries are available on Bank's website https://www.bankofmaharashtra.in in the Tenders Section.

Chief Information Security Officer
Integrated Risk Management Department

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

31.08.2020

CORRIGENDUM

Please refer to RFP 102020 published on **30.07.2020** inviting bids for **Supply, Installation, and Maintenance of Information Security Solutions Endpoint Detection and Response (EDR), Firewall Rule Analyser(FRA), Web Application Firewall (WAF) & Deception Solutions.**

Following correction be read in the tender document.

1. Change in timelines for Bid submission enclosed in Annexure – 1.
2. Revised Project Schedule in Annexure - 1
3. Amendment in clauses in RFP. The amendments are enclosed as Annexure-I.
4. Due to present lockdown situation arising out of outbreak of COVID-19, the bid submission mode has been changed from physical to online mode.

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

The contact details for any queries related to Profile approval/ Tender information/ online bid submission are as under:

Contact Numbers: +91-9081000427, 9904407997 (Prefer these due to Work from Home)

Sr. No.	Name	Contact Number	E-mail ID
1	Imtiyaz Tajani	079 – 6813 6831	imtiyaz@eptl.in
2	Ekta Maharaj	079 – 6813 6852	ekta.m@eptl.in
3	Salina Motani	079 – 6813 6843	salina.motani@eptl.in
4	Sujith Nair	079 – 6813 6857	sujith@eptl.in
5	Deepak Narekar	079 – 6813 6863	deepak@eptl.in
6	Jainam Belani	079 – 6813 6820	jainam@eptl.in
7	Devang Patel	079 – 6813 6859	devang@eptl.in
8	Riddhi Panchal	635-491-9566	riddhi.panchal@auctiontiger.net

(Ganesh Dabhade)
Chief Information Security Officer
Integrated Risk Management Department

Annexure I

1. **Page No. 09: 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	27-08-2020 14:00 Hrs	22-09-2020 14:00 Hrs
Time and Date for Opening of Technical Bid	27-08-2020 16:00 Hrs	22-09-2020 16:00 Hrs

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

2. **Page No. 12 Clause 2.3.1: Project Schedule**

Stage	Activity	# Weeks	Time Lines for completion
1	Submission of Detailed Project Plan including integrating all the present security solutions	2	2 weeks from the issue of Purchase Order to SI
2	Deployment of Resources at Bank's premises for Solution Proposed	8	8 weeks from the issue of Purchase Order to SI
3	Pre-Implementation Training to bank staff	2	8 weeks from the issue of Purchse Order to SI
4	Delivery of related Hardware/ Software and license and deployment of resources at bank premises	8	8 weeks from the issue of Purchase Order to SI
5	Installation and Configuration of security Hardware/ Applications in DC & DR	4	12 weeks from the issue of Purchase Order to SI
6	Integration of Installed security solution with other applicable deployed solution in Bank Environment	4	16 weeks from the issue of Purchase Order to SI
7	UAT (functional testing) of Deployed Security Solution	4	20 weeks from the deployment of resources
8	Implementation of complete solution as per RFP scope in all location	8	28 weeks from the from the deployment of resources
9	Post Implementation Training	1	Within 6 months from Date of Project Closure

3. Amendment in clauses in RFP:

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
1	14	2.3.2 Training	The training should be provided by the OEM employee and should be of minimum 3 days, 8 hours a day for each solution under this RFP	The training should be provided by the OEM employee (Certified) and should be of minimum 3 days, 8 hours a day for each solution under this RFP
2	19	Project Scope	The solution must integrate with various systems / applications in the Bank environment for monitoring and security control.	Tentative list of soluton support required for integration are mentioned under RFP technical scope .Bank existing solution specific details will be shared with succssful bidders.
3	21	EDR-Prevention & Detection	The solution must generate inventory report of managed and un-managed assets on a network.	The solution must generate inventory report of managed & un-managed assets under EDR soltion for all EDR solution supported asset available in Bank network
4	21	EDR-Prevention & Detection	The solution should gain complete visibility into all endpoints regardless of whether they are on or off the network .	The solution should gain complete visibility into all endpoints regardless of whether they are online or offline of the network .
5	21	EDR-Detection & Prevention	The solution should detect & block advanced tradecraft and activity across the kill-chain including: Exploitation, Execution, Privilege Escalation, Social Engineering, Credential Theft, Persistence, Exfiltration, Actions on Objectives, etc.	The solution should detect & respond advanced tradecraft and activity across the kill-chain including: Exploitation, Execution, Privilege Escalation, Social Engineering, Credential Theft, Persistence, Exfiltration, Actions on Objectives, etc.
6	21	EDR-Detection & Prevention	The solution should provide USB device control features leveraging same lightweight agent and offers complete visibility and control over USB storage devices including whitelisting / blacklisting and granularity like assigning read, write or execute access for them and visibility into files copied into USB storage devices.	RFP Clause removed
7	21	EDR-Detection & Prevention	The solution must have an internal protection mechanism against access and manipulation of unauthorized users.	RFP clause removed

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
8	21	EDR- Detection & Prevention	The solution must identify malicious files and prevent them from execution, including viruses, Trojans, ransomware, spyware, cryptominers and any other malware type.	The solution must identify & respond to malicious files during execution
9	21	EDR- Detection & Prevention	The EDR solution having NGAV & Integrated Sandboxing capabilities would be an added advantage.	RFP clause removed
10	21	EDR- Detection & Response	The EDR solution having the IDRBT patents on detection of zero day privilege escalation malware and detection and prevention of data breach and ransomware attacks is an added advantage.	RFP Clause removed
11	22	EDR – Operation	The solution must have the ability to export the current configuration of the program in order to later be imported to the same or another computer.	RFP Clause removed
12	22	EDR- Operation	The solution must assign a risk score to all objects within the protected environment.	RFP Clause removed
13	22	EDR – INFRASTRUCTURE 2	The solution must have a single management dashboard for servers, endpoints and mobile devices.	The solution must have a single management dashboard for Endpoints & Servers
14	23	4.2.3 Firewall Rule Analyser Scope	Bidder shall complete the implementation of the solution and Integration with Bank of Maharashtra Firewalls, Security Routers, Web Proxy & other Network devices covered under scope. Total Count of Generic network devices for completing the network topology - 50 (Includes ACI switches).	Bidder shall complete the implementation of the solution and Integration with Bank of Maharashtra Firewalls, Security Routers, Web Proxy & other Network devices covered under scope. Total Count of Generic network devices for completing the network topology - 50 Nos (Approx 25 Nos ACI Leaf Switches & 25 Nos -L3 Network devices)
15	25	WAF Features & Functional Requirements	Solution should be able to protect against UDP, TCP, SIP, DNS, HTTP, SSL and other network attack targets while delivering uninterrupted service for legitimate connections	Solution should be able to protect against TCP, DNS, HTTP, SSL and other network attack targets while delivering uninterrupted service for legitimate connections

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
16	25	Deception Solution Scope	High Availability (HA) mode at DC and standalone mode at DR	ReferRTO/RPO cluase under RFP section 7.1 Service Criteria
17	27	Technical and Functional Requirements for Deception - 4.2.5.13	Bidder should conduct System/Solution health check-up twice a year and provide report to the Bank.	Bidder should conduct System/Solution health check-up twice a year through solution OEM and provide report to the Bank
18	34	5.1.4.1	If the contract is awarded, the Bidder shall furnish a Performance Guarantee to the extent of 15% of the value of the contract within 10 days of signing of the contract.	If the contract is awarded, the Bidder shall furnish a Performance Guarantee to the extent of 10% of the value of the contract within 10 days of signing of the contract.
19	39	5.1.8 Bid Security	The Bidder shall furnish, as part of its Technical bid, bid security of an amount of Rs. 60,00,000/= (Rupees Sixty Lakhs Only). The bid security is required to protect the Bank against the risk and shall be in the form of a Demand Draft favouring "bank of maharashtra" by a scheduled Commercial Bank or a Foreign bank located in India in the form provided in Annexure 9 of this RFP Any bid not secured in accordance with the above will be rejected by the Bank as nonresponsive.	The Bidder shall furnish, as part of its Technical bid, bid security of an amount of Rs. 60,00,000/= (Rupees Sixty Lakhs Only). The bid security is required to protect the Bank against the risk and shall be in the form of a **Demand Draft/ Bank Guarantee** favouring "bank of maharashtra" by a scheduled Commercial Bank or a Foreign bank located in India in the form provided in Annexure 9 of this RFP Any bid not secured in accordance with the above will be rejected by the Bank as nonresponsive.
20	68	8	Payment Terms: Application - 80% on Inspection and 20% after Sign-Off Hardware - 80% on Inspection and 20% after Sign-Off Installation - 100% after Sign-Off Training - 100% after completion & feedback of employees FMS / AMC / ATS - Quarterly in arrears	Payment Terms: Application - 80% on Delivery and 20% after Sign-Off Hardware - 80% on Delivery and 20% after Sign-Off Installation - 100% after Sign-Off Training - 100% after completion FMS - Quarterly in arrears AMC / ATS - Annually in advance
21	76	31	Sensors support 32-bit and 64-bit workstation, server, AND embedded system operating systems.	Sensors support 32-bit and 64-bit workstation, server, AND embedded system operating systems such as Windows Embedded XP, standard7, 8,8.1,10,Pos V1 etc.

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
22	74	Technical and Functional Requirements for EDR-4	The proposed solution must analyse Windows internal structures for alteration and consistency.	The RFP clause removed
23	74	Technical and Functional Requirements for EDR-2	The proposed solution must gather security information from the host including its network shares, patch level, and running Windows tasks.	The proposed solution must gather security information from the host including its network shares, and running Windows tasks.
24	74	Technical and Functional Requirements for EDR-1	The proposed solution must, at minimum perform Continuous Centralized Recording & the following checks on client in real time: a) Hooking - kernel and user mode hooks in SSDT, IDT, IAT/EAT, and IRP_MJ b) System entry (SYSENTER and int2E) hooks c) Local and global Windows hooks (Set WindowsHookEx)	Mentioned sub-caluses removed
25	74	Technical and Functional Requirements for EDR-7	The proposed solution must be able to provide a complete environmental correlation that shows the clients and the number of systems where the identified malicious file was found. Ability to have local access to all data for correlation with on premise devices such as next generation firewalls (Checkpoint, Palo Alto , Cisco) and SIEMs	RFP Clause removed
26	74	Technical and Functional Requirements for EDR-53	The solution must support containment of suspected hosts while maintaining access to the Endpoint Forensics solution for investigation as well as other whitelisted resources used for investigation or remediation. The investigation should be possible even if the computer is now offline or even reformatted.	The solution must support containment of suspected hosts while maintaining access to the Endpoint Forensics solution for investigation as well as other whitelisted resources used for investigation or remediation from central console. The investigation should be possible based on data collected on Central console even if the computer is now offline or even reformatted."

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
27	74	Technical and Functional Requirements for EDR-9	The solution must support the ability to exclude applications or files from exploit detection.	The RFP Clause is removed
28	74	Technical and Functional Requirements for EDR-78	It should be possible to integrate publicly available IP and Hash blacklists as well as other external Threat Intelligence Feeds that provide indicators of comprise like blacklists of IP addresses, domains and MD5 sums out of the box without any additional licenses	It should be possible to integrate publicly available IP and Hash blacklists as well as other external Threat Intelligence Feeds (Minimum that provide indicators of comprise like blacklists of IP addresses, domains and MD5 sums out of the box without any additional cost to bank.At Minimum solution should receive the feeds from 3rd party feeds provider such as MITRE ATT&CK,NVD,SANS,VIRUS TOTAL etc."
29	74	Technical and Functional Requirements for EDR-36	It should be possible to remotely control, an endpoint from the endpoint response tool, even if that endpoint has been disconnected from all other network connections..	It should be possible to remotely control, an endpoint from the EDR Management console , even if that endpoint has been disconnected from all other network connections (Except connection to management console)
30	74	Technical and Functional Requirements for EDR-5876	Solution should include prebuilt search queries in natural language to aid learning of EDR tool. Ability to add custom queries to help L1 analysts run EDR queries	Solution should include prebuilt search queries to aid learning of EDR tool. Ability to add custom queries to help L1 analysts run EDR queries
31	74	Technical and Functional Requirements for EDR-72	Solution should have the capability to query endpoints for zero-day vulnerabilities	Solution should have the capability to detect & respond to the Zero-Day exploits.
32	75	Technical and Functional Requirements for EDR-16	The proposed solution should provide centralized storage of all endpoint event data whereby queries and analysis are performed on the server as opposed to the endpoints themselves. It should show which process, including version information and digital signature status, made a network connection.	The proposed solution should provide centralized storage of all endpoint event data whereby queries and analysis are performed on the server and endpoint to be queried if network connection is disrupted due to technical or business reasons, more information is required and reasons deemed fit. It should show which process, including version information and digital signature status, made a network connection.

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
33	75	Technical and Functional Requirements for EDR-19	The proposed solution must be able to set scan priority on the host to prevent performance degradation on the client (low priority scan option).	The proposed solution must be able to set scan priority or collection of events to prevent performance degradation on the client (low priority scan option)
34	76	Technical and Functional Requirements for EDR-27	The solution should support agent capping for CPU and memory utilization. CPU consumption on endpoint should be less than 1%; memory (RAM) consumption should be less than 20 MB	The solution should support agent capping for CPU and memory utilization. CPU consumption on endpoint should be less than 1% & memory (RAM) consumption should be less than 8% (Ideal endpoint configuration i3 procesor with 4GB RAM).
35	76	Technical and Functional Requirements for EDR-26	The scan report must provide a preliminary assessment of the state of the client at the end of the scan, accompanied with supporting detail to support the result.	The solution should provide report with preliminary assessment of the state of the client accompanied with supporting detail to support the result
36	77	Technical and Functional Requirements for EDR-50	Solution should provide granular policy rules for Prevention actions, rather than simple On/Off switch, such as processes allowed to invoke legitimate command interpreters like Powershell, Python, WMIC etc.	RFP clause removed
37	76	Technical and Functional Requirements for EDR-22	The proposed solution must be able to report on the client status: · Idle	The proposed solution must be able to report on the client status: · Online .Offline .Scan in Progress
38	77	Technical and Functional Requirements for EDR-48	The solution must be able to automatically kill exploited applications or automatically prevent any payload from exploited application to run. Provide a fully recorded “kill chain” of malware.	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
39	77	Technical and Functional Requirements for EDR-45	The solution must be able to throttle the triage collection if a widespread compromise or false positive is generating inordinate number of triage requests.	The solution administrator must be able to control the triage collection if a widespread compromise or false positive is generating inordinate number of triage requests

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
40	77	Technical and Functional Requirements for EDR-49	End-user shall be notified of automatically containment/ killed applications and payloads ensuring seamless user experience.	The RFP Clause removed
41	77	Technical and Functional Requirements for EDR-47	Solution should be able to terminate malicious payload at run time for exploited applications as well as it should provide capability to terminate exploited application based on behavioural analysis. Security vendor must have their own integrated exploit detection and prevention engine without relying on 3rd party tools	Solution should be able to detect & respond to malicious payload identified based on behaviour analysis
42	78	Technical and Functional Requirements for EDR-52	Solution must be able to mitigate the impact of a compromised system with network isolation using workflow driven containment in order to prevent lateral spread. The solution must have a two-stage process for containment requests, with the ability to separate the requestor and approver roles.	Solution must provide ability to incident responder for quickly isolation of compromized machine from network in order to prevent lateral spread
43	79	Technical and Functional Requirements for EDR-66	Solution must provide the following live response capabilities (when endpoint is isolated or not): -Capture and review actual “hands on the keyboard” activity by intruders.	Solution must provide the live response capabilities for Living of the land/ Fileless attacks.
44	81	Technical and Functional Requirements for EDR	The solution must include IDRBT patents for detecting zero day privilege escalation malware	The RFP clause removed.
45	81	Technical and Functional Requirements for EDR-80	The solution should have built-in vulnerability assessment & dynamic application/process whitelisting & blacklisting functionality in order to provide closed loop remediation.	The solution should have built-in capabilities to detect and respond to Zero-Day exploits & hash banning functionality
46	84	Technical and Functional Requirements for EDR	The solution must include IDRBT patents for detection and prevention of data breach and ransomware attacks	The RFP clause removed.

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
47	92	Technical and Functional Requirements for WAF 2.11	Appliance should support a LCD panel/LED to display alerts and fault information for an administrator to monitor the system	The RFP clause removed.
48	93	Technical and Functional Requirements for WAF-3.8	The solution must identify and mitigate the OWASP Top Ten 2020 web application security vulnerabilities.	WAF solution should protect against common threats such as those identified in the OWASP Top 10 & should provide inbuilt OWASP dashboard on GUI with remediation
49	96	Technical and Functional Requirements for WAF-4.2	The solution appliance must have dual hot-swap hard drives and dual hot-swap power supplies for high availability from the same. Inheritance should support restricting modifications to the base policy settings	The solution must have dual hot-swap power supplies for high availability . Inheritance should support restricting modifications to the base policy settings
50	97	Technical and Functional Requirements for WAF 5.1	Proposed solution should be able to integrate with external SSL visibility solution. Also Proposed WAF Solution should have capability to integrate with Anti- Fraud vendors to provide web fraud protection.	Proposed solution should be able to integrate with external SSL visibility solution
51	97	Technical and Functional Requirements for WAF-5.5	WAF should integrate with Bank's Network Trend Micro	The Proposed WAF Solution should support ICAP(Internet Content Adaption Protocol) integration with other security devices (industry leading security solutions i.e McAfee,Trend Micro DDAN etc.
52	98	Technical and Functional Requirements for WAF 2.11	Because the protected Web applications will access and transfer sensitive data to internal databases, the vendor should integrate with Bank's Mcafee DAM solution for end-to-end security.	The RFP clause removed.
53	98	Technical and Functional Requirements for WAF-6.6	The solution must be able to operate in FIPS (Federal Information Processing Standard) 140-2 compliance mode.	The RFP clause removed
54	99	Technical and Functional Requirements for WAF-7.5	The solution must support the creation of custom log messages and provide system variable placeholders mechanism to make this use	The Proposed WAF Solution Should support integration with external siem/syslog messages

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
			case possible. For example, the Username placeholder looks like (${Alert.username})	
55	104	Functional Requirements for Deception Solution Point 42	Solution should automatically detect scanning and L2 attacks such as ARP flood and IP scan etc.	Solution should automatically detect scanning and L2 attacks such as IP scanning etc
56	105	Functional Requirements for Deception Solution point 49	Solution should provide granular control over decoys in each network segment. In addition, should provide capability to turn off all decoys in a particular group/ network segment	Solution should provide granular control over decoys in each network segment. In addition, should provide capability to turn off all decoys or whitelist services in a particular group/ network segment"
57	105	Functional Requirements for Deception Solution Point 50	Solution should provide maintenance mode wherein decoys of a particular VLAN can be switched off during maintenance of the VLAN	Solution should provide Whitelist options wherein decoys of a particular VLAN can be whitelisted during maintenance of the VLAN" as this would help detect any attack during the maintenance window.
58	105	Functional Requirements for Deception Solution Point 51	The solution should integrate with existing patch management solution of the bank to keep the decoys in sync with the patch level of devices in production environment	The solution should provide a mechanism to patch decoys so as to keep the decoys in sync with the patch level of devices in production environment.
59	105	Functional Requirements for Deception Solution Point 54	The solution should support creation of unlimited number of decoys and the number of decoys per VLAN should be controllable from the management console	RFP Clause is removed.
60	105	Functional Requirements for Deception Solution Point 59	Solution should provide ability to forward emails to sandboxing functionality for email/malware analysis	The RFP clause is removed
61	105	62 / d) Technical and Functional Requirements for Deception Solution:	Web application decoys should be able to provide full licensed application deceptions of solutions currently deployed in bank	Web application decoys should be customisable at the network and content layers to include decoy versions of applications deployed in the bank.

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
62	106	Functional Requirements for Deception Solution Point 77	The endpoint deception agent should be able to select users/computers on the basis of the following selection criteria: - Process list	The endpoint deception agent should be able to deploy deception based on the computer usage behavior seen at the endpoint, which could include but not limit to browser history, installed programs, files, logged on user, etc. seen at the endpoint
63	106	Technical and Functional Requirements for EDR-71	System should be able to detect and track stolen credentials by integrating with SIEM on API's	The RFP clause removed
64	106	66 / d) Technical and Functional Requirements for Deception Solution:	The solution must support path discovery and provide topographical network map for lateral movements to critical assets.	The RFP Clause is removed
65	106	69 / d) Technical and Functional Requirements for Deception Solution:	The solution should support sending Darknet IP traffic to the platform. Should be able to create unused IP‟s in production subnets and dark networks on routers and forward traffic to these IP‟s to deceptive VM‟s for engagement.	The RFP clause is removed
66	106	70 / d) Technical and Functional Requirements for Deception Solution:	Solution should be able to spin up or create an automatic decoy as per the request seen from the attacker.	The RFP Clause is removed
67	106	71/ d) Technical and Functional Requirements for Deception Solution:	System should be able to detect and track stolen credentials by integrating with SIEM on API's	The RFP clause is removed
68	113	Annexure 5.2	The OEM should be listed in Gartner list for 2018,2019. Or 2020.	The RFP clause will be applicable only to Web Application Firewall(WAF).
69	113	Annexure 5: Eligibility Criteria Compliance	The OEM should have been in existence for a minimum period of five years in India as on 31-Mar-2020	The OEM should have been in existence for a minimum period of three years in India as on 31-Mar-2020”

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
70	131	Annexure 14: Resource Deployment Plan	Proposed Project Director is required to have implementation experience for EFRMS solution in at least 2 Public Sector Bank / Scheduled Commercial Bank.	The RFP clause removed.

Chief Information Security Officer
Integrated Risk Management Department