Response to pre-bid queries -
RFP Ref No. BCC:CISO:111:111:448 dated 22-Nov-2019

Sr no	Page no	Point / Section #	Category	Clarification point as stated in the tender document	Comment/ Suggestion/ Deviation	Bank's Response
1	7	1.3.1	Scope of work	100+ branches/offices overseas including branches of our subsidiaries, distributed in 23 countries.	Does the activity also cover the offices in 23 subsidary contries. How is the network delployment at the subsidary countries. Please provide the list of countries.	This activity covers only domestic locations i.e. India as Erst. Vijaya Bank and Erst. Dena Bank have no offices in International locations.
2	7	1.3.1	Scope of work	100+ branches/offices overseas including branches of our subsidiaries, distributed in 23 countries.	Will the vendor need to travel to various office laocations for the intended activity? If yes then, who will bear the cost for the same	If the deployment cannot be done through centralized tools by the vendor, the vendor will be required to travel to such locations and the cost should be factored by the vendor.
3	7	1.3.1	Scope of work	Final submission of report to the Bank along with certification for systems identified for remediation to be moved to BOB network or not.	For migration of a branch , the timeline provided is for 21 days from indentifictaion to remediation and final report delivery. Please let us know, if the timeline if 21 days provided is for a single branch migration or more at a given point in time.	The details of branches for migration as per migration plan like 50 branches are given on X date to bidder and after 3-4 days, 70 branches are given for CA. This timeline of 21 days is from the date when such branch details are provided to vendor for CA.
4	43	C.1	Experience & Support Infrastructure	Bidder/OEM should have experience in Compromise Assessment completion in at least 01 BFSI sector having Min. 500 branches /Govt. Sector in India or globally.	We understand that experience of Govt & Global clients - Non BFSI will also be considered against this point. Kindly confirm	Non BFSI experience will be considered only in case of Govt. sector.
5	65	Point 5	Annexure 13 - Technical specifications	The bidder must provide technology to deploy and monitor network traffic in order to identify signs of attacker activity, Backdoor command and control connections and traffic towards malicious IP addresses and malicious domains.	Technology for network monitoring will require additional licenses and infrastrure for storage . Please advise if bidder needs to factor the cost of procurement of the same	Bidder must factor cost for conducting CA which includes network level montoring for malicious activities.
6	65	Point 6	Annexure 13 - Technical specifications	The bidder must provide standard tools and scripts for analysis of systems and they must be compatible with existing technologies and architecture of Bank's network.	Pls provide list for all the hardware and software components deployed in the network for factoring the assumption for license prourement for the CA	Details cannot be shared at pre-bid stage.
7	66	Point 10	Annexure 13 - Technical specifications	The bidder must be able to conduct log data analysis activities if necessary	For conduction log data analysis , will SIEM tool needed to be deployed.	SIEM solution is not required to be deployed.
8	66	Point 13	Annexure 13 - Technical specifications	The bidder must be able to develop plan of incident response, from the initial detection to the final resolution of the incident.	Is it an augmentation of the existing incident response plan or formation of new incudent response plan.	The vendor should develop new incident response plan based on inputs received by the Bank and taking reference of existing plan.
9	6	1.2	Project Overview	Systems comprise of all the devices connected to the network including but not limited to desktops, servers (windows / Linux / Unix based operating system), network devices (switch, router, etc.), headless devices (printers, scanners, etc.).	Can we get list of all nodes for exact scope prepartion and planning ? Excat scope will definitely help for our internal assessment.	Details cannot be shared at pre-bid stage.
10	8	1.3.1	Scope of work	Compromise Assessment should assess and report the following core security issues: Existing vulnerabilities and presence of malware in servers, endpoint and network. Malware and persistence mechanisms Command and Control activities User account anomalies Data exfiltration and sabotage	We request for more elloboratiove details of expectation of tool that can be used or can't be used if any	High level details of project have already been defined in RFP for CA.

Response to pre-bid queries -
RFP Ref No. BCC:CISO:111:111:448 dated 22-Nov-2019

Sr no	Page no	Point / Section #	Category	Clarification point as stated in the tender document	Comment/ Suggestion/ Deviation	Bank's Response
11	25	3.7.1 3.7.2	Other RFP Requirer	3.7.1This tender document may undergo change by either additions or deletions or modifications before the actual award of the contract by the Bank. The Bank also reserves the right to change any terms and conditions of the tender document and its subsequent addendums as it deems necessary at its sole discretion. The Bank will inform all bidders about changes, if any. 3.7.2The Bank may revise any part of the tender document, by providing a written addendum at stage till the award of the contract. The Bank reserves the right to issue revisions to this tender document at any time before the award date. The addendums, if any, shall be published on Bank's website only.	Again proper finalised scope will help us to plan and prepare commercials. We hope change in scope if any should be intimated and bank should allow us to rework on our proposal accordingly.	No Change
12	42		Eligibility Criteria	Bidder must be a Government Organization / PSU / PSE / partnership firm / LLP or private / public limited company in India at least for the last 5 Years	I hope 5 or more years tenure needed as per eligibility. Any specific document need to be presented to support this?	Documents required is mentioned in Annexure 02 of RFP
13	18	3.2.24	Rules for respondi	All out of pocket expenses, traveling, boarding and lodging expenses for the entire life of the contract should be a part of the financial bid submitted by the bidder to the Bank. No extra costs on account of any items or services or by way of any out of pocket expenses, including travel, boarding and lodging etc. will be payable by the Bank. The bidder cannot take the plea of omitting any charges or costs and later lodge a claim on the Bank for the same	As per scope, effort will be estimated for resources, travel and lodging. Change in scope may change effort and duration and that will also impact costing. Request bank to suggest on this point.	No Change
14	12	2.2	Technical bid evalu	Experience in conducting Compromise assessment completed in BFSI sector having Min. 500 branches /Govt. Sector in India or globally.	Please elaborate more how many customer references we need to provide?	Please refer Annexure 02 Eligiblity Criteria of RFP. Regarding bid evaluation, refer Evaluation process section of the RFP.
15	Page 65	Technical Spe	All	Technical Specifications and Scope related to CA execution by "Security Vendor"	Please change the "Bidder" to "Bidder/Security Vendor" for technical specifications and Scope. Because, the CA will be executed by "Security Vendor", hence the security vendor needs to have the mentioned criteria/qualification/experience for eg: 1. Security Vendor should be named leader in Incident Response by Forrester Wave 2. The Security Vendor must have deep knowledge of attack methodologies, background, objectives, target countries/verticals categorised by specific APT groups and should leverage human attacker based IOC's (TTP's) for CA. 3. Security Vendor must have at least 15 years of experience in incident response and forensic investigations related to cyber security across various countries and verticals Above change will enable effective assessment of respective bidders/security vendors and is recommended.	Modifications for changing bidder to bidder/OEM in Annexure 13 of RFP will be incorporated in Addendum.
16	Page 8	Scope of Worl	Scope	Existing vulnerabilities and presence of malware in servers, endpoint and network.	Suggestion: We request the bank to keep assessment of vulnerabilities as separate periodic activity (part of Bank's Vulnerability Management program). However, as security vendor, we shall report any exploited vulnerability by malware, if identified.	Vulnerability Management is not to be done by the bidder. In case of compromise is detected, the details of vulnerability and exploit should be submitted to the Bank in report.

Response to pre-bid queries -
RFP Ref No. BCC:CISO:111:111:448 dated 22-Nov-2019

Sr no	Page no	Point / Section #	Category	Clarification point as stated in the tender document	Comment/ Suggestion/ Deviation	Bank's Response
17	Page 9	Assessment A	Scope	The CA activity should cover all the systems / devices connected to eVijaya and eDena network including but not limited to desktops, servers, network devices (like router, switch, etc), printers, scanners and other IOTs.	Comment - Endpoint agents cant be deployed nor supported on Router, switches, printers, scanners and other IOT devices. However this can be covered by Network Forensics for any mailicous communication via these devices	Bank expects compromise assessment of all the devices connected to eVB and eDB network. Methodology for CA should be demonstrated by the bidder during technical evaluation stage, if found eligible.
18	Page 65	Technical Spe	General - OEM Exp	The personnel engaged in the activity must have atleast 5 years hands on experience in identifying compromises and responding to breaches along with malware and/or IOC analysis.	The personnel engaged in the activity must have atleast 5 years hands on experience in identifying compromises and responding to breaches along with malware and/or IOC analysis. Further the Security Vendor must have at least 15 years of experience in incident response and forensic investigations related to cyber security across various countries and verticals	No Change
19	Page 65	Technical Spe	General - Technolo	The bidder must provide the technology deployed for searching the systems for Compromise Assessment. Any agents / clients / software distribution tool including applicable licenses should be provided by the bidder.	The **security vendor** must provide the technology deployed for searching the systems for Compromise Assessment. Any agents / clients / software distribution tool including applicable licenses should be provided by the bidder. The Security Vendor must provide the Network forensic technology to be deployed to monitors traffic destined from the network to the Internet in order to identify signs of attacker activity. The Security Vendor must have deep knowledge of attack methodologies, background, objectives, target countries/verticals categorised by specific APT groups and should leverage human attacker based IOC's (TTP's) for CA.	Modifications for changing bidder to bidder/OEM in Annexure 13 of RFP will be incorporated in Addendum.
20	Page 65	Technical Spe	General - Technolo	The bidder must have threat intelligence which must be utilized for the purpose of the compromise assessment.	The **security vendor** must have threat intelligence which must be utilized for the purpose of the compromise assessment. Also, The Security Vendor must have at least 100 or more cyber threat intelligence analysts and The Security Vendor must be able to provide profiles of at least 10 advance persistant threat groups targeting financial organisation with comprehensive insights built on tracking of and responding to threats/breaches originating from these APT groups	Modifications for changing bidder to bidder/OEM in Annexure 13 of RFP will be incorporated in Addendum.
21	Page 65	Technical Spe	General - Technolo	The bidder must provide technology to deploy and monitor network traffic in order to identify signs of attacker activity, Backdoor command and control connections and traffic towards malicious IP addresses and malicious domains.	The **security vendor** must provide technology to deploy and monitor network traffic in order to identify signs of attacker activity, Backdoor command and control connections and traffic towards malicious IP addresses and malicious domains associated with targeted attacker activity. The Security Vendor must have the capability to sweep the Network with IOC's related to Custom Malware looking for Lateral Movement techniques used by human attackers. The Security Vendor must have proven experience with tracking intelligence and attacker groups within APJ region for financial attacker groups.	Modifications for changing bidder to bidder/OEM in Annexure 13 of RFP will be incorporated in Addendum.
22	Page 65	Technical Spe	General - Technolo	The bidder must have the capability to analyze and provide details on all stages of attack: Initial reconnaissance, compromise, establish foothold, escalate privileges, internal reconnaissance and final attack.	The **security vendor** must have the capability to analyze and provide details on all stages of attack: Initial reconnaissance, compromise, establish foothold, escalate privileges, internal reconnaissance and final attack. **Security Vendor** should be named leader in Incident Response by Forrester Wave	Modifications for changing bidder to bidder/OEM in Annexure 13 of RFP will be incorporated in Addendum.
23	Page 65	Technical Spe	General - Technolo	The bidder must be able to search for various artifacts of malicious threat vectors including but not limited to persistence mechanisms, lateral movement mechanisms, registry keys update, malicious process, etc.	The **security vendor** must be able to search for various artifacts of malicious threat vectors including but not limited to persistence mechanisms, lateral movement mechanisms, registry keys update, malicious process, etc. The Security vendor must have a constantly updated knowledgebase of 1000's of indicators of compromise for endpoints and networks and it must be utlized for the purpose of the engagement.	Modifications for changing bidder to bidder/OEM in Annexure 13 of RFP will be incorporated in Addendum.

Response to pre-bid queries -
RFP Ref No. BCC:CISO:111:111:448 dated 22-Nov-2019

Sr no	Page no	Point / Section #	Category	Clarification point as stated in the tender document	Comment/ Suggestion/ Deviation	Bank's Response
24	Page 65	Technical Spe	General - Methodo	The bidder must be able to conduct log data analysis activities if necessary	The **Security Vendor** must be able to conduct log data analysis activities if necessary. If required, the Security Vendor must have the ability to perform malware analysis and reverse engineering of malware samples using both automated and manual techniques and provide host-based and network-based indicators that are used to find the malware variants in the wild.	Modifications for changing bidder to bidder/OEM in Annexure 13 of RFP will be incorporated in Addendum.
25	Page 65	Technical Spe	General - Methodo	The bidder must have the capability to detect non-malware attacker activity, behavioral based attacks, insider threat including misuse of privileged credentials.	The **Security Vendor** must have the capability to detect non-malware attacker activity, behavioral based attacks, insider threat including misuse of privileged credentials. The Security Vendor must inspect all defined systems for IOCs Detecting rootkits, hidden files, and hidden processes	Modifications for changing bidder to bidder/OEM in Annexure 13 of RFP will be incorporated in Addendum.
26	Page 65	Technical Spe	General - Methodo	The bidder must have appropriate licenses, as applicable, for proposed tools and technology for compromise assessment.	The **Security Vendor** must have appropriate licenses, as applicable, for proposed tools and technology for compromise assessment. The Security Vendor must offer continuous monitoring services to augment the consulting services after the latter have completed. There must be a seamless transition from consulting services to such monitoring services. The Security Vendor must offer incident response retainer packages that allow a seamless transition from compromise assessment to incident response and other consulting services as necessitated by the situation.	Modifications for changing bidder to bidder/OEM in Annexure 13 of RFP will be incorporated in Addendum.
27	6	1.2	Project overview	Systems comprise of all the devices connected to the network including but not limited to desktops, servers (windows / Linux / Unix based operating system), network devices (switch, router, etc.), headless devices (printers, scanners, etc.)	Approx No. of systems/devices for eVijaya & eDena 1.End Points 2.Servers 3.N/W Devices	Data cannot be shared at RFP stage. Data will only be shared with successful bidder at later stage.
28	8	1.3.1.	Scope of Work	The technology for compromise assessment must be deployed on premise by the bidder at centralized location i.e. Mumbai, Hyderabad and Bengaluru DC/DR/NDR setup	On premise deployment is only for 3 said location	eDB: DC is Mumbai and DR is Banglore eVB: DC is Bengaluru and DR is Hyderabad. BOB: DC is Mumbai and DR is Hyderabad. On premise deployment as per CA activity to be done by the bidder
29	7	1.3.1	Scope of Work (Activity- Point 2)	Deployment of agent, script, etc. on the systems at branch for CA by successful bidder/ OEM	Deployment is to be done only at centralized locaton or it includes the branches	The CA coverage includes all branches and offices of eVB and eDB migrating to BOB network.
30	9	2	Assessment Activity (Point a)	Deployment of tools (agents, scripts, etc.) on systems / devices approved by the Bank	Pl clarify	The complete CA assessment plan should be documented and approved by the Bank.
31	8	1.3.1.	Scope of Work	Locations covered under this scope: · All devices connected to eDena network and migrating to BOB network. · All devices connected to eVijaya network and migrating to BOB network.	eDena - No. of branches eVijaya- No. of branches	eDena: 1900 (approx.) eVijaya: 2300 (approx.)
32	8	1.3.1.	Activities and Deliverables by the Bidder/OEM:	submission of complete understanding document along with CA approach to the Bank.	What is the expectation from Bidder	Bidder to submit understanding document including details of IT infrastructure, migration plan,etc. along with proposed CA approach.
33	12	2.2	Technical Bid Evaluation : Criteria	Experience in conducting Compromise assessment completed in BFSI sector having Min. 500 branches /Govt. Sector in India or globally.	1.any specific year of assessment e.g. during last three years 2.Is it asking for compromise assessment conducted for a Min 500 branches or any compromise assessment in BSI sector which have min 500 branches	No Change

Response to pre-bid queries -
RFP Ref No. BCC:CISO:111:111:448 dated 22-Nov-2019

Sr no	Page no	Point / Section #	Category	Clarification point as stated in the tender document	Comment/ Suggestion/ Deviation	Bank's Response
34	47	Annexure 5	05 – Undertaking from the Bidder (Point 5 a)	a) Commission or gratuities, if any paid or to be paid by us to agents relating to this Bid and to Contract execution, if we are awarded the Contract are listed below.	if no agents involved ---sub point 5a. point to be Not Applicable	No Change
35	56	Annexure 10	PRE CONTRACT INTEGRITY PACT	Chief Executive Officer	Integrity pact mentions "CEO", We take the declaration/signatures from Partners, so whether Partner name can be mentioned inplace of CEO	Person authorised to execute/sign the document can sign.
36	65	7	Scope	The bidder must have the capability to analyze and provide details on all stages of attack: Initial reconnaissance, compromise, establish foothold, escalate privileges, internal reconnaissance and final attack.	This is not possible as the agent would be scanning the systems for potential compromise which has already occurred. All stages of attacks may not be visible on the Endpoints as initial phases would have occurred outside of the End Points/Desktop/Servers. We recommend to change this to final attack/compromised stage on the End Point/Desktop/Servers	Cases where compromise has already occurred, the exhaustive details of the suspected activity which can be gathered from end point and network can be provided to the Bank.
37	65	8	Scope	The bidder must be able to utilize a mix of automated and manual techniques to identify indicators of compromise and submission of exhaustive reports to the Bank. Bidder must also have the ability to perform malware analysis and reverse engineering of malware samples	Does this mean the solution deployed should have the ability to do it or is it a must?	All technical requirements as per Annexure 13 of RFP are mandatory.
38	66	13	Scope	The bidder must be able to develop plan of incident response, from the initial detection to the final resolution of the incident.	The initial detection stage/Compromised stage would have occurred even before the CA scan is carried out. We recommend to change this to provide remediation advisory/Resolution of the identified Incident.	Cases where compromise has already occurred, the exhaustive details of the suspected activity which can be gathered from end point and network can be provided to the Bank along with remediation action of the incident/alert/event.
39	7	NA	General	The bidder must provide technology to deploy and monitor network traffic in order to identify signs of attacker activity, Backdoor command and control connections and traffic towards malicious IP addresses and malicious domains.	Does this mean we have to provide a solution to detect network traffic at the Gateway/Egress points as well? If so how many Network/Egress points?	Malicious activity at network level should also be covered in the CA coverage.
40	66	14	Scope	The bidder must have the capability to detect non-malware attacker activity, behavioral based attacks, insider threat including misuse of privileged credentials.	We recommend to take this point out as this would be for an EDR solution and not Compromise Assessment.	No Change