Setup and Implementation Of Deception Technology

REQUEST FOR PROPOSAL (RFP)

CORRIGENDUM # 1
And
Response to Pre-bid queries

(01st April 2021)
RFP: ReBIT/2021 / CPO / 031

Reserve Bank Information Technology Pvt. Ltd.
502, Building No 1, Mindspace Juinagar, Nerul, Navi Mumbai – 400706

Following are the changes / clarification in the RFP terms. All the bidders are requested to refer the "Corrigendum / Revised Terms" column as below:

Page No	Clause No	Existing Terms	Corrigendum / Revised Terms
43	Annexure G: Minimum Eligibility Criteria S.No 5	**REQUIREMENTS** The bidder should have executed 2 or more projects of size 400 user systems each of the proposed OEM's Solution in the last 3 years and should be go-live as on 31-12-2020. **List of Documents to be submitted** A) Bidder to submit documentary evidence such as satisfaction/ credential letter from the client clearly stating the scope of work and project value OR Completion letter from the client indicating the scope of work executed by the Bidder and the project value B) Contract / PO Copy as documentary evidence proving project value The onus of proving the credential via documentary evidence is of the Bidder. In case, the Bidder is unable to provide any of the above, it will be the ReBIT's discretion to evaluate the claim in this regard. Note: Only completed assignments will be evaluated. Projects under implementation or not completed for any reason will not be evaluated. The name of the Bidder and the proposed OEM solution needs to be in sync with the credential letters / contract copies. Exceptions may be made in case of divesture, M&A.	**REQUIREMENTS** The bidder**/OEM** should have executed 2 or more projects of size 400 user systems each of the proposed OEM's Solution in the last 3 years and should be go-live as on 31-12-2020. **List of Documents to be submitted** A) Bidder to submit documentary evidence such as satisfaction/ credential letter from the client clearly stating the scope of work and project value OR Completion letter from the client indicating the scope of work executed by the Bidder and the project value B) Contract / PO Copy as documentary evidence proving project value The onus of proving the credential via documentary evidence is of the Bidder. In case, the Bidder is unable to provide any of the above, it will be the ReBIT's discretion to evaluate the claim in this regard. Note: Only completed assignments will be evaluated. Projects under implementation or not completed for any reason will not be evaluated The name of the Bidder and the proposed OEM solution needs to be in sync with the credential letters / contract copies. Exceptions may be made in case of divesture, M&A. **Additional document to be submitted if the bidder alone is not meeting this criterion but submitting the bid on behalf of its OEM based on OEM's past project implementation experience (PO shall be issued in the name of the bidder):** **The bidder shall provide along with the bid submission a declaration and certification from the OEM that "OEM will**

Page No	Clause No	Existing Terms	Corrigendum / Revised Terms
			do the implementation, support and all deliverables at ReBIT as per the RFP. OEM shall be liable for all the terms and conditions of the RFP." **Also, the OEM team details who will work on this project shall be provided as per Annexure - L.**
14	5.6 Project Milestones S.No 1	**Project Milestones:** Receipt of Software and Hardware **Payment:** 10% of Hardware and Software Cost. (S. No. 1 and 2 of Annexure I - Price Bid Format)	**Project Milestones:** Receipt of Software and Hardware **Payment:** **50% of** Hardware and Software **subscription Cost for Year 1.** (S. No. 1 and 2 of Annexure I - Price Bid Format) **upon receipt and acceptance by ReBIT.**
15	5.6 Project Milestones S.No 2	**Project Milestones:** Implementation upto Go Live as mentioned in section 5.4 **Payment:** 90% of Hardware and Software Cost (S. No. 1 and 2 of Annexure I - Price Bid Format)	**Project Milestones:** Implementation upto Go Live as mentioned in section 5.4 **Payment:** **50%** of Hardware and Software **subscription Cost for Year 1** (S. No. 1 and 2 of Annexure I - Price Bid Format) **upon Go-live and acceptance by ReBIT.**
15	5.6 Project Milestones S.No 4	**Project Milestones:** Renewal of Licenses Support / Subscription for Year 2 **Payment:** 100% of subscription cost for Year 2 (S.No. 1 of Annexure I - Price Bid Format)	**Project Milestones:** Renewal **of Hardware and Software subscription** for Year 2 **Payment:** 100% of **Hardware and Software** subscription cost for Year 2 (S.No. 1 **and 2** of Annexure I - Price Bid Format)
15	5.6 Project Milestones S.No 5	**Project Milestones:** Renewal of Licenses Support / Subscription for Year 3 **Payment:** 100% of subscription cost for Year 3 (S.No. 1 of Annexure I - Price Bid Format)	**Project Milestones:** Renewal **of Hardware and Software subscription** for Year 3 **Payment:** 100% of **Hardware and Software** subscription cost for Year 3 (S.No. 1 **and 2** of Annexure I - Price Bid Format)
7	5.2 Software requirements , viii.	viii. Internet decoys also need to be solutioned as part of this solution and the vendor should provide all the requirements for this as part of this solution.	viii. Internet decoys also need to be solutioned as part of this solution and the vendor should provide all the requirements for this as part of this solution. **ReBIT will provide the Public IP addresses required from its internal pool.**
28	17.4 Performance	The solution related minimum service expectation as a percentage of	The solution related minimum service expectation as a percentage of "Business

Page No	Clause No	Existing Terms	Corrigendum / Revised Terms
	Tracking and Reporting	"Business Utility" is of 99.99% to be calculated on monthly basis.	Utility" is of **99.95%** to be calculated on monthly basis.
47	Annexure – H Technical Specifications , S.No 9	**Requirement specification:** The solution should be able to create decoys for platforms like: ·Windows ·Linux ·MacOS ·Public cloud IaaS (AWS, Azure) ·IoT devices (Printers, CCTV, etc.) ·Network Devices (Routers, Switches etc.) **Requirement categorisation** Must Have	**Requirement specification:** The solution should be able to create decoys for platforms like: ·Windows ·Linux ·MacOS **(Optional)** ·Public cloud IaaS (AWS, Azure) ·IoT devices (Printers, CCTV, etc.) ·Network Devices (Routers, Switches etc.) **Requirement categorisation** Must Have
47	Annexure – H Technical Specifications , S.No 14	**Requirement specification:** The solution needs to have an active detection system that will detect/highlight attacks based on **signatures** **Requirement categorisation** Business Critical	**Requirement specification:** The solution should have an active detection system to detect both **signatures and signatureless attack.** **Requirement categorisation** Business Critical
47	Annexure – H Technical Specifications , S.No 15	**Requirement specification:** The solution needs to have an active detection system that will detect/highlight attacks based on **pattern or behaviour** **Requirement categorisation** Business Critical	**Requirement specification:** The solution should have an active detection system that will detect/highlight any **attacks based on decoy.** **Requirement categorisation** Business Critical
48	Annexure – H Technical Specifications , S.No 20	**Requirement specification:** The solution should have capability to dynamically deploy decoy or modify a decoy to lure the attacker as per attack technique. **Requirement categorisation** Business critical	**Requirement specification:** The solution should have capability to **dynamically or manually** deploy decoy or modify a decoy to lure the attacker as per attack technique. **Requirement categorisation** Business critical
49	Annexure – H Technical Specifications , S.No 28	**Requirement specification:** Solution should provide **granular control** over decoys in each network segment. In addition, should provide capability to turn off or on all decoys in a particular group/ network segment.	**Requirement specification:** Solution should provide granular control over decoys in each network segment. In addition, solution should provide capability to **turn off all decoys or whitelist services** in a particular group/ network segment"

Page No	Clause No	Existing Terms	Corrigendum / Revised Terms
		Requirement categorisation Good to have	**Requirement categorisation** Good to have
49	Annexure – H Technical Specifications , S.No 30	**Requirement specification:** The solution should be capable of creating decoy processes on the endpoint with custom name and path. **Requirement categorisation** Business Critical	**Requirement specification:** The solution should be capable of **protecting end point devices by creating decoy with custom name and path or through any other means. Additionally, deception technology solution should not expose processes of the endpoint.** **Requirement categorisation** Business Critical
49	Annexure – H Technical Specifications , S.No 31	**Requirement specification:** The endpoints with Windows OS, deception should be able to detect attempts to **access Answer file** within the OS. **Requirement categorisation** Business Critical	**Requirement specification:** The endpoints with Windows OS, deception should be able to detect attempts to access Answer file within the OS **for agent-based solution.** **Requirement categorisation** Business Critical
49	Annexure – H Technical Specifications , S.No 32	**Requirement specification:** Deception platform must be capable of creating file decoys that are deployed on real systems and trigger alerts not only when opened but also when copied, modified and deleted **Requirement categorisation** Good to have	**Requirement specification:** Deception platform should be capable to create file decoys that are deployed on real systems and trigger alerts **when any anomalous activities observed on it.** **Requirement categorisation** Good to have
50	Annexure – H Technical Specifications , S.No 40	**Requirement specification:** The solution should have some technique to cater to **Phishing email**. The bidder shall explain the technique in Remarks. **Requirement categorisation** Business Critical	**This requirement stands deleted.**
50	Annexure – H Technical Specifications , S.No 42	**Requirement specification:** The solution should have the ability to record the screen in a video or screenshots (state which option is available) and must also capture keystrokes and mouse movements for	**Requirement specification:** The solution should have the ability to record the attack lifecycle in a video or screenshots or any other way (state which option is available) and provide a downloadable report of the attacker's activity in the decoy.

Page No	Clause No	Existing Terms	Corrigendum / Revised Terms
		hi-interaction remote desktop connections on Windows decoys and provide a downloadable video replay with keystroke capture of the attacker's activity in the decoy. **Requirement categorisation** Good to have	**Requirement categorisation** Good to have
52	Annexure – H Technical Specifications , S.No 55	**Requirement specification:** The solution should provide a **sinkhole capability** to redirect the attacker and allow the attack to develop and progress. **Requirement categorisation** Business Critical	**Requirement specification:** **The solution should be configured in such way that the attacker is not able to go back to the compromised endpoint or able to make lateral movements behind the deception environment.** **Requirement categorisation** Business Critical
52	Annexure – H Technical Specifications , S.No 56	**Requirement specification:** The solution should have an inbuilt feature to allow automatic isolation of an attacking source system based on preset or custom rules. This should be possible without relying on integrations to external systems. **Requirement categorisation** Business critical	**Requirement specification:** The solution should have an inbuilt feature to allow automatic isolation of an attacking source system based on pre-set or custom rules. This should be possible without relying on integrations to external systems or with integrations to external system such as EDR and firewall. **Requirement categorisation** Business critical
53	Annexure – H Technical Specifications , S.No 61	**Requirement specification:** The solution should automatically recommend un-listed subdomains to be deployed as decoys. **Requirement categorisation** Business critical	**Requirement specification:** The solution should automatically**/manually recommend** un-listed subdomains to be deployed as decoys **and it should also be able to prevent domain and subdomains enumeration and reconnaissance attempts both external and internal.** **Requirement categorisation** Business critical
53	Annexure – H Technical Specifications , S.No 62	**Requirement specification:** The solution should allow the user to choose from various server and versions for each un-listed subdomain. **Requirement categorisation** Business critical	**Requirement specification:** The solution should allow the user to choose **automatically/manually** from various server and versions for each un-listed subdomain. **Requirement categorisation** Business critical

Page No	Clause No	Existing Terms	Corrigendum / Revised Terms
53	Annexure – H Technical Specifications, S.No 68	**Requirement specification:** The solution must use a numeric risk score for each attacker based on dynamic analysis of attacker behaviour. **Requirement categorisation** Business critical	**Requirement specification:** The solution should use a numeric risk score and MITRE mapping for each attacker based on dynamic analysis of attacker behaviour. **Requirement categorisation** Business critical
53	Annexure – H Technical Specifications, S.No 70	**Requirement specification:** Besides email alerts, the solution shall have the built in ability for real-time voice phone calls and SMS alerts based on preset or custom notification rules **Requirement categorisation** Good to have	**Requirement specification:** The solution should have feature to send alert through e-mails for attack based on pre-set or custom notification rules. **Requirement categorisation** Good to have
54	Annexure – H Technical Specifications, S.No 76	**Requirement specification:** Reports should be downloadable in excel and PDF format. **Requirement categorisation** Must Have	**Requirement specification:** Report should be downloadable in excel or PDF format. **Requirement categorisation** Must Have
54	Annexure – H Technical Specifications, S.No 79	**Requirement specification:** Solution should be able to whitelist authorized IP addresses and applications based on Hashes, certificate, and PE header. **Requirement categorisation** Must Have	**Requirement specification:** Solution should be able to whitelist authorized IP addresses and applications based on **services or Hashes or certificate or PE header.** **Requirement categorisation** Must Have
54	Annexure – H Technical Specifications, S.No 83	**Requirement specification:** Automatically create deceptions in accordance with organizational naming conventions **Requirement categorisation** Must Have	**Requirement specification:** **Automatically or manually** create deceptions in accordance with organizational naming conventions. **Requirement categorisation** Must Have
58	Annexure M: Bank Guarantee for EMD, First paragraph	M/s _____ having their registered office at _____ (hereinafter called the "Bidder") wish to respond to the Request for Proposal (RFP) for Setup and Implementation of RSB, self and other associated Bidders	M/s _____ having their registered office at _____ (hereinafter called the "Bidder") wish to respond to the Request for Proposal (RFP) for Setup and Implementation of **Deception Technology**, self and other associated

Page No	Clause No	Existing Terms	Corrigendum / Revised Terms
		and submit the proposal for the same as listed in the RFP document.	Bidders and submit the proposal for the same as listed in the RFP document.

Please read the aforesaid corrigendum along with the issued RFP document. All other terms and conditions which are not covered in this Corrigendum, will be as per the original RFP - Setup and Implementation Of Deception Technology Ref: ReBIT/2021 / CPO / 031 dated 16th March 2021.

Setup and Implementation Of Deception Technology

REQUEST FOR PROPOSAL (RFP)

RESPONSE TO PRE-BID QUERIES

(31st March 2021)
RFP: ReBIT/2020 / CPO / 031

Sr. No	Query Reference (Page)	Query Reference (Clause)	Existing clause of the RFP	Query by the Vendor	ReBIT's Response
1	49	28	Solution should provide granular control over decoys in each network segment. In addition, should provide capability to turn off or on all decoys in a particular group/ network segment.	Technically, It is not recommended to give a open window to attacker by not providing resources in the necessary network segment. However, Deception technology will not impact your existing production environment. We request to amend this clause for should provide capability to turn off and turn on, to it should not impact given network segment during any maintenance activities.	Solution should provide granular control over decoys in each network segment. In addition, solution should provide capability to turn off all decoys or whitelist services in a particular group/ network segment". Please refer Corrigendum # 1.
2	53	61	The solution should automatically recommend un-listed subdomains to be deployed as decoys.	This clause is specific to one OEM and restricting / disallowing fair participation for other Deception Technology (DT) OEM's.	The solution should automatically/manually recommend un-listed subdomains to be deployed as decoys and it should also be able to prevent domain and subdomains enumeration and reconnaissance attempts both external and internal. Please refer Corrigendum # 1.
3	53	62	The solution should allow the user to choose from various server and versions for each un-listed subdomain.	This clause is specific to one OEM and restricting / disallowing fair participation for other Deception Technology (DT) OEM's.	The solution should allow the user to choose automatically/manually from various server and versions for each un-listed subdomain. Please refer Corrigendum # 1.
4	53	63	The solution should allow custom decoy SSL certificate upload for each unlisted subdomain	This clause is specific to one OEM and restricting / disallowing fair participation for other Deception Technology (DT) OEM's.	This is an independent requirement. Not associated with other specifications. Hence, no Change
5	53	68	The solution must use a numeric risk score for each attacker based on dynamic analysis of attacker behaviour.	This clause is specific to one OEM and restricting / disallowing fair participation for other Deception Technology (DT) OEM's.	“The solution should use a numeric risk score and MITRE mapping for each attacker based on dynamic analysis of attacker behaviour”. Please refer Corrigendum # 1.

Sr. No	Query Reference (Page)	Query Reference (Clause)	Existing clause of the RFP	Query by the Vendor	ReBIT's Response
6	54	79	Solution should be able to whitelist authorized IP addresses and applications based on Hashes, certificate and PE header	This clause is specific to one OEM and restricting / disallowing fair participation for other Deception Technology (DT) OEM's.	Solution should be able to whitelist authorized IP addresses and applications based on services or Hashes or certificate or PE header. Please refer Corrigendum # 1.
7	9	5.3	Warranty should not become void if ReBIT buys any other supplemental hardware from a third party and installs them with this hardware. However, the warranty will not apply to such supplemental hardware items installed.	This clause need to removed. As our solution is appliance based and as a manufacture it is not recommended to open appliance or do any changes without valid downtime and approval from support.	Any supplemental hardware shall be installed with the appliance/hardware as per OEM's recommendation. No change in this clause.
8	10	5.4.2	Selected bidder has to design the solution with high availability at secure infrastructure in Data Centre as per Industry accepted security standards and best practices. Bidder also has to recommend which component of the proposed DECEPTION TECHNOLOGY solution should fit into what network zone as per best industry practices considering the organizational business requirements.	In this clause we need to understand, whether solution need to be placed in Active/Stand-by mode or Active/Cold Stand-by Mode.	Bidder may provide suitable solution catering to the High Availability (Active/Cold Standby) needs of ReBIT. Bidder has only to ensure that solution is deployed in such a way that it meets the SLA requirement in terms of uptime.
9	11	5.4.3	Setting up of test environment at ReBIT will be Bidder's responsibility.	In this clause , we need to understand whether we need to provision separate appliance for UAT testing or we will be preforming testing on proposed appliance and after all necessary testing same will be added to Go-live for production.	No separate testing environment is needed. Testing on proposed appliance will be performed as a part of UAT and post that same set of component will be deployed in Go-live for production.

Sr. No	Query Reference (Page)	Query Reference (Clause)	Existing clause of the RFP	Query by the Vendor	ReBIT's Response
10	43	point 5 (eligibility Criteria) Annx E	The bidder should have executed 2 or more projects of size 400 user systems each of the proposed OEM's Solution in the last 3 years and should be go-live as on 31-12-2020. A) Bidder to submit documentary evidence such as satisfaction/ credential letter from the client clearly stating the scope of work and project value OR Completion letter from the client indicating the scope of work executed by the Bidder and the project value. B) Contract / PO Copy as documentary evidence proving project value. The onus of proving the credential via documentary evidence is of the Bidder. In case, the Bidder is unable to provide any of the above, it will be the ReBIT's discretion to evaluate the claim in this regard.	This is a niche technology and in large accounts customers demand the implementation from OEM only. So It is difficult for bidder to provide completion letter / credential letter. We request that ReBIT should ask references from both Bidder and OEM. For Bidder, PO copies of at least 2 projects and from OEM PO copies + sign off/ completion email or letter from any of their two clients	If the OEM's implementation reference is provided, then the bidder shall provide along with the bid submission a declaration and certification from the OEM that "OEM will do the implementation, support and all deliverables at ReBIT as per the RFP. OEM shall be liable for all the terms and conditions of the RFP". Also, the OEM team details who will work on this project shall be provided as per Annexure - L. PO shall be issued in the name of the bidder. Please refer Corrigendum # 1
11		Suggestion	Suggestion	Detect MITM attacks like NBNS, LLMNR, MDNS, ARP, DHCP in every VLAN of the enterprise including branch and remote offices without deploying additional appliance. MITM is a technique that is followed widely by attackers to steal credentials and the deception product should detect MITM attacks in every VLAN since initial compromise can happen in any VLAN. This feature allows for the ability to detect an attack where the attacker secretly relays and possibly alters the communication on these protocols between two endpoints who believe they are directly communicating with each other.	No change

Sr. No	Query Reference (Page)	Query Reference (Clause)	Existing clause of the RFP	Query by the Vendor	ReBIT's Response
12		Suggestion	Suggestion	API Integration with the existing solution like NGFW , SIEM , NAC etc. This helps the client to take an remediation step on the attack detected.	No Change
13		Suggestion	Suggestion	Solution should redirect attackers to the decoys without configuring IP Addresses in each VLAN and thereby taking over all dark IP's. The effectiveness of a deception solution is highly dependent on its ability to lure an attacker inside the network. This feature effectively increases the scale of deception by converting the unused IP address space into deception IP addresses and also helps detect an attacker inside the network during the lateral movement stage itself.	No Change
14		Suggestion	Suggestion	Remediate the exposed credentials at endpoints to decrease attack surface available for an attacker in the enterprise This feature helps to remediate the exposures in your environment that is increasing your attack surface. Remediate lateral movement paths that are exposed in your network and making your crowned jewels vulnerable to attacks.	No change
15		Suggestion	Suggestion	Deploy deceptive kerberos tickets as breadcrumbs to the real endpoints Microsoft’s Kerberos implementation in Active Directory has been targeted over the past couple of years by security researchers and attackers alike. This feature enables to distribute Kerberos tickets to real endpoints to deceive, detect and defend the attackers who harvest these tickets for moving laterally once they have a beachhead inside the network.	No Change

Sr. No	Query Reference (Page)	Query Reference (Clause)	Existing clause of the RFP	Query by the Vendor	ReBIT's Response
16		Suggestion	Suggestion	Solution must support auto refresh of fake credentials at the end points to make the credentials look alive and real. When a system is compromised, the attacker first looks for credential and the time stamp on the credentials. A stale credential is a give-away of deception and easily circumvented by attacker. Credentials without updated time stamps are like dead bait and actually are counter productive to deception strategy.	No Change
17		Suggestion	Suggestion	Deceive attackers who employ advanced attack techniques like kerberoasting to compromise privileged credentials. Advanced Persistent Threats are constantly seeking privileged credentials in the network to ensure they are able to move freely in the network. Putting Kerberoasting lures in your production DC, you will be able to safeguard your privileged credentials against theft of credentials.	No Change
18		Suggestion	Suggestion	Solution must support built-in Sandbox capabilities to identify the TTP of the attacker. This feature helps the client to understand the exact behaviour of a payload and the TTP used by the attacker.	No change
19		Suggestion	Suggestion	The solution should be capable of hiding real privilege domain credentials like domain admins, administrators, enterprise admins and schema admins and present deceptive data pointing to decoys upon querying via commands and tools. This feature helps to prevent any attack on the Active Directory. The attacker would be presented with fake credentials while performing an recon and thus helps in thwarting an attack.	No Change

Sr. No	Query Reference (Page)	Query Reference (Clause)	Existing clause of the RFP	Query by the Vendor	ReBIT's Response
20		Suggestion	Suggestion	The solution should be capable of hiding real service accounts in and present deceptive data for the same. This feature helps the client to protect their service accounts from being used by any adversary. The adversary would be fed with deceptive credentials and lured on usage of these credentials.	No Change
21		Suggestion	Suggestion	The solution should be capable of hiding real domain controllers and present deceptive data for the same upon querying via commands from nltest and powershell. Domain controllers are on the critical assets inside an organisation. By this feature the clients can protect any attack towards the Domain controllers. The attacker would be presented with false credential to trap/lure in the decoys.	No Change
22		Suggestion	Suggestion	The system should support deflecting attacker traffic scanning non existing services on real systems endpoint to decoys. This capability provides protection from advanced attackers using targeted reconnaissance to reach their targets.	No Change
23		Suggestion	Suggestion	The system should support quarantining the infected endpoints automatically. This feature helps the administrator to isolate respective infected endpoint from spreading the malware actions on other endpoint in the network.	No Change
24			The bidder should have executed 2 or more projects of size 400 user systems each of the proposed OEM's Solution in the last 3 years and should be go-live as on 31-12-2020.	We request to the Bank to consider for one project of size 200 user systems of the proposed OEM solution in the last three years	No change in the criteria.

Sr. No	Query Reference (Page)	Query Reference (Clause)	Existing clause of the RFP	Query by the Vendor	ReBIT's Response
25	47	Capability - Point 9	The solution should be able to create decoys for platforms like: •Windows •Linux •MacOS •Public cloud IaaS (AWS, Azure) •IoT devices (Printers, CCTV, etc.) •Network Devices (Routers, Switches, etc.)	What is the purpose of network devices? Pls help us to understand. Public cloud IaaS would be windows or linux servers, let us know if ReBIT is having different understanding here. Currently we don't support MacOS. Pls accept the same.	Beside below platform, deception solution should be able to create decoy for network infrastructure such as routers and switches, telecommunications devices, applications and services. •Windows •Linux •MacOS (Optional) •IoT devices (Printers, CCTV, etc.) •Public cloud IaaS •HCI based private cloud Please refer Corrigendum # 1
26	47	Capability - Point 11	"The solution should be able to create decoys for applications like •Browsers •Database •Scanners •FTP •Files •Emails •Network protocols •RDP •Recent connections •SSH •Scripts •Share drives •Windows credentials/Active Directory"	We don't have separate decoy for browser as it is already part of windows decoy. Pls accept the same. Scanning is a behaviour that we need to identify. What is the purpose of asking Scanner Decoy? Services for Windows include RDP, SMB, and TCPLISTENER. Services for SCADA include HTTP, FTP, TFTP, SNMP. Services for ubuntu include SSH, SAMBA, and TCPLISTENER. Pls accept the same.	If the browsers are supported through windows decoy it could be considered as compliant. Printing and scanning both operations are performed by single device hence it is expected to have decoy for this device which covers both the activities.
27	48	Capability - Point 20	"The solution should have capability to dynamically deploy decoy or modify a decoy to lure the attacker as per attack technique"	Requesting to make it dynamically or manually.	The solution should have capability to dynamically or manually deploy decoy or modify a decoy to lure the attacker as per attack technique. Please refer Corrigendum # 1.
28	48	Capability - Point 23	"The solution should have a central management console to manage the deployment and event notifications. All other components should be controlled and configured through the central management console only."	As of now we don't have central management tool to manage multiple appliances. So remove this clause so that we can participate.	No Change

Sr. No	Query Reference (Page)	Query Reference (Clause)	Existing clause of the RFP	Query by the Vendor	ReBIT's Response
29	49	Capability - Point 30	The solution should be capable of creating decoy processes on the endpoint with custom name and path.	A token is created on Endpoint which redirect to decoy. What is need to make a genuine endpoint a decoy ?	The solution should be capable of protecting end point devices by creating decoy with custom name and path or through any other means. Additionally, deception technology solution should not expose processes of the endpoint. Please refer Corrigendum # 1
30	49	Capability - Point 32	Deception platform must be capable of creating file decoys that are deployed on real systems and trigger alerts not only when opened but also when copied, modified and deleted	This is the functionality of File Integrity Monitoring solution. What is the reason of asking on Deception? Requesting to remove the clause as it will stop other OEMs from bidding.	Deception platform should be capable to create file decoys that are deployed on real systems and trigger alerts when any anomalous activities observed on it. Please refer Corrigendum # 1.
31	43	Point 5	The bidder should have executed 2 or more projects of size 400 user systems each of the proposed OEM's Solution in the last 3 years and should be go-live as on 31-12-2020.	Please consider Bidder or OEM should have executed similar projects in the last 3 years and should be go-live as on 31-12-2020.	Please refer response to S.No 10
32	7	5.2.8	Internet decoys also need to be solutioned as part of this solution and the vendor should provide all the requirements for this as part of this solution.	Please confirm if REBIT to confirm if these internet decoys can be deployed in Smokescreen's cloud infra? If yes, would REBIT require a separate management console for these decoys or would provide connectivity from the management console in the DC to the appliance in Smokescreen's cloud? If not, will REBIT be able to trunk DMZ VLAN to our appliance and also provide a public IP from their DMZ?	Internet decoys also need to be solutioned as part of this solution and the vendor should provide all the requirements for this as part of this solution. ReBIT will provide the Public IP addresses required from its internal pool. Please refer Corrigendum # 1.
33	8	5.2.14	There should not be any restriction on number of decoys that can be created based on the licensing.	Request REBIT to remove this clause, as some of the decoys such as Network decoys and Private Threat Intelligence decoys (Internet decoys) require resources to run, hence the license will also be restricted based on requirement.	The solution should be designed to cater the Deception technology requirement for 1 Office location with 1 Data center, 10 network zones including DMZ, guest Wi-Fi and 400 end point systems scalable to 2 office locations with 1000 end point systems in 3 years

Sr. No	Query Reference (Page)	Query Reference (Clause)	Existing clause of the RFP	Query by the Vendor	ReBIT's Response
34	8	5.3	Hardware shall be provided on subscription basis.	Please clarify the expectation as if it is on OPEX mode, hardware won't be on ReBIT name. Also there is no Payment Terms mentioned in Opex Mode.	The hardware and software licenses including OS proposed in the solution should be procured in the name of ReBIT and will remain the property of ReBIT during the contract period. Licensing of appliance/hardware should be based on subscription basis and payment for the same will be released as per the payment terms. Please refer Corrigendum # 1.
35	9	5.3 Hardware requirements	Warranty should not become void if ReBIT buys any other supplemental hardware from a third party and installs them with this hardware. However, the warranty will not apply to such supplemental hardware items installed.	Request Rebit to remove this Clause since none of the Hardware OEM's will support this clause.	Please refer response at S.No 7
36	11	5.4.6.1	Bidder can use the ReBIT test hardware which is provided for this project for UAT.	Request REBIT to confirm if the appliances provided by Smokescreen can be used for both - UAT and Production. Meaning, appliances will be deployed for UAT first and then after getting the UAT completion certificate from REBIT, the same appliances will be used for Production as well.	Hardware/appliance will be used first to perform test (UAT) and once UAT has successfully completed and accepted by ReBIT, same will be deployed in production environment
37	11	5.4.4	Backup and Archiving	Please confirm whether backup and archival infra will be provided by ReBIT	Solution should be able to use ReBIT existing backup solution for backup and archival purpose
38	12	5.4.8	ReBIT expects the Bidder to train the administrator/ business users till the personnel gain enough expertise in the system and capable of taking over the training function.	Request ReBIT to quantify training requirement i.e. no of training instances/days and batch size so that bidder can cost it properly. Please confirm whether training class and refreshment will be arranged by ReBIT.	Bidder/OEM is expected to train ReBIT's resources during the implementation stage, before Go-live to ReBIT's satisfaction as per this feedback from the trainees. If the feedback is not satisfactory, the bidder shall repeat the training. Hand holding training to be provided to at least 5 users to manage the solution. Training can be provided on-line or in class room.

Sr. No	Query Reference (Page)	Query Reference (Clause)	Existing clause of the RFP	Query by the Vendor	ReBIT's Response
39	14	5.6 Project Milestones	1. Receipt of Software and Hardware--Receipt of all necessary Software and hardware for Deception technology.---4 to 6 weeks from PO---Payment-10% of Hardware and Software Cost. (S. No. 1 and 2 of Annexure I - Price Bid Format) 2. Implementation upto Go Live as mentioned in section 5.4---• Install hardware and software. • VAPT Compliance sign off • Completion of ReBIT audit • Fixing observations • Completion of Security risk assessments • User and Technical Documentation • Client Training Feedback from Users • Client Handbook • E-Learning • Other scope as mentioned at 5.3 • Go-live certificate 6 to 8 weeks from delivery. Payment -90% of Hardware and Software Cost (S. No. 1 and 2 of Annexure I - Price Bid Format)	Request ReBIT to include the "Site Not Ready " clause also part of the Payment Terms if applicable. Clause as " if the site is not ready for installation from purchaser side for 15 days from the date of delivery , Purchaser will release 100% of the Product payment towards the same on submission of Invoice , Delivery acknowledgement. It will be bidder responsibility to complete the implementation once site is ready"	ReBIT will make all efforts to provide the site ready as per the project milestones. No change in this clause related to site readiness.
40	27	17.1 Purpose and Objective of SLA	The Bidder should provide SLA monitoring tool/system which will be used for monitoring SLA based on the SLA defined.	Request ReBIT to remove this clause as the proposed solution will integrate with existing SLA monitoring tool. Giving dedicated SLA monitoring tool for Deception solution is not cost effective option.	The Bidder's solution should be capable to provide a dashboard based view which can be used to review and measure the SLAs defined.

Sr. No	Query Reference (Page)	Query Reference (Clause)	Existing clause of the RFP	Query by the Vendor	ReBIT's Response
41	34	30. No Employer-Employee Relationship	The Bidder or any of its holding/subsidiary/joint-venture/ affiliate / group / client companies or any of their employees / officers / staff / personnel / representatives / agents shall not, under any circumstances, / be deemed to have any employer-employee relationship with the ReBIT or any of its employees /officers / staff / representatives / personnel / agents. A self-declaration is required from the Bidder as part of the technical bid.	Request Rebit to share the list of Employee Details to verify this from Bidder Side.	Bidder is required to verify the same as per its employees and provide self-declaration in the format provided at Annexure - C as per the RFP
42	51	Annexure H - 44	Solution should have the ability to create specialised Internet facing decoys to detect external reconnaissance of Internet facing websites. These decoys should only respond to requests on HTTP/HTTPS and only for their requests to the configured domain names. The Internet facing decoys should consume backscatter threat intelligence from platforms like MISP, Grey noise, Shodan etc.It should not respond to the scans on the IP addresses. (If internet facing decoys require public IP addresses then this solution should be provisioned to provide public IP address by the Bidder and cost for the same shall be bourne by the bidder. Public IP address shall be provided by the bidder.)	Please confirm if REBIT to confirm if these internet decoys can be deployed in Smokescreen's cloud infra? If yes, would REBIT require a separate management console for these decoys or would provide connectivity from the management console in the DC to the appliance in Smokescreen's cloud? If not, will REBIT be able to trunk DMZ VLAN to our appliance and also provide a public IP from their DMZ as the IP should be from same range?	Please refer response to S.No 32.
43	7	5.2.1	Bidder shall provide complete on premise DECEPTION TECHNOLOGY solution which will be required to detect and report attacks on decoys systems deployed through this solution	Request REBIT to confirm if they would prefer OnPrem VM or Hardware appliances?	Bidder shall provide complete on premise DECEPTION TECHNOLOGY . solution which will be required to detect and report attacks on decoys systems deployed through this solution. On Prem VM or Hardware appliances both are acceptable

Sr. No	Query Reference (Page)	Query Reference (Clause)	Existing clause of the RFP	Query by the Vendor	ReBIT's Response
44	7	5.2.6	The solution should be designed to cater the Deception technology requirement for 1 Office location with 1 Datacenter, 10 network zones including DMZ, guest Wi-Fi and 400 end point systems scalable to 2 office locations with 1000 end point systems in 3 years.	Request REBIT to confirm if all the 10 Network Zones, DMZ / Guest WIFI VLANs can be trunked into our deception appliance in the DC? This will help us understand how many such appliances would be required. These appliances are used for creating network decoys in the network segments / VLANs.	As per industry best practices, bidder should decide and propose number of appliances/ hardware component required to cater ReBIT need to 1 Office location with 1 Datacenter, 10 network zones including DMZ, guest Wi-Fi and 400 end point systems scalable to 2 office locations with 1000 end point systems in 3 years.
45	13	5.5.2	Remote access would not be permitted.	Request REBIT to provide remote access in case any support required for initial troubleshooting.	Initial troubleshooting will be performed over call or email but if the issue not fixed by these means, engineer from the bidder has to visit ReBIT office and fix the issue. No remote access will be provided to trouble shoot the issues
46	48	Annexure H - 20	The solution should have capability to dynamically deploy decoy or modify a decoy to lure the attacker as per attack technique	Request REBIT to remove this point as dynamically deploying decoys may cause internal IP conflict in the network.	Please refer response to S.No 27
47	52	Annexure H - 53	The Solution should have a sandbox where suspicious attacks can be sent for deep investigation. Sandbox should be isolated virtually or physically. The bidder shall mention if Sandbox is on cloud in Remarks column.	Please confirm if integrations with state of the art sandboxes for this use case will be applicable?	Integration with state of art sand boxes can be considered. Bidder has to clearly call out in their technical proposal that how these sandboxes will work and be integrated with deception technology and what payload will be sent for analysis.
48	52	Annexure H - 56	The solution should have an inbuilt feature to allow automatic isolation of an attacking source system based on preset or custom rules. This should be possible without relying on integrations to external systems	Request REBIT to consider this modifying this point to allow isolation through integrations with Firewall/EDR as well.	The solution should have an inbuilt feature to allow automatic isolation of an attacking source system based on preset or custom rules. This should be possible without relying on integrations to external systems or with integrations to external system such as EDR and firewall. Please refer Corrigendum # 1.

Sr. No	Query Reference (Page)	Query Reference (Clause)	Existing clause of the RFP	Query by the Vendor	ReBIT's Response
49	53	Annexure H - 67 & 68	Solution should have basic critical / high / medium / low categorization for incidents/attacks. The solution must use a numeric risk score for each attacker based on dynamic analysis of attacker behaviour.	Points 67 & 68 are contradictory, request REBIT to make them optional and recategorise them as "business critical"	Specification no 67 is a Must Have requirement where as Specification no 68 is Business Critical for which score will be provided if the proposed solution has this feature.
50	54	Annexure H - 75	Reports should contain charts and be customizable	Request REBIT to consider reports without charts	Reports should contain statistics of incident and trend etc. It should also be custmizable
51	54	Annexure H - 76	Reports should be downloadable in excel and PDF format.	Request REBIT to consider reports downloadable in excel format and also please recategorise this point as "Good to have"	Report should be downloadable in excel or PDF format. Please refer Corrigendum # 1.
52	54	Annexure H - 83	Automatically create deceptions in accordance with organizational naming conventions	Request REBIT to remove this point, as this will require the solution to run scans on the network and may cause network bandwidh issues.	Automatically or manually create deceptions in accordance with organizational naming conventions. Please refer Corrigendum # 1.
53	48	Annexure H	NA	Request REBIT to provide the excel sheet for Annexure H	The Bidder pay convert the PDF, if required.
54	43	Annexure G	The bidder should have executed 2 or more projects of size 400 user systems each of the proposed OEM's Solution in the last 3 years and should be go-live as on 31-12-2020.	Request REBIT to change this clause to: The bidder/ OEM should have executed 2 or more projects of size 400 user systems each of the proposed OEM's Solution in the last 3 years and should be go-live as on 31-12-2020.	Please refer response to S.No 10
55	27	17.1 Purpose and Objective of SLA	The Bidder should provide SLA monitoring tool/system which will be used for monitoring SLA based on the SLA defined.	Request REBIT to amend this statement to: The Bidder should provide portal and ticketing system through which the data will be provided to measure the SLA's	Please refer response to S.No 40.
56	28	17.4 PerformanceTrackingandReporting	The solution related minimum service expectation as a percentage of "Business Utility" is of 99.99% to be calculated on monthly basis.	Request REBIT to consider the below amendment to the clause: "minimum service expectation as a percentage of "Business Utility" is of 99.95%, barring any physical interruptions to the appliance on premise"	The solution related minimum service expectation as a percentage of "Business Utility" is of 99.95% to be calculated on monthly basis. Please refer Corrigendum # 1.

Sr. No	Query Reference (Page)	Query Reference (Clause)	Existing clause of the RFP	Query by the Vendor	ReBIT's Response
57	14	5.6 Project Milestones	**Receipt of Software and Hardware** - 10% of Hardware and Software Cost. (S. No. 1 and 2 of Annexure I - Price Bid Format) **Implementation upto Go Live as mentioned in section 5.4** - 90% of Hardware and Software Cost (S. No. 1 and 2 of Annexure I - Price Bid Format) **30 days after GoLive** - 100% of Implementation cost for Year 1 (S. No. 3 of Annexure I – Price Bid Format)	Request REBIT to change the Payment terms to: **Receipt of Software and Hardware -** 70% of Hardware & Software cost (S. No. 1 and 2 of Annexure I - Price Bid Format) on delivery **Implementation upto Go Live as mentioned in section 5.4 -** 30% of Hardware and Software Cost (S. No. 1 and 2 of Annexure I - Price Bid Format) on Go live.	**Receipt of Software and Hardware** - 50% of Hardware & Software cost for Year 1(S. No. 1 and 2 of Annexure I - Price Bid Format) on delivery and acceptance. **Implementation upto Go Live as mentioned in section 5.4 -** 50% of Hardware and Software Cost for Year 1(S. No. 1 and 2 of Annexure I - Price Bid Format). Please refer Corrigendum # 1
58		To Be Added	Preference to Make in India Clause to Be Added	**Request REBIT to add the Preference to Make in India clause:** ReBIT will follow the guidelines on Public Procurement (Preference to Make in India), Order 2017 (PPP-MII Order), Order No. P-45021/2/2017-BEII dated 15.06.2017, as amended by Order No. P-45021/2/2017-BE-II dated 28.05.2018 and Order No. P-45021/2/2017-BE-II dated 29.05.2019 and revision issued vide letter No. P-45021/2/2017(BE-II) dated 04.06.2020.	No change in the RFP with respect to this criteria
59	47	10	Specify if the solution is able to create decoys for Security solutions like Anti- Virus, Firewall, IPS/IDS, email gateway security, SIEM.	This clause is proprietary to a particular to OEM, all other OEM's had different technology. Requested you to kindly make it open " as per offered solution".	Solution should have feature to create decoy or detect attacks through any possible mechanisms impersonating security solution such as Anti virus, Firewall, IPS/IDS, email gateway security and SIEM etc.
60	47	14	The solution needs to have an active detection system that will detect/highlight attacks based on signatures	Now a Days new deception solutions are not based on signatures. Requested you to kindly make it signature less.	The solution should have an active detection system to detect both signatures and signatureless attack. Please refer Corrigendum # 1.

Sr. No	Query Reference (Page)	Query Reference (Clause)	Existing clause of the RFP	Query by the Vendor	ReBIT's Response
61	47	15	The solution needs to have an active detection system that will detect/highlight attacks based on pattern or behaviour	New deception solutions are not based on pattern. If the attacker uses the lures, that will be kind of "behaviour". And we monitor his behaviour on the decoy. Requested you to amend the clause from pattern or behaviour to Decoy.	The solution should have an active detection system that will detect/highlight any attacks based on decoy. Please refer Corrigendum # 1.
62	49	30	The solution should be capable of creating decoy processes on the endpoint with custom name and path.	This is proprietary feature of a particular OEM. Requested you to kindly amend the clause Deception technology solution should not expose processes on the endpoint.	Please refer response to S.No 29
63	49	31	The endpoints with Windows OS, deception should be able to detect attempts to access Answer file within the OS.	This is proprietary feature of a particular OEM. The concept of the Deception technology is agent less and thus does not cause actions (like file inspection) on the endpoints. Requested you to kindly amend the this point and make it generic, so that you get better solution and healthy competition.	Solution should be able to detect access to answer file within operating system. The endpoints with Windows OS, deception should be able to detect attempts to access Answer file within the OS for agent based solution. Please refer Corrigendum # 1.
64	50	40	The solution should have some technique to cater to Phishing email. The bidder shall explain the technique in Remarks.	Phishing solution is a separate technology and where as per the specs it's a tender for Deception Technology. Requested you to kindly remove this point, so that other OEM's can participate and it's not restricted to one OEM.	This clause can be removed. Please refer Corrigendum # 1.

Sr. No	Query Reference (Page)	Query Reference (Clause)	Existing clause of the RFP	Query by the Vendor	ReBIT's Response
65	50	42	The solution should have the ability to record the screen in a video or screenshots (state which option is available) and must also capture keystrokes and mouse movements for hi-interaction remote desktop connections on Windows decoys and provide a downloadable video replay with keystroke capture of the attacker's activity in the decoy.	Based on our understanding you are looking for a feature where system records the attackers behaviour and you want to analyze the video. New Deception technology never allow the attacker to enter your active network. The feature which you had asked was available when Honeypot technology came in the international market. This is proprietary feature of a particular OEM. Requested you to kindly amend this feature or delete this. Requested you to include feature – Attacker should not be allowed to enter the active network, once its detected.	The solution should have the ability to record the attack lifecycle in a video or screenshots or any other way (state which option is available) and provide a downloadable report of the attacker's activity in the decoy. Please refer Corrigendum # 1
66	52	52	For security, the base operating platform (host operating platform on which the decoys run) of the deception appliance should be secured and should not have vulnerabilities like those of decoys.	This feature is specific to one or Two OEM's which are selling appliance based solution and other OEM's will not be able to participate in this tender. Requested you to kindly make it generic, for making other OEM's to participate in this tender.	Base operating system of deception technology appliance/VMs should be secured and free from any known bugs or vulnerabilities
67	52	55	The solution should provide a sinkhole capability to redirect the attacker and allow the attack to develop and progress.	This technique is old technology. Requested you to kindly amend it with" The solution should be configured in a way, that the attacker is not able to go back to the compromised endpoint or able to make lateral movements behind the deception environment".	The solution should be configured in such way that the attacker is not able to go back to the compromised endpoint or able to make lateral movements behind the deception environment. Please refer Corrigendum # 1.
68	52	56	The solution should have an inbuilt feature to allow automatic isolation of an attacking source system based on preset or custom rules. This should be possible without relying on integrations to external systems.	Requested you to kindly elaborate this point.	Please refer response to S.No 48.

Sr. No	Query Reference (Page)	Query Reference (Clause)	Existing clause of the RFP	Query by the Vendor	ReBIT's Response
69	53	61	The solution should automatically recommend un-listed subdomains to be deployed as decoys.	There is no way where system responds to admin for un-listing. It's always done manually. Requested you to kindly make it to Manually. This is proprietary feature of a particular OEM	Please refer response to S.No 2.
70	53	62	The solution should allow the user to choose from various server and versions for each un-listed subdomain.	There is no way where system responds to admin for un-listing. It's always done manually. Requested you to kindly make it to Manually. This is proprietary feature of a particular OEM	Please refer response to S.No 3.
71	53	63	The solution should allow custom decoy SSL certificate upload for each unlisted subdomain	Different solutions work on different patterns/ technology. This is proprietary feature of a particular OEM.	Please refer response to S.No 4.
72	53	70	Besides email alerts, the solution shall have the built in ability for real-time voice phone calls and SMS alerts based on pre-set or custom notification rules	This point is favoring to some OEM's. every solution has different ways of alert sharing. Requested you to kindly make it OPEN for all the OEM'S.	The solution should have feature to send alert through e-mails for attack based on pre-set or custom notification rules. Please refer Corrigendum # 1
73	53	71	There should be clear mechanism in the solution or process defined so that attacks on decoys are not mixed with actual attacks observed on the SIEM.	Different OEM's has different method to deploy the system. Different OEM's has different technology and this a proprietary feature.	Incident triggered from the Deception solution shall be easily identifiable and distinguished from actual attacks.
74	54	79	Solution should be able to whitelist authorized IP addresses and applications based on Hashes, certificate and PE header	This is proprietary feature of a particular OEM.	Please refer response to S.No 6.
75	54	81	Ability to integrate with any third party or custom threat feed	Requested you to kindly share the detail information about the Third party solution integration.	Ability to integrate with known and market reputed standard threat feed.
76	43	Annexure G - 5	The bidder should have executed 2 or more projects of size 400 user systems each of the proposed OEM's Solution in the last 3 years and should be go-live as on 31-12-2020.	Request to change the Clause to OEM/Bidder responsibility.	Please refer response to S.No 10
77	27	17.1 Purpose and Objective of SLA	The Bidder should provide SLA monitoring tool/system which will be used for monitoring SLA based on the SLA defined.	Request REBIT to amend this statement to: The Bidder should provide portal and ticketing system through which the data will be provided to measure the SLA's	Please refer response to S.No 40.

Sr. No	Query Reference (Page)	Query Reference (Clause)	Existing clause of the RFP	Query by the Vendor	ReBIT's Response
78	7	5.2.1	Bidder shall provide complete on premise DECEPTION TECHNOLOGY solution which will be required to detect and report attacks on decoys systems deployed through this solution	Request REBIT to confirm if they would prefer OnPrem VM or Hardware appliances?	Both VM or appliances can be considered.
79	43	Annexure G	The bidder should have executed 2 or more projects of size 400 user systems each of the proposed OEM's Solution in the last 3 years and should be go-live as on 31-12-2020.	Request REBIT to change this clause to: The bidder/ OEM should have executed 2 or more projects of size 400 user systems each of the proposed OEM's Solution in the last 3 years and should be go-live as on 31-12-2020.	Please refer response to S.No 10
80	14	5.6 Project Milestones	Receipt of Software and Hardware- Timeline - 4 to 6 weeks from PO	Receipt of Software and Hardware- Timeline - 8 to 10 weeks from PO	Receipt of Software and Hardware- Timeline - 6 to 8 weeks from the date of release of PO
81	43	Annexure G: Minimum Eligibility Criteria	The Bidder should have a positive net worth in last three (3) financial years, i.e. 2017- 18, 2018 – 19, 2019-2020.	Request to modify the clause as: The Bidder or Bidder's Parent Company (in case bidder is a 100% wholly owned subsidiary of parent company) should have a positive net worth in last three (3) financial years, i.e. 2017- 18, 2018 – 19, 2019-2020.	No change in this criteria. As discussed in the pre-bid meeting, if the company is newly formed by spin-off/carved-out from the parent company, the bidder shall provide all necessary documents to prove the same and consideration of the bid.
82	43	Annexure G: Minimum Eligibility Criteria	All Clauses	Request to consider " Bidder or Bidder's Parent Company (in case bidder is a 100% wholly owned subsidiary of parent company) " where ever "Bidder" has been mentioned.	Please refer response to S.No 81
83	43	Annexure G: Minimum Eligibility Criteria	The bidder should have executed 2 or more projects of size 400 user systems each of the proposed OEM's Solution in the last 3 years and should be go-live as on 31-12-2020.	Bidder or Bidder's Parent Company (in case bidder is a 100% wholly owned subsidiary of parent company) or OEM should have executed 2 or more projects of size 400 user systems each of the proposed OEM's Solution in the last 3 years and should be go-live as on 31-12-2020.	Please refer response to S.No 81

Sr. No	Query Reference (Page)	Query Reference (Clause)	Existing clause of the RFP	Query by the Vendor	ReBIT's Response
84	3	Schedule of Events	EMD - 50000/-	Request to Waive off the EMD against which we shall provide Bid Security Declaration that we may be liable to be suspended from participation in any future tenders of the Bank if 1. The bid submitted by us is withdrawn/modified during the period of bid validity. 2. If any statement or any form enclosed by us as part of this Bid turns out to be false / incorrect at any time during the period of prior to signing of Contract. 3. In case of we becoming successful bidder and if: a) we fail to execute Contract within the stipulated time. b) we fail to furnish Performance Bank Guarantee within the timelines stipulated in this RFP document.	No change in the RFP terms.
85	29	18. Liquidated Damages (LD)	i. In case of delay by the Bidder in any stage of the project milestone, the LD as per the ReBIT's discretion will be imposed on the Bidder at 1% of the total contract value per week of delay, subject to the maximum of 10% of the total contract value as per the agreement between ReBIT and the successful Bidder.	Request to modify the clause as: i. In case of delay by the Bidder in any stage of the project milestone, the LD as per the ReBIT's discretion will be imposed on the Bidder at 0.5% of the delayed merchandise/equipment per week of delay, subject to the maximum of 10% of the total contract value as per the agreement between ReBIT and the successful Bidder.	No change in the RFP terms.
86	12	5.4.8 Training	ReBIT expects the Bidder to train the administrator/business users till the personnel gain enough expertise in the system and capable of taking over the training function. The training should include features, facilities, operations, implementation, troubleshooting, system administration, database administration, operating system administration, DR elements, back-up, archiving and retrieval etc. All training will be hands-on training along with the trainer for the users. The Bidder should also provide e-learning facilities for users of the solution.	Help to confirm : 1) Training will required from OEM or Bidder. 2) Help to confirm training should be Classroom or basic training. 3) Nos of Professional to be trainied.	Bidder/OEM is expected to train ReBIT's resources during the implementation stage, before Go-live to ReBIT's satisfaction as per this feedback from the trainees. If the feedback is not satisfactory, the bidder shall repeat the training. Hand holding training to be provided to atleast 5 users to manage the solution. Training can be provided on-line or in class room.