Bank Response to RFP No. SBI/GITC/NW & Comm./2021/2022/797 21.10.2021
RFP FOR PROCUREMENT OF CYBER SECURITY THREAT DECEPTION (HONEYPOT) SOLUTION

Sr. No	RFP Page No	RFP Clause No	Existing Clause	Query/ Suggestions	Type of response	Banks' Response
1	2	4	From 15:30 hrs. to 16:30 hrs on 03.11.2021 at GITC, CBD Belapur, Navi Mumbai or through online meeting.	We request the bank to please postpone the pre-bid meeting date to anytime later than Nov 4th (Diwali) incase the meeting is onsite.	No change	No change in the terms of the RFP.
2	32	36	Insurance The insurance shall be for an amount equal to 100 percent of the value of the Products from place of dispatch to final destination on “All Risks” basis, valid for a period of one month after delivery of Products at the defined destination.	Post delivery, HW ownership will be with SBI. Vendor cannot take out insurance for something he does not own. We are happy to provide insurance until point of delivery, post delivery Insurance must be under existing SBI warehouse insurance	No change	No change in the terms of the RFP.
3	32	Clause 38	38. LIMITATION OF LIABILITY: i. The maximum aggregate liability of Service Provider, subject to clause 38 (iii), in respect of any claims, losses, costs or damages arising out of or in connection with this RFP/Agreement shall not exceed the total Project Cost. ii. Under no circumstances shall either Party be liable for any indirect, consequential or incidental losses, damages or claims including loss of profit, loss of business or revenue. iii. The limitations set forth herein shall not apply with respect to: a) claims that are the subject of indemnification pursuant to infringement of third party Intellectual Property Right; b) damage(s) occasioned by the Gross Negligence or Willful Misconduct of Service Provider, c) damage(s) occasioned by Service Provider for breach of Confidentiality Obligations, d) Regulatory or statutory fines imposed by a Government or Regulatory agency for non-compliance of statutory or regulatory guidelines applicable to the Bank, provided such guidelines were brought to the notice of Service Provider.	NTT Comment - We request that liability under this RFP is capped to the annual contract value.	No change	No change in the terms of the RFP.
			INTELLECTUAL PROPERTY RIGHTS AND OWNERSHIP: iii. Subject to clause 39 (iv) and 39 (v) of this RFP, Service Provider shall, at its own expenses without any limitation, indemnify and keep fully and effectively indemnified the Bank against all cost, claims, damages, demands, expenses and liabilities whatsoever nature arising out of or in connection with all claims of infringement of Intellectual Property Right, including patent, trademark, copyright, trade secret or industrial design rights of any third party arising from use of the technology / Software / products or any part thereof in India or abroad, for Software licensed/developed as part of this engagement. In case of violation/ infringement of patent/ trademark/ copyright/ trade secret or industrial design or any other Intellectual Property Right of third party, Service Provider shall, after due inspection and testing, without any additional cost (a) procure for the Bank the right to continue to using the Software supplied; or (b) replace or modify the Software to make it non-infringing so long as the replacement to or modification of Software provide substantially equivalent functional, performance and operational features as the infringing Software which is being replaced or modified; or (c) to the extent that the activities under clauses (a) and (b) above are not commercially reasonable, refund to the Bank all amounts paid by the Bank to Service Provider under this RFP/Agreement.			

4	35	Clause 43	vi. For OEM specific software licenses:- Service Provider shall grant the Bank a fully paid-up, irrevocable, non-exclusive, unlimited, perpetual license throughout the territory of India or abroad to access, replicate and use software provided by Service Provider, including all inventions, designs and marks embodied therein perpetually. The source code / object code / executable code and compilation procedures of the Software Solution should be placed under an Escrow arrangement. All necessary documentation in this behalf should be made available to the Bank. In case of Escrow arrangement, complete details and the location and the terms and conditions applicable for escrow must be specified. Any update or upgrade to source code should be informed and brought under Escrow or made available to the Bank.	NTT Comment - We request necessary modification to this clause, as we are not an OEM but a reseller and integrator of the OEM products. All IPR rights, indemnities and warranties in respect of the products supplied will be governed by the OEM terms and conditions in respect of such products and Bidder will pass them to the Bank "-as-is".	No change	No change in the terms of the RFP.
			vii. For software or integration or interface or application developed for the Bank:- Service Provider shall grant the Bank a fully paid-up, irrevocable, exclusive, ,unlimited, no. of perpetual license purchased throughout the territory of India or abroad to access, replicate and use software provided/developed by Service Provider for Bank, including all inventions, designs and marks embodied therein perpetually. The source code /object code /executable code and compilation procedures of the Software Solution made under this agreement are the proprietary property of the Bank and as such Service Provider shall make them available to the Bank after successful User Acceptance Testing. Service Provider agrees that the Bank owns the entire right, title and interest to any inventions, designs, discoveries, writings and works of authorship, including all Intellectual Property Rights, copyrights. Any work made under this agreement shall be deemed to be 'work made for hire' under any Indian/U.S. or any other applicable copyright laws.			
			viii. Service provider agrees that the Bank owns the entire right, title and interest to any inventions, designs, discoveries, writings and works of authorship, including all intellectual property rights, copyrights. Any work made under this RFP shall be deemed to be 'work made for hire' under any Indian/U.S. or any other applicable copyright laws.			
5	37	44. Liquidated Damages	If the Service Provider fails to deliver product and/or perform any or all the Services within the stipulated time, schedule as specified in this RFP/Agreement, the Bank may, without prejudice to its other remedies under the RFP/Agreement, and unless otherwise extension of time is agreed upon without the application of liquidated damages, deduct from the Project Cost, as liquidated damages a sum equivalent to 0.5% of total Project Cost for delay of each week or part thereof maximum up to 5% of total Project Cost. Once the maximum deduction is reached, the Bank may consider termination of the Agreement.	We request this to be amended to a max of 5% of Hardware and Installation cost	No change	No change in the terms of the RFP.
6	63	49	Solution must support Bank defined signature detection for 'known bad' events and must be updated with the latest emerging threat signatures.	We request bank to please provide details of the defined signature detection software which is being requested for support	Clarification	Solution must be able to incorporate(if required) the 'know bad' events generated by IPS, WAF etc
7	64	57	The solution should allow custom decoy SSL certificate upload for each unlisted subdomain	We request the bank to provide more information on this requirement (are the unlisted subdomain deceptive and are they being required to put on DMZ?)	Clarification	Site created on the decoy should able to allow custom decoy SSL certificate upload

8	65	63	The solution should use a numeric risk score and MITRE mapping for each attacker based on dynamic analysis of attacker behaviour. It should also include risk categorization as critical / high /medium / low buckets.	We request the bank to modify the clause to "The solution should use a numeric risk score or MITRE mapping for each attacker based on dynamic analysis of attacker behaviour. It should also include risk categorization as critical / high /medium / low buckets."	No change	No change in the terms of the RFP.
9	67	Technical & Functional Specifications - point 78	Bidder will engage CERT-IN Empaneled ISSPs for ensuring security posture of their support and security certification (ISO, PCI-DSS etc)	What is the expectation from SBI on the cert-in empaneled vendor and the frequency for the same.	Clarification	To achive high standards of security posture. Frequency is as and when required.
10	74	Term of the Project - Project Schedule;Miles tones and delivery locations - point iii	ii. Delivery Schedule are as follows: Supply of Hardware & Software: Within 8 weeks from the date of Purchase Order. iii. Installation Schedule: Installation, Configuration, Integration and Commissioning of Hardware & Other Items (including OS & Solutions): The successful bidder should ensure installation, configuration, Integration and commissioning of all hardware and other items including solutions within 10 weeks from the date of Purchase Order.	Bank is requested to amend the clause as below- ii. Delivery Schedule are as follows: Supply of Hardware & Software: Within 12 weeks from the date of Purchase Order. iii. Installation Schedule: Installation, Configuration, Integration and Commissioning of Hardware & Other Items (including OS & Solutions): The successful bidder should ensure installation, configuration, Integration and commissioning of all hardware and other items including solutions within 14 weeks from the date of Purchase Order	Corrigendum	The clasuess may be amended as below- ii. Delivery Schedule are as follows: Supply of Hardware & Software: Within 10 weeks from the date of Purchase Order. iii. Installation Schedule: Installation, Configuration, Integration and Commissioning of Hardware & Other Items (including OS & Solutions): The successful bidder should ensure installation, configuration, Integration and commissioning of all hardware and other items including solutions within 12 weeks from the date of Purchase Order.
11	80	10	i. The initial requirement for the Cyber Security Threat Deception (Honeypot) Solution is for 169 “User Systems” in offices/branches/DC, 72 VLANs, 118 Decoys (36 Active Directory decoys, 10 email decoys, 24 Web Decoy, 24 DB Decoy, 24 File Server Decoy) in 2 DC locations (including subscription licenses) . ii. The solution should be scalable and designed to cater to the Cyber Security Threat Deception (Honeypot) Solution requirement for 5000 “User Systems” in offices/branches/DC, 144 VLANs, 190 Decoys (36 Active Directory decoys, 10 email decoys, 48 Web Decoys, 48 DB Decoys, 48 File Server Decoys) in 2 DC locations (including subscription licenses) iii. Hardware should support minimum 3 lac endpoints, 144 VLANs & 190 Decoys. iv. The Bank initially proposes to procure 5000 licenses. Thereafter, based on the requirement additional licenses would be procured. The licenses requirements have been split into slabs such as 5,001 to 20000; 20001 to 50000; 50001 to 100000 and so on.	We request the bank to please clarify the below for sizing the Bill of Materials. 1. Whether the solution needs to be deployed in different zones like DMZ, Internal, Partners for DC and DR. 2. In point (i) 169 user systems are mentioned but point (iv) mentions 5000 licenses. We request the bank to clarify the actual number of endpoints to be covered as part of this RFP.	Clarification	1. Sufficient provisions has to be made as per best industry practice. As of now Bank needs appliances to be deployed in High Availability (HA) mode in Two Zones at each DC & DR. 2. To start with 169 users systems and 5000 endpoints licences are considered in this RFP. Bank shall take a decision to install more end points in due course.
12	82	11 - Regulatory / Compliance Requirements	The system should provide for adequate audit trail including log reports for all the activities and any changes in configuration, information, data changes, updation etc. As per the statutory / regulatory / legal requirements the logs have to archived for 10 years and active retention of logs in the solution should be 1 year	Please clarify if SBI will provide the storage abd backup solution to archive the logs for 10 years	Clarification	Solution must have active log retention for 1 year and should be able to take backup on tape or on Bank's cloud
13	85	17. Payment schedule	Bank has proposed, 50% on delivery, 40% after two months of successful running, 10% on providing a BG for Warranty period	We request this to be amended to industry standard of 70% on Delivery, 20% on install and 10% on providing a BG for warranty period	No change	No change in the terms of the RFP.
14	101	Uptime Penalty	There is no upper cap on the penalty imposed	We request that all SLA based penalties be upto a max of 5% of Annual contract value excluding Hardware and Installation cost	Clarification	The cap on penalty will be 20 percentage of Purchase Order Value as given on page no 110

15	105	Table B - Uptime requirement/Vulnerabilities (On an ongoing basis) - point 2	Fixing the security vulnerabilities, taking prompt action on the advisories sent by the Bank's Security Consultant or by the Bank officials within three working days.	There are factors where there will be a dependency on the OEM to release the bug fix. Hence request Bank to consider timelines post Oem release and approval from SBI management	Clarification	No change for fixing the security vulnerabilities that are not dependent on OEM. Work around for the vulnerability till date of bug fix released by the OEM and strong followup to complete the task within timelines given.
16	105	Table A- Delivery, Installation and commissioning Point 2	Installation, testing, and successful commissioning of Cyber Security Threat Deception (Honeypot) Solution (equipment and software) should be done within 13 weeks from date of Purchase order.	Babk is requested to amend this clause as under- Installation, testing, and successful commissioning of Cyber Security Threat Deception (Honeypot) Solution (equipment and software) should be done within 13 weeks from date of Purchase order.	Clarification	the query is same as the existing clause. Hence, no response
17	107	Table G: Patch management, Hardening of Devices as per SCDs - point 1	The security features like firmware upgradation and hardening of devices related to all devices must be done.	For critical, request Bank to consider timelines post approval from SBI management	No change	No change in the terms of the RFP.
18	107	Table G: Patch management, Hardening of Devices as per SCDs - point 2	Implementation of Patches from its release	Request Bank to consider timelines post approval from SBI management	No change	No change in the terms of the RFP.
19	135	Appendix-K - Clause 16	SOURCE CODE ESCROW AGREEMENT	NTT Comment -- Considering the scope of work, please confirm that this provision of source code escrow agreement will not be relevant	No change	No change in the terms of the RFP.
20	183	Appendix-O PRE CONTRACT INTEGRITY PACT - Clause 6	6. Fall Clause The BIDDER undertakes that it has not supplied/is not supplying similar product/systems or subsystems at a price lower than that offered in the present Bid in respect of any other Ministry/Department of the Government of India or PSU or any other Bank and if it is found at any stage that similar product/systems or sub systems was supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU or a Bank at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the BUYER, if the contract has already been concluded.	NTT Comment - We agree to execute the Pre-Contract Integrity Pact given by Bank, provided that Fall Clause is deleted. Please note that prices quoted are based on several factors, including quantity, location of delivery, dollar rates, discounts received from OEMs and other contractual risks. For all practical purposes, we request deletion of the Fall Clause from the Integrity Pact. The CVC has issued circular of 2017, where it is apparent that Fall Clause is not a requirement to Integrity Pact.	No change	No change in the terms of the RFP.

21	123, 124 and 125	APPENDIX K - 5.3, 5.11 AND 5.13	Service Level Agreement 5.3 Service Provider warrants that at the time of delivery the Software or its component is free from malware, free from any obvious bugs, and free from any covert channels in the code (of the versions of the applications/software being delivered as well as any subsequent versions/modifications delivered). 5.11 Service Provider warrants that to the best of its knowledge, as on the Effective Date of this Agreement, the Software does not violate or infringe any patent, copyright, trademarks, trade secrets or other Intellectual Property Rights of any third party 5.13 During the Warranty Period if any software or any component thereof is supplied by Service Provider is inoperable or suffers degraded performance not due to causes external to the software, Service provider shall, at the Bank's request, promptly replace the software or specified component with new software of the same type and quality. Such replacement shall be accomplished without any adverse impact on the Bank's operations within agreed time frame.	NTT Comment - We request some changes in respect of this clause considering that we are a reseller of products. Bidder warrants that products supplied will be new and original and unused. All other warranties in respect of the products will be as per the OEM warranty terms and conditions and SBI will be bound by the same.	No change	No change in the terms of the RFP.
22			**Additional points to be considered**			
23			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.	Clarification	If Vendor would like to provide any additional/value added feature, can proivde without any additional cost to the bank
24			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.	Clarification	If Vendor would like to provide any additional/value added feature, can proivde without any additional cost to the bank
25			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.	Clarification	If Vendor would like to provide any additional/value added feature, can proivde without any additional cost to the bank
26			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.	Clarification	If Vendor would like to provide any additional/value added feature, can proivde without any additional cost to the bank
27			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.	Clarification	If Vendor would like to provide any additional/value added feature, can proivde without any additional cost to the bank
28			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.	Clarification	If Vendor would like to provide any additional/value added feature, can proivde without any additional cost to the bank

29			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.	Clarification	If Vendor would like to provide any additional/value added feature, can proivde without any additional cost to the bank
30			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.	Clarification	If Vendor would like to provide any additional/value added feature, can proivde without any additional cost to the bank
31	30	33. INSPECTION AND TESTING:	i. The Bank reserves the right to carry out pre-shipment inspection or demand a demonstration of the product on a representative model at Service Provider's location.	Request bank to confirm this requirement since vendor has to provide necessary facility / equipment at their premises, and also to confirm , who bear all the cost of such inspection like travel, boarding, lodging & other incidental expenses of the Bank's representatives.	Clarification	Please refer point No.33 ii b) page No.30
32	53	Bidder's Eligibility Criteria , 3	The Bidder must have an average turnover of minimum Rs.50 crore during last 03 (three) financial year(s) i.e. FY17-18, FY18-19 and FY19-20.	Kindly confirm last 3 year financials as FY 2018-19 , FY 2019-20 , FY 2020-21.	Corrigendum	3 year financials as FY 2018-19 , FY 2019-20 , FY 2020-21.
33	56	Appendix-C point 1.	The proposed and presented solution should be an on-premises solutions that will be placed in multiple SBI Data centres.	We will need VM/server to create decoy in specific zone. Please confirm whether Bank will provide the same.	Clarification	Bidder should provision the hardware /VM/Server for implementation of the solution as per requirement
34	56	Appendix-C point 1.	The proposed and presented solution should be an on-premises solutions that will be placed in multiple SBI Data centres.	We assume that Space, power and network connectivity for solution implementation will be provided by Bank. Please confirm.	Clarification	Space, power and network connectivity for solution implementation will be provided by the Bank
35	67	Appendix-C 78.	Bidder will engage CERT-IN Empaneled ISSPs for ensuring security posture of their support and security certification (ISO, PCI-DSS etc)	Please clarify expectation for PCI-DSS here as bidder won't process any card data. Is it Ok if bidder is ISO27001 certified from competent authority?	No change	No change in the terms of the RFP.
36	71	Appendix E, point 2 (iv)	Specify in detail how many Servers, VMs, network components will be required for this deception solution to be deployed in SBI.	Request the bank to confirm if virtual appliances can provided as a solution or does the bidder have to provide the hardware as well?	Clarification	Bidder has to provide all hardware, Software, Licenses related to the solution to meet the Bank's requirement
37	71	Appendix E, point 2 (v)	Vendor has to recommend which component of the proposed Cyber Security Threat Deception (Honeypot) Solution should fit into what network zone as per best industry practices considering the organizational business requirements.	Our decoys in the datacenters are deployed using the VLAN trunking. Request the bank to confirm if one appliance each in DC & DR would be sufficient to trunk all the VLANs where decoys have to be deployed? If there are zones which are behind firewall such as DMZ, then a separate appliance may be required for that zone. Please let us know how many such zones are in scope for deploying decoys.	Clarification	Sufficient provisions has to be made as per best industry practice. As of now Bank needs appliances to be deployed in High Availability (HA) mode in Two Zones at each DC & DR.
38	74	Appendix-E	Installation Schedule: Installation, Configuration, Integration and Commissioning of Hardware & Other Items (including OS & Solutions): The successful bidder should ensure installation, configuration, Integration and commissioning of all hardware and other items including solutions within 10 weeks from the date of Purchase Order.	Request bank to give 20 weeks for implementation and integration as delivery will take 8-10 weeks and implentation will require 10-12 weeks.	Corrigendum	Installation Schedule: Installation, Configuration, Integration and Commissioning of Hardware & Other Items (including OS & Solutions): The successful bidder should ensure installation, configuration, Integration and commissioning of all hardware and other items including solutions within 12 weeks from the date of Purchase Order.

39	74	Appendix-E	iv. Project implementation will be in three phases. Phase implementation scheduled is mentioned in the table below: Phases Phase-I Phase-IIPhase-III Timelines from date of Purchase Order11 weeks12 weeks13 weeks Details of each phase are as under: v.Phase-I (User Acceptance Test): The Bidder has to ensure User Acceptance Test (UAT) setup within 11 Weeks from the date of Purchase Order along with the Closure of CSR and VA observations has to be done in UAT by the bidder. vi.Phase-II (Pilot Implementation): Bidder has to ensure pilot implementation within 12 weeks from the date of purchase order at both locations (DC & DR). vii.Phase-III (Go-Live): After successful completion of Pilot implementation for the security Solutions of the Bank, the selected Bidder shall commence the roll out of the entire solution integrating other solutions and products and complete within 13 weeks from the date of purchase order at both locations. Bank at its discretion will roll out the solution in a single go or in a phased manner.	Please give 18 weeks for Phase 1, 22 weeks for phase 2 and 24 weeks for phase 3 from PO date as delivery will take 8-10 weeks and implemtation will require 10-12 weeks.	Corrigendum	iv. Project implementation will be in three phases. Phase implementation scheduled is mentioned in the table below: Phases Timelines from date of Purchase Order Phase-I Phase-IIPhase-III 13 weeks14 weeks15 weeks Details of each phase are as under: v.Phase-I (User Acceptance Test): The Bidder has to ensure User Acceptance Test (UAT) setup within 13 Weeks from the date of Purchase Order along with the Closure of CSR and VA observations has to be done in UAT by the bidder. vi.Phase-II (Pilot Implementation): Bidder has to ensure pilot implementation within 14 weeks from the date of purchase order at both locations (DC & DR). vii.Phase-III (Go-Live): After successful completion of Pilot implementation for the security Solutions of the Bank, the selected Bidder shall commence the roll out of the entire solution integrating other solutions and products and complete within 15 weeks from the date of purchase order at both locations.
40	78	Appendix-E , Scope of Work and Payment Schedule	Comprehensive Annual Maintenance Contract (AMC) / Annual Technical Support (ATS): vii. Comprehensive Annual Maintenance Contract (AMC) for Products mentioned above (after the end of five year comprehensive warranty) will be negotiated in the range of 8% to 12 % p.a. of the Product cost. The Bank shall negotiate with the selected bidder for extending the Comprehensive annual maintenance Contract for Products by another 2 years post expiry of initial Comprehensive annual maintenance of 5 years, at the Banks' sole discretion.	Request SBI not to limit the AMC percentage range as it is depend upon OEM pricing policy after 5 Year.	No change	No change in the terms of the RFP.
41	80	Scalability Requ	iii. Hardware should support minimum 3 lac endpoints, 144 VLANs & 190 Decoys.	Please clarify if bank wants to implement decoy in all of the endpoints and factor hardware from day 1	Clarification	Bidder should provision the hardware to support 3 lac endpoints from day 1

42	81	Appendix-E , Scope of Work and Payment Schedule	Scalability Requirements iv. The Bank initially proposes to procure 5000 licenses. Thereafter, based on the requirement additional licenses would be procured. The licenses requirements have been split into slabs such as 5,001 to 20000; 20001 to 50000; 50001 to 100000 and so on. The rate shall be discovered for 5000 end point licenses for a period of 5 years. Then this rate would be used for discovering rates for various slabs using multiplication factor mentioned in the below table. The rate arrived at after using multiplication factor shall be divided by the highest value of the slab to arrive at per licenses value. This value would be used for arriving at rate for the additional licenses. The payment shall be made for actual number of licenses procured and for the period put to use. Multiplication factor for additional licenses after 5000 endpoints shall be as under: Sr. no---Description----------Amount (INR) 1----Rate discovered up to 5000 endpoint licenses for 5 years----------X 2----Rate shall be valid for 5 year payable for licenses procured from 5001 to 20000 licenses.-----X*2 3----Rate shall be valid for 5 year payable for licenses procured from 20001 to 50000 licenses.------X*3 4----Rate shall be valid for 5 year payable for licenses procured from 50001 to 100000 licenses.------X*6 5----Rate shall be valid for 5 year payable for licenses procured from 100001 to 150000 licenses.-----X*10 6----Rate shall be valid for 5 year payable for licenses procured from 150001 to 200000 licenses.-----X*15 7----Rate shall be valid for 5 year payable for licenses procured from 200001 to 250000 licenses.-----X*20	Request you to clarify the basis of calculation.	Corrigendum	Please refer example given in Revised "Appendix-F" (Indicative Price Bid)
43	84	Appendix-E , Scope of Work and Payment Schedule	Payment schedule:- Sl.----Payment Stage----------% of Payment 1-----Hardware (Hardware Appliance / Server / Other Items etc.)-----50 % of the cost of the hardware will be paid against proof of delivery of equipment 2-----Software (End Points, Decoys, OS & DB Licenses etc.)-------50 % of the cost of the software will be paid against proof of delivery of licenses/software. 3-----Installation/ Commissioning---------On completion of Task 4-----UAT & Production & Go Live----------40 % of Hardware & Software/Licenses Cost after two months of successful running of product /solution and the final 10% against submission of performance Bank Guarantee valid for 63 months.	Request SBI to consider the payment terms as " Payment schedule Sl.----Payment Stage----------% of Payment 1-----Hardware (Hardware Appliance / Server / Other Items etc.)-----50 % of the cost of the hardware will be paid against proof of delivery of equipment 2-----Software (End Points, Decoys, OS & DB Licenses etc.)-------50 % of the cost of the software will be paid against proof of delivery of licenses/software. 3-----Installation/ Commissioning---------On completion of Task 4.----UAT Completion ---20% of Hardware & Software/Licenses Cost. 5. ----Pilot Implementation----10% of Hardware & Software/Licenses Cost. 6-----Go Live----------10 % of Hardware & Software/Licenses Cost after two months of successful running of product /solution and against submission of performance Bank Guarantee valid for 63 months	No change	No change in the terms of the RFP.
44	84	Appendix E, point 13	The initial requirement for the Cyber Security Threat Deception (Honeypot) Solution is for 169 “User Systems” in offices/branches/DC, 72 VLANs, 118 Decoys (36 Active Directory decoys, 10 email decoys, 24 Web Decoy, 24 DB Decoy, 24 File Server Decoy) in 2 DC locations (including subscription licenses) .	Request the bank to confirm if this UAT testing can be done on the same solution provided for 5000 user systems? Or this is separate requirement?	Clarification	UAT testing to performed for 169 endpoints but solution should support 3 lac endpoints if deployed in near future

45	86	Appendix-E Scope of Work and Payment Schedule	Payment schedule:- Comprehensive warranty for Products for 05 years. -Warranty period will start from the date of acceptance of solution by the Bank. -----Yearly in arrears and within one month after submission of invoices.	Request SBI to release warranty support payment as Yearly in Advance.	No change	No change in the terms of the RFP.
46	88	Appendix-F Indicative Price Bid	1. Hardware (Hardware Appliance / Server / Other Items etc.) to support Three lac endpoints as per point no.10 (iii) of Appendix-E for both DC & DR) **(This cost should not be more than 20% of the total cost (A).** 2. Cost of Software Solution sufficient to handle Three lac endpoints, 190 Decoys including OS & DB Licenses etc. for a contract period of 5 years. **(This cost should not be more than 25% of the total cost (A)** 3. Cost for 5000 endpoint licenses for period of 5 years. **(This cost should not be more than 5% of the total cost (A).** This rate will determine the cost per license. 4. Installation/ Commissioning **(This cost should not be more than 3% of the total cost (A))** 5. Comprehensive warranty for Hardware & Software Solution mentioned in items above for 5 years from the go live date. **(This cost should not be more than 30% of the total cost (A)** 6. Onsite support --16x5 basis --Two L2 engineers required for 8hrs including handover period on bank's working days. **(This cost should not be more than 15% of the total cost (A)** 7. Training and Certification (from OEM) for Deployment and Management of Cyber Security Threat Deception (Honeypot) Solution for 10 officials per year. **(This cost should not be more than 2% of the *total cost (A)**	Request SBI to remove the percentage limitation in all the Line items.	No change	No change in the terms of the RFP.
47	88	Appendix-F poin	Onsite support 16x5 basis Two L2 engineers required for 8hrs including handover period on bank's working days.	Is it one L2 per shift or 2 L2 per shift?	Corrigendum	Onsite support 16x6 basis one L2 engineer required in each shift of 8hrs including handover period (Refer Revised Appendix-F)
48	89	Appendix-F poin	Training and Certification (from OEM) for Deployment and Management of Cyber Security Threat Deception (Honeypot) Solution for 10 officials per year. (This cost should not be more than 2% of the *total cost (A)	Please clarify whether training will be at GITC and number of days for training instance.	Clarification	Training will be at mutually agreed location. Training should be comprehensive meeting the Bank's requirements. Accordingly vendor to decide the number of days for training.
49	104	Appendix-J Other Terms and Penalties	Table A- Delivery, Installation and commissioning Delivery of hardware & software in 8 weeks at DCs in Navi Mumbai & Hyderabad---- Penalty for the breach---In the event of the hardware & software not being delivered within 8 weeks from the date of Purchase Order, a penalty of one (1) percent of the total consideration (Total Purchase Order value) for each week or part thereof the delay, subject to maximum amount of ten (10) percent of the total consideration (Total Purchase Order value) will be charged to vendor. This amount of penalty so calculated shall be deducted at the time of making final payment after successful installation and commissioning of hardware.	Request SBI to consider the delivery penalty as 0.5% per week and Maximum to 5% of the delayed Product.	No change	No change in the terms of the RFP.

50	105	Appendix-J Other Terms and Penalties	Table A- Delivery, Installation and commissioning Installation, testing, and successful commissioning of Cyber Security Threat Deception (Honeypot) Solution (equipment and software) should be done within 13 weeks from date of Purchase order.---- Penalty for the breach---Penalty of one (1) percent of the total consideration (Total Purchase Order value) for each week or part thereof the delay, subject to maximum amount of ten (10) percent of the total consideration (Total Purchase Order value) will be charged to vendor. This amount of penalty so calculated shall be deducted at the time of making final payment after successful installation and commissioning of hardware.	Request SBI to consider the Installation penalty as 0.5% per week and Maximum to 5% of the delayed Product.	No change	No change in the terms of the RFP.
51	110	Appendix-J Other Terms and Penalties	The cap on penalty will be 20 percentage of Purchase Order Value.	Request SBI to CAP the penalty as 10% of the purchase order value.	No change	No change in the terms of the RFP.
52	35	iii	Subject to clause 39 (iv) and 39 (v) of this RFP, Service Provider shall, at its own expenses without any limitation, indemnify and keep fully and effectively indemnified the Bank against all cost, claims, damages, demands, expenses and liabilities whatsoever nature arising out of or in connection with all claims of infringement of Intellectual Property Right, including patent, trademark, copyright, trade secret or industrial design rights of any third party arising from use of the technology / Software / products or any part thereof in India or abroad, for Software licensed/developed as part of this engagement. In case of violation/ infringement of patent/ trademark/ copyright/ trade secret or industrial design or any other Intellectual Property Right of third party, Service Provider shall, after due inspection and testing, without any additional cost (a) procure for the Bank the right to continue to using the Software supplied; or (b) replace or modify the Software to make it non-infringing so long as the replacement to or modification of Software provide substantially equivalent functional, performance and operational features as the infringing Software which is being replaced or modified; or (c) to the extent that the activities under clauses (a) and (b) above are not commercially reasonable, refund to the Bank all amounts paid by the Bank to Service Provider under this RFP/Agreement.	We request for modification as product/solution is owned by the OEM: Subject to clause 39 (iv) and 39 (v) of this RFP, Service Provider and OEM shall, at its own expenses without any limitation, indemnify and keep fully and effectively indemnified the Bank against all cost, claims, damages, demands, expenses and liabilities whatsoever nature arising out of or in connection with all claims of infringement of Intellectual Property Right, including patent, trademark, copyright, trade secret or industrial design rights of any third party arising from use of the technology / Software / products or any part thereof in India or abroad, for Software licensed/developed as part of this engagement. In case of violation/ infringement of patent/ trademark/ copyright/ trade secret or industrial design or any other Intellectual Property Right of third party, Service Provider and OEM shall, after due inspection and testing, without any additional cost (a) procure for the Bank the right to continue to using the Software supplied; or (b) replace or modify the Software to make it non-infringing so long as the replacement to or modification of Software provide substantially equivalent functional, performance and operational	No change	No change in the terms of the RFP.
53	43	vi	If existing Service Provider is breach of this obligation, they shall be liable for paying a penalty of 10% of the total Project Cost on demand to the Bank, which may be settled from the payment of invoices or Bank Guarantee for the contracted period or by invocation of Bank Guarantee.	We request modification as mentioned below: We propose to delete this clause as in case of breach of oabligtion BG will be forfeited	No change	No change in the terms of the RFP.
54	115	1.1.7	“Intellectual Property Rights” shall mean, on a worldwide basis,	We request modification as mentioned below: Intellectual Property Rights” shall mean and include any and all:	No change	No change in the terms of the RFP.

55	133	15.12	The foregoing obligations (collectively referred to as “Confidentiality Obligations”) set out in this Agreement shall survive the term of this Agreement and for a period of five (5) years thereafter provided Confidentiality Obligations with respect to individually identifiable information, customer’s data of Parties or software in human-readable form (e.g., source code) shall survive in perpetuity.	We request modification as mentioned below: The foregoing obligations (collectively referred to as “Confidentiality Obligations”) set out in this Agreement shall survive the term of this Agreement and for a period of three (3) years thereafter provided Confidentiality Obligations with respect to individually identifiable information, customer’s data of Parties or software in human-readable form (e.g., source code).	No change	No change in the terms of the RFP.
56	128	12.3	Subject to clause 12.4 and 12.5 of this Agreement, Service Provider shall, at its own expenses without any limitation, indemnify and keep fully and effectively indemnified the Bank against all cost, claims, damages, demands, expenses and liabilities whatsoever nature arising out of or in connection with all claims of infringement of Intellectual Property Right, including patent, trademark, copyright, trade secret or industrial design rights of any third party arising from use of the technology / Software / products or any part thereof in India or abroad, for Software licensed/developed as part of this engagement. In case of violation/ infringement of patent/ trademark/ copyright/ trade secret or industrial design or any other Intellectual Property Right of third party, Service Provider shall, after due inspection and testing, without any additional cost (a) procure for the Bank the right to continue to using the Software supplied; or (b) replace or modify the Software to make it non-infringing so long as the replacement to or modification of Software provide substantially equivalent functional, performance and operational features as the infringing Software which is being replaced or modified; or (c) to the extent that the activities under clauses (a) and (b) above are not commercially reasonable, refund to the Bank all amounts paid by the Bank to Service Provider under this Agreement.	We request for modification as product/solution is owned by the OEM: Subject to clause 12.4 and 12.5 of this Agreement, Service Provider and OEM shall, at its own expenses without any limitation, indemnify and keep fully and effectively indemnified the Bank against all cost, claims, damages, demands, expenses and liabilities whatsoever nature arising out of or in connection with all claims of infringement of Intellectual Property Right, including patent, trademark, copyright, trade secret or industrial design rights of any third party arising from use of the technology / Software / products or any part thereof in India or abroad, for Software licensed/developed as part of this engagement. In case of violation/ infringement of patent/ trademark/ copyright/ trade secret or industrial design or any other Intellectual Property Right of third party, Service Provider and OEM shall, after due inspection and testing, without any additional cost (a) procure for the Bank the right to continue to using the Software supplied; or (b) replace or modify the Software to make it non-infringing so long as the replacement to or modification of Software provide substantially equivalent functional, performance and	No change	No change in the terms of the RFP.
57	128	12.4	The Bank will give (a) notice to Service provider of any such claim without delay/provide reasonable assistance to Service provider in disposing of the claim;	We request for modification as product/solution is owned by the OEM: The Bank will give notice to Service Provider of any such claim without delay/provide reasonable assistance to Service Provider in disposing of the claim; and Service Provider along with assistance of OEM	No change	No change in the terms of the RFP.
58	54	Appendix-B Bidder’s Eligibility Criteria Sr. No. 7	Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has executed similar projects in India. (Start and End Date of the Project to be mentioned) in the past (At least 2 client references are required)	Kindly amend; Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder/OEM has executed similar projects in India. (Start and End Date of the Project to be mentioned) in the past (At least 2 client references are required)	No change	No change in the terms of the RFP.
59	71	Appendix E, poir	Specify in detail how many Servers, VMs, network components will be required for this deception solution to be deployed in SBI.	Request the bank to confirm if virtual appliances can provided as a solution or does the bidder have to provide the hardware as well?	Clarification	Bidder has to provide all hardware, Software, Licenses related to the solution to meet the Bank's requirement

60	71	Appendix E, poir	Vendor has to recommend which component of the proposed Cyber Security Threat Deception (Honeypot) Solution should fit into what network zone as per best industry practices considering the organizational business requirements.	Our decoys in the datacenters are deployed using the VLAN trunking. Request the bank to confirm if one appliance each in DC & DR would be sufficient to trunk all the VLANs where decoys have to be deployed? If there are zones which are behind firewall such as DMZ, then a separate appliance may be required for that zone. Please let us know how many such zones are in scope for deploying decoys.	Clarification	Sufficient provisions has to be made as per best industry practice. As of now Bank needs appliances to be deployed in High Availability (HA) mode in Two Zones at each DC & DR.
61	84	Appendix E, poir	The initial requirement for the Cyber Security Threat Deception (Honeypot) Solution is for 169 “User Systems” in offices/branches/DC, 72 VLANs, 118 Decoys (36 Active Directory decoys, 10 email decoys, 24 Web Decoy, 24 DB Decoy, 24 File Server Decoy) in 2 DC locations (including subscription licenses) .	Request the bank to confirm if this UAT testing can be done on the same solution provided for 5000 user systems? Or this is separate requirement?	Clarification	UAT testing to performed for 169 endpoints but solution should support 3 lac endpoints if deployed in near future
62	2	4	From 15:30 hrs. to 16:30 hrs on 03.11.2021 at GITC, CBD Belapur, Navi Mumbai or through online meeting.	We request the bank to please postpone the pre-bid meeting date to anytime later than Nov 4th (Diwali) incase the meeting is onsite.	No change	No change in the terms of the RFP.
63	63	49	Solution must support Bank defined signature detection for 'known bad' events and must be updated with the latest emerging threat signatures.	We request bank to please provide details of the defined signature detection software which is being requested for support	Clarification	Solution must be able to incorporate(if required) the 'know bad' events generated by IPS, WAF etc
64	64	57	The solution should allow custom decoy SSL certificate upload for each unlisted subdomain	We request the bank to provide more information on this requirement (are the unlisted subdomain deceptive and are they being required to put on DMZ?)	Clarification	Site created on the decoy should able to allow custom decoy SSL certificate upload
65	65	63	The solution should use a numeric risk score and MITRE mapping for each attacker based on dynamic analysis of attacker behaviour. It should also include risk categorization as critical / high /medium / low buckets.	We request the bank to modify the clause to "The solution should use a numeric risk score or MITRE mapping for each attacker based on dynamic analysis of attacker behaviour. It should also include risk categorization as critical / high /medium / low buckets."	No change	No change in the terms of the RFP.
66	80	10	i. The initial requirement for the Cyber Security Threat Deception (Honeypot) Solution is for 169 “User Systems” in offices/branches/DC, 72 VLANs, 118 Decoys (36 Active Directory decoys, 10 email decoys, 24 Web Decoy, 24 DB Decoy, 24 File Server Decoy) in 2 DC locations (including subscription licenses) . ii. The solution should be scalable and designed to cater to the Cyber Security Threat Deception (Honeypot) Solution requirement for 5000 “User Systems” in offices/branches/DC, 144 VLANs, 190 Decoys (36 Active Directory decoys, 10 email decoys, 48 Web Decoys, 48 DB Decoys, 48 File Server Decoys) in 2 DC locations (including subscription licenses) iii. Hardware should support minimum 3 lac endpoints, 144 VLANs & 190 Decoys. iv. The Bank initially proposes to procure 5000 licenses. Thereafter, based on the requirement additional licenses would be procured. The licenses requirements have been split into slabs such as 5,001 to 20000; 20001 to 50000; 50001 to 100000 and so on.	We request the bank to please clarify the below for sizing the Bill of Materials. 1. Whether the solution needs to be deployed in different zones like DMZ, Internal, Partners for DC and DR. 2. In point (i) 169 user systems are mentioned but point (iv) mentions 5000 licenses. We request the bank to clarify the actual number of endpoints to be covered as part of this RFP.	Clarification	1. Sufficient provisions has to be made as per best industry practice. As of now Bank needs appliances to be deployed in High Availability (HA) mode in Two Zones at each DC & DR. 2. To start with 169 users systems and 5000 endpoints licences are considered in this RFP. Bank shall take a decision to install more end points in due course.
67	53	Annexure B (Eligibility Criteria, Point 5)	Bidder should have experience of minimum one year in providing the Software Solution/services.	Kindly consider Bidder experience of **deception solution** in BFSI segment " The Bidder should have an experience of minimum one year in providing the **proposed deception soltware/solution in BFSI segment with atleast 20,000 end points"**	No change	No change in the terms of the RFP.

68	NA	Additional	OEM should have experince of minimum three years in providing the proposed deception software solution/services	Proposed OEM soultion should have successfully working for atleast 50,000 end points in a single installation for top Indian/Blue chip/BSFI sector company in India during last three years	Clarification	If Vendor would like to provide any additional/value added feature, can proivde without any additional cost to the bank
69	NA	Additional	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.	Clarification	If Vendor would like to provide any additional/value added feature, can proivde without any additional cost to the bank
70	NA	Additional	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.	Clarification	If Vendor would like to provide any additional/value added feature, can proivde without any additional cost to the bank
71	NA	Additional	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.	Clarification	If Vendor would like to provide any additional/value added feature, can proivde without any additional cost to the bank
72	NA	Additional	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.	Clarification	If Vendor would like to provide any additional/value added feature, can proivde without any additional cost to the bank
73	NA	Additional	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.	Clarification	If Vendor would like to provide any additional/value added feature, can proivde without any additional cost to the bank
74	NA	Additional	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.	Clarification	If Vendor would like to provide any additional/value added feature, can proivde without any additional cost to the bank
75	NA	Additional	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.	Clarification	If Vendor would like to provide any additional/value added feature, can proivde without any additional cost to the bank
76	NA	Additional	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.	Clarification	If Vendor would like to provide any additional/value added feature, can proivde without any additional cost to the bank
77	54	6	The Bidder (including its OEM, if any) should either be Class-I or Class-II local supplier as defined under this RFP. Certificate of local content to be submitted as per Appendix-G.	We request you to allow exemption to MSME Companies and if OEM is not present in India as per this clause, he can't participate in this tender with its Partner. Requested you to kindly amend this clause and give MSME Companies the relaxation.	No change	No change in the terms of the RFP.

78	54	11	The bidder, if participating as Channel Partner of any OEM, then OEM should have a support center and level 3 escalation (highest) located in India. For OEMs, directly participating, the conditions mentioned above for support center remain applicable. Bidder should specifically certify in **Appendix-A** in this regard.	This clause is favoring to particular OEM. In case of an international OEM with Indian partner front ending the bid, resources of the Indian partner present pan India would be trained /certified by OEM. This clause requires amendment. We request you to change to Operational support mechanism with SI be available in India.	No change	No change in the terms of the RFP.
79	57	Technical Specifications Clause No. 6	VMs with Windows, Linux, HP-UX, Unix (different flavors of Unix), AIX server can be used as part of solution to simulate such trap environment.	This point i.e. AIX Server is favoring to a particular Server OEM. Requested to relax this clause, as other OEM's can simulate such trap environment on HP, Dell or Lenovo servers.	No change	No change in the terms of the RFP.
80	59	Technical Specifications Clause No. 15	Ability to create deception of any web or mobile application to cover attacks on Mobile endpoints connected to Data centre Servers.	This deployment is customized to particular OEM and other OEM's has different system architecture for implementing the solution using deception technology (Lures and Decoys). We request you to make this clause generic, so as to make other OEM's to participate in this tender.	No change	No change in the terms of the RFP.
81	60	Technical Specifications Clause No. 22	The endpoint deception agent should be able to select users / computers on the basis of the following selection criteria (and not limited to): - Process list - Browser history - Installed programs – important files Interesting files - Recent commands - Active TCP connections - OU	This technology is particular to a single OEM. Requested you to dilute this point.	No change	No change in the terms of the RFP.
82	60	Technical Specifications Clause No. 23	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.	This technology is particular to a single OEM. Requested you to dilute this point.	No change	No change in the terms of the RFP.
83	60	Technical Specifications Clause No. 25	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.	This technology is particular to a single OEM. Requested you to dilute this point.	No change	No change in the terms of the RFP.
84	60	Technical Specifications Clause No. 27	The solution should have the ability to capture commands executed for high-interaction SSH connections on Linux decoys without any instrumentation processes or agents running within the decoys.	This deployment is customized to particular OEM and other OEM's has different system architecture for implementing the solution using deception technology (Lures and Decoys). We request you to make this clause generic, so as to make other OEM's to participate in this tender.	No change	No change in the terms of the RFP.
85	61	Technical Specifications Clause No. 30	The solution should be able to deploy built in application decoys that look like (and not limited to) webmail portals, VPN login portals, network printer, PIM login, HRMS, Email (Outlook/Lotus notes), Citrix, Cisco, GitLab, etc.	This technology is particular to a single OEM. Requested you to dilute this point.	No change	No change in the terms of the RFP.
86	61	Technical Specifications Clause No.33	Solution should include high-interaction Windows decoys that are accessible over the following channels: WMI, RDP, RPC-DCOM. NetBIOS, SMB and SNMP	This technology is particular to a single OEM. Requested you to dilute this point.	No change	No change in the terms of the RFP.
87	61	Technical Specifications Clause No. 34	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.	This requirement is specific to a particular OEM and other OEM's have different technology i.e. they don't allow the attacker to enter into the network.	No change	No change in the terms of the RFP.
88	62	Technical Specifications Clause No. 40	For authenticity, Linux high-interaction decoys should be one-to-one (the solution should not re-use of a few internal VMs configured with multiple IPs to show multiple decoys).	This technology is particular to a single OEM. Requested you to dilute this point.	No change	No change in the terms of the RFP.
89	62	Technical Specifications Clause No. 42	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.	This technology is particular to a single OEM. Requested you to dilute this point.	No change	No change in the terms of the RFP.
90	62	Technical Specifications Clause No. 43	Detections sent to the Sandbox should be visible in console with their results.	This technology is particular to a single OEM. Requested you to dilute this point.	No change	No change in the terms of the RFP.

91	66	Technical Specifications Clause No. 73	Solution should be able to generate actionable intelligence and should be able to integrate with existing threat intel platform	Requested to share the existing Threat Intel Platform for integration.	No change	No change in the terms of the RFP.
92	59	Technical Specifications Clause No. 20	The solution should be able to carry out a session replay of the attack carried out on the decoy for further analysis. The details available in session replay shall be mentioned in Remarks.	The solution is customized to a particular OEM and other OEM's have different system architecture for implementing the solution using deception technology (Lures and Decoys) We request you to make this point generic.	No change	No change in the terms of the RFP.
93	63	Technical Specifications Clause No. 50	Solution must allow visual dissection of the PCAP traffic and preserve all network traffic to and from the decoys while having the ability to export PCAPs based on a time filter.	The solution is customized to particular OEM and other OEM's have different system architecture for implementing the solution. We request you to make this point generic.	No change	No change in the terms of the RFP.
94	65	Technical Specifications Clause No. 63	The solution should use a numeric risk score and MITRE mapping for each attacker based on dynamic analysis of attacker behaviour. It should also include risk categorization as critical / high /medium / low buckets.	The solution is customized to particular OEM and other OEM's have different system architecture for attack behaviour. We request you to make this point generic.	No change	No change in the terms of the RFP.
95	66	Technical Specifications Clause No. 75	The solution must have the ability to reconstruct raw attack data into plain English attack analysis. It must also provide attacker / APT group attribution, mitigation recommendations, MITRE mapping within the user interface for the analyst.	The solution is customized to particular OEM and other OEM's have different attack analysis. We request you to make this point generic.	No change	No change in the terms of the RFP.
96	62	Technical Specifications Clause No. 41	For security, the base operating platform (host operating platform on which the decoys run) of the deception appliance should not be on Linux or Windows which are prone to regular remotely exploitable vulnerabilities.	This requires elaboration on same.	Clarification	Linux or Windows versions which are prone to regular remotely exploitable vulnerabilities should not be used
97	66	Technical Specifications Clause No. 74	The system must have the ability to save and share custom views filtered based on time and any event metadata for analyzing specific events. Results of saved queries must be exportable.	Requested you to kindly elaborate this point.	Clarification	Statement is self explanatory
98	63	Technical Specifications Clause No. 51	Decoys must be very robust and shall never interfere with business functions/ objectives of the setup where they are placed.	This solution is customized and favoring to a particulate OEM, Different OEM had different system architecture. We request you to make this point generic.	No change	No change in the terms of the RFP.
99	80	Scope of Work and Payment Schedule **Clause No. 10**	The initial requirement for the Cyber Security Threat Deception (Honeypot) Solution is for 169 “User Systems” in offices/branches/DC, 72 VLANs, 118 Decoys (36 Active Directory decoys, 10 email decoys, 24 Web Decoy, 24 DB Decoy, 24 File Server Decoy) in 2 DC locations (including subscription licenses). ii. The solution should be scalable and designed to cater to the Cyber Security Threat Deception (Honeypot) Solution requirement for 5000 “User Systems” in offices/branches/DC, 144 VLANs, 190 Decoys (36 Active Directory decoys, 10 email decoys, 48 Web Decoys, 48 DB Decoys, 48 File Server Decoys) in 2 DC locations (including subscription licenses) iii. Hardware should support minimum 3 lac endpoints, 144 VLANs & 190 Decoys. iv. The Bank initially proposes to procure 5000 licenses. Thereafter, based on the requirement additional licenses would be procured. The licenses requirements have been split into slabs such as 5,001 to 20000; 20001 to 50000; 50001 to 100000 and so on. The rate shall be discovered for 5000 end point licenses for a period of 5 years. Then this rate would be used for discovering rates for various slabs using multiplication factor mentioned in the below table. The rate arrived at after using multiplication factor shall be divided by the highest value of the slab to arrive at per licenses value. This value would be used for arriving at rate for the additional licenses. The payment shall be made for actual number of licenses procured and for the period put to use.	This solution is customized and favoring to a particular OEM, Different OEM had different system architecture using deception technology (Lures and Decoys). We request you to remove this point and should be open for all the OEM.	Clarification	Vendor can provide a solution with different architecture that achieves the purposes specified in technical specifications of RFP

<table>
<tr><td>100</td><td>84</td><td>Scope of Work and Payment Schedule
Clause No. 13</td><td>The initial requirement for the Cyber Security Threat Deception (Honeypot) Solution is for 169 “User Systems” in offices/branches/DC, 72 VLANs, 118 Decoys (36 Active Directory decoys, 10 email decoys, 24 Web Decoy, 24 DB Decoy, 24 File Server Decoy) in 2 DC locations (including subscription licenses)</td><td>The POC is customized and favoring to a particular OEM, Different OEM had different system architecture using deception technology (Lures and Decoys). We request you to remove this point and should be open for all the OEM.</td><td>Clarification</td><td>Vendor can provide a solution with different architecture that achieves the purposes specified in technical specifications of RFP</td></tr>
<tr><td>101</td><td colspan="3">Payment schedule for Required Hardware for the solution with required OS, Database License and other Licenses will be as under:
<table><tr><th>Sl.</th><th>Payment Stage</th><th>% of Payment</th></tr><tr><td>1</td><td>Hardware (Hardware Appliance / Server / Other Items etc.)</td><td>50 % of the cost of the hardware will be paid against proof of delivery of equipment</td></tr><tr><td>2</td><td>Software (End Points, Decoys, OS & DB Licenses etc.)</td><td>50 % of the cost of the software will be paid against proof of delivery of licenses/software</td></tr><tr><td>3</td><td>Installation/ Commissioning</td><td>On completion of Task</td></tr><tr><td>4</td><td>UAT & Production & Go Live</td><td>40 % of Hardware & Software/Licenses Cost after two months of successful running of product /solution and the final 10% against submission of performance Bank Guarantee valid for 63 months.</td></tr><tr><td>5</td><td>Onsite Technical Support (OTS) Cost of two L2 Resources at GITC Navi Mumbai</td><td>Quarterly arrear basis. (after deduction of penalties, if any).</td></tr><tr><td>6</td><td>Training and Certification (from OEM) for Deployment and Management of Cyber Security Threat Deception (Honeypot) Solution of 10 officials every year</td><td>Yearly in arrears and within one month after submission of invoices</td></tr><tr><td></td><td>Comprehensive warranty for Products for 05 years.</td><td></td></tr></table></td><td>Requested you to make the Hardware and software payment 80% on Delivery, as OEM takes 100% payment advance before dispatching the Hardware and Software.
UAT & Production and Go Live: SBI would be keeping the PBG of 3% for next 5 Years, so requesting you to release the balance 20% Payment of satisfactory installation within 30 Days.
Comprehensive warranty for Products for 05 years. – Requested you to release 5 Years warranty payment as per above two request.</td><td>No change</td><td>No change in the terms of the RFP.</td></tr>
</table>

	7	Warranty period will start from the date of acceptance of solution by the Bank.	Yearly in arrears and within one month after submission of invoices			