इंडियन बैंक Indian Bank
इलाहाबाद ALLAHABAD

CO: Information Technology Department

Date: 25.03.2022

Clarifications to the Pre-Bid Queries- RFP for Procurement of Incident Response [IR] Service for

Cyber Security Incidents and Cyber Security Preparedness of the bank Ref: CO/ITD/2486/R1/2021-22 dated 14/03/2022

Clarifications

S.No.	RFP Clause	Query Raised	Clarification
1	**Page No. 1 - Last Date for receipt of bids** 06/04/2022 at 03:00 PM	Request you to clarify and keep the last date of submission of Bid as 12 th April 2022.	Please Adhere to RFP timelines
2	**Page No. 14- Section III- Conditions of Contract - Point No. 5, Broad Scope of Work.**	1) Does 80 hours include SP/OEM support service and addon bidder hours or is it the total time between OEM and bidder 2) Is it 80 man-hours in total for individual consultants or per consultant support hours (You have mentioned at 2 consultants should be available on site within 24 hours)(for eg Initial response + acceptance time +2 consultant on site for 1 day will be equal to around 20 hours time) 3) Scope a, b (Initial response and proceed to acceptance) is per incident based and combination of onsite and offsite. Hence the efforts time will start right from initial triaging and response till end of completion of IT activities. Hence both off site time and on site will be considered to calculate the number of hours Please confirm. 4) Scope c (IRPS), is one time task to be done at start on engagement and in part of the 80 hours package , please confirm 5) Scope d (IR retainer) is to be done 2 time in a year and part of the 80 hour package. Please confirm.	*The scope of work of proposed solution is to procure Incident Response Retainer [IRR] Service for three years (80 hours per year), for Cyber Security incidents responses and Cyber Security preparedness of the Bank. * Both offsite and onsite time will be considered to calculate the number of hours. *(IRPS), is one time task to be done at start on engagement and in part of the 80 hours package in first year. *IR retainer services are part of the 80 hour package.

3	**Page No. 14- Section III- Conditions of Contract - Point No. 5, Broad Scope of Work.** **(a) Initial Response** (i) Triage Security issue on receipt of information from Bank immediately and should acknowledge within 2 Hours.	*Please clarify exactly what is expected in 2 Hrs time time frame, only acknowledge or Triaging post receipt of information. * SLA is 2 hours, wet will engage with Customer to determine if Incident Response Services are required or if we should able to effectively assist based on the situation.	Within 2 hours the vendor should acknowledge and determine if Incident Response Services are required or not
4	**Page No. 14- Section III- Conditions of Contract - Point No. 5, Broad Scope of Work.** **(a) Initial Response** (ii) Provide detailed information of the Threat Adversary identified in the initial assessment based on intelligence of service provider and experience.	*We will provide relevant available information of the Threat Adversary with us if the Threat Adversary has been identified in the initial assessment. * Will this require to submit our findings in form of a report? If yes, will the report be shared with any other third party? Does the Bank have any existing policies in place for Digital Forensics Collection, Incident Response and evidence storage?	Required information will be shared with service provider who is awarded with the contract
5	**Page No. 15- Section III- Conditions of Contract - Point No. 5, Broad Scope of Work.** **(a) Initial Response** (iii) Live response analysis of the systems to identify malicious activity within 4 hours of receipt of information from bank. The incident responder is expected to come online immediately on receipt of information.	*****Please clarify exactly what is expected in 4 Hrs time time frame, the responder is expected to come online and start analysis? *Live response takes 8 Hr to 48 hours to collect telemetry data from the system and another 8 to 16 hours for the analysis. Kindly suggest whether this is acceptable * In case of an incident, will the bank provide the required tools and systems to perform in house analysis or will the bank allow us to carry the acquired evidence to our forensic labs for processing? After the collection of evidence and analysis, where does the bank expect to store the evidence?	Bank is having various security tools in place, additional tools required for evidence collection or analysis to be arranged by the service provider. Collected evidence and analysis report to be shared to the bank.
6	**Page No. 15- Section III- Conditions of Contract - Point No. 5, Broad Scope of Work.** **(a) Initial Response** (iv) At least 2 consultants should be available onsite within 24 hours	*Since many incidents can be handled faster and better remotely by a larger pool of incident responders. Change required- At least 2 consultants should be available onsite within 24 hours as and when required. *We will try on best efforts basis and considering all the applicable travel restrictions. We will anyway initiate the IR services from	At least 2 consultants should be available onsite within 24 hours if required. Travel restrictions and travel time are accepted as additional hours. Locations

	excluding travel time.	Remote as per the SLA. Kindly suggest whether this is acceptable ***Which all locations are expected to be covered for this point?	required are Chennai and Mumbai.
7	**Page No. 15- Section III- Conditions of Contract - Point No. 5, Broad Scope of Work.** **(b) To Proceed Acceptance** Both bank team and responder accept mutually that incident response services are required to be concluded within 2 hours.	*As we understand that this is acknowledgement by both parties that IR services are required. Sometime this may take time to really understand if there ia an attack or not. Change Required- Both bank team and responder accept mutually that incident response services are required post analysing the incident logs. The same should try and be ascertained within 6-8 hours of getting the information. *Incident Service cannot be concluded in 2 hours. We will repond to Bank's request for IR activation with 2 hr (as per the contract). We will provide estimated hours required to work on the IR. Once approved by the Bank, we will activate IR retainer. The completion time depends on the time taken for investiation by us and implementation of recommendations by Bank. We believe the bank's expectation is to conclude within 2 HR SLA whether the IR services has to be intitated (or) Not. Kindly clarify.	Within 2 hours bidder should acknowledge and determine if Incident Response Services are required. Live response analysis of the systems to identify malicious activity within 4hours of receipt of information from bank. The incident responder is expected to come online immediately on receipt of information.
8	**Page No. 15- Section III- Conditions of Contract - Point No. 5, Broad Scope of Work.** **(c) INCIDENT RESPONSE PREPAREDNESS SERVICES(IRPS) DELIVERABLES OTHER THAN INCIDENT RESPONSE.** (i)Review of existing monitoring, logging and detection technologies (ii)Review current network and host architecture (iii)Evaluation of first response capabilities and provide necessary training	As we understand that this is required only once in the first year. Kindly clarify *The customer may choose to opt for an additional exercise called Incident Response Prepardness Service (IRPS), at an additional cost. This services will touch upon the necessary aspect wrt activating IR retainer contract. It also provides a high level of assessment on some of these things. We have separate comprehenive services to enable the BANK improve their Cyber Defence Capabilities, Response Readiness and Information Security Postures. KIndly clarify that this preparedness service is something which will be separate and charged additionally to the 80 Hours of IR. ***What all technologies are currently in place for monitoring, logging	**IRPS** is required on first year only. IRPS services will be included within 80 Hours package in first year**.**

	(iv)Recommendations for areas of improvement (v)Support in increasing the maturity level of bank to have ability to quickly contain an incident (vi)Cyber security IR Planning services to prepare the organization to better respond to cyber incidents and attacks.	and detection technologies?	
9	**Page No. 15- Section III- Conditions of Contract - Point No. 5, Broad Scope of Work.** **(d) CONSULTING AND EDUCATION SERVICES TO BE PROVIDED (IR RETAINER SERVICES)** (i) Incident Response tabletop exercise once in six months (ii) Response readiness assessment (iii) Cyber security and intelligence (iv) Security Incident First responder training to train key staff members to collect data, maintain chain of custody etc..	*Kindly Clarify frequency and details of other services leaving table top exercise. As understood that table top would be conducted once in six months for entire duration of three years, hence a total of 6 table top exercises are required. *****Should be scoped and priced separately (Not part of the 80 Hours and Preparedness Service) Kindly Clarify	CONSULTING AND EDUCATION SERVICES TO BE PROVIDED will be part of 80 Hours package. Bank will inform the requirement and hours applicable will be deducted by service provider
10	**Page No. 15- Section III- Conditions of Contract - Point No. 5, Broad Scope of Work.** **(e) Other terms and Conditions** **(ii)** Travel and accommodation expenses are to be borne by the successful bidder for one visit of 2 days for two persons per year. If any additional visit is required for incident Management, bank will reimburse actual expenditure.	Expenses for travel and accommodations will be charged separately on actual basis. We will seek explicit approval from the Bank before incurring any expenses. Since we have IR consultants in various region and we will not be able to upfront decide on the logistics cost and it will be known only when an IR service is triggered by the Bank team Requesting you to kindly accept the above request.	Please Adhere to RFP terms and conditions

11	**Page No. 17- Section III- Conditions of Contract - Point No. 6, Onsite Support.** Successful bidder has to do Live response analysis of the systems to identify malicious activity within 4 hours of receipt of information from bank. The incident responder is expected to come online immediately on receipt of information.	*The same is not in consonance with query for Para 5(a) (iii). Please clarify. *Live response takes 8 Hr to 48 hours to collect telemetry data from the system and another 8 to 16 hours for the analysis. Kindly suggest whether this is acceptable	Within 2 hours bidder should acknowledge and determine if Incident Response Services are required. Live response analysis should start within 4 hours of receipt of information from bank. The incident responder is expected to come online immediately on receipt of information**.**
12	**Page No. 17- Section III- Conditions of Contract - Point No. 7, Qualification Criteria.** 7(1) The Bidder should have turnover of at least ₹ 20 Crore (Rs. Twenty Crore only) each year for the preceding three Financial years. [2018-19, 2019-20, 2020-21]	*Can we request to relax the criteria to INR15 Cr each year. *We request you to allow exemption to MSME and Start-up companies	Please refer Amendment.
13	**Page No. 17- Section III- Conditions of Contract - Point No. 7, Qualification Criteria.** 7(4) Bidder should be providing Security operations Center (SOC) services to at least one BFSI organizations in India.	*OEM should be providing Incident Response services to at least one BFSI organizations in India & world. (Since Bank is asking for Incident Response services from OEM, we will request Bank to ask OEM for their references) Bidder should be providing Security operations Centre (SOC) services to at least one BFSI/Corporate organizations in India. *Bidder should be providing Security Operations Centre (SOC) Consulting/Implementation services to at least one BFSI/Private/PSU organizations in India.	Please refer to amendment

		*We request you to allow Corporate clients as well, where bidder has provided the SOC/ SIEM Services. So that other bidders can also participate.	
14	**Page No. 17- Section III- Conditions of Contract - Point No. 7, Qualification Criteria.** 7(6) The bidder shall be the OEM certified or authorized agent/ reseller/ partner of the solution offered for more than one year. The OEM should assure to provide support services to the Bank for 3 years.	The bidder shall be the OEM certified or authorized agent/ reseller/ partner of the solution offered for more than one year. The OEM should assure to provide support services to the Bank for **2** years.	Please Adhere to RFP terms
15	**Page No. 17- Section III- Conditions of Contract - Point No. 7, Qualification Criteria.** 7(7) The bidder should quote for the IR Services provided from any one of the following service providers 1.M/s IBM India Pvt Ltd 2.M/s Cisco systems 3.M/s Mandiant Solutions	*Does it mean the bidder needs go resell the IT services as offered by the mentioned Service provider /OEM *We request you to kindly remove the name of these OEM's, so that other OEM's should participate in the tender and you get one of best IR services at a better price. This will allow only these three companies to participate in the tender.	Yes. Please Adhere to RFP terms
16	**Page No. 17- Section III- Conditions of Contract - Point No. 8, Terms of Payment.** **(**2) No additional payment apart from the tender bid value will be made under any circumstances. If any additional visit is required (apart from one visit of 2 days for two persons per year) for incident Management, bank will reimburse actual expenditure.	*There may be additional payment required if more than 80 Hrs are required for Incident Response. Please see para 5 e (i) on Page 16 "If additional hours required for the incident response bank will pay for the additional hours as per the quoted rates."	Correct. For additional hours consumed by bank beyond 80 hours bank will make payment at mutually agreed cost.

17	**Page No. 27, 28 (point no 30,31)** (30) INSPECTION OF RECORDS Bank at its discretion may verify the accounts and records or appoint third party for verification including an auditor for audit of records including the solution provided to the Bank under the RFP and the Service Provider shall extend all cooperation in this regard. Service Provider shall provide unrestricted access to its premises and records being maintained with regard to the job being performed as per its contract with the Bank, to the authorized personnel of the Bank / its auditors (internal and external)/ any statutory / regulatory authority / authorized personnel from RBI to carry out any kind of process of audit including that of its operations and records related to the Bank, as per its own satisfaction at the office / factory or any other premises of the Service Provider, in the presence of representatives of the Service Provider, at any point of time by giving notice. 31) INSPECTIONS AND TESTS The Purchaser or its representative(s) shall have the right to visit and /or inspect any of the Bidder's premises to ensure that data provided by the Bank is not misused. The Purchaser shall notify the Supplier in	Given our confidentiality obligations with other Clients, we do not provide such broad audit rights to our Clients. If bank request, we shall provide the bank with time and expense related reports for the Services. Will this be agreeable?	Please Adhere to RFP terms

	writing, in a timely manner, of the identity of any representatives retained for these purposes. Any charges payable to the Purchaser's representative designated for inspection shall be borne by the Purchaser. Should any inspected or tested Goods/software fail to conform to the Specifications, the Purchaser may reject the Goods/software, and the Supplier shall make alterations necessary to meet specification requirements at no additional cost to the Purchaser. The Purchaser's right to inspect, test and, where necessary, reject the Goods or software after the delivery shall in no way be limited or waived by reason of the software having previously been inspected, tested and passed by the Purchaser.		
18	**Page No. 38- Part-II** Commercial Bid (To be submitted after Online Reverse Auction)	The bid format is only asking for pack of 80 hours. In case on completion of the 80 hours package, will bank considered change request for additional pack of 80 hours based on how many are consumed. The effort for IR may vary based on the type and impact of incidence. Post initial acceptance /triage and consultant arrival on site efforts bidder may arrive at the total time required. Will change request will be accepted while the IRR is being attended (refer point 3 as above)	For additional hours consumed by bank beyond 80 hours bank will make payment at mutually agreed cost
19	**Page No. 45 Annexure-V Non-Disclosure Agreement** NOW THERFORE THIS AGREEMENT WITNESSETH and it is hereby agreed by and	We have a fixed term for confidentiality obligations. We suggest a time frame of around 3-5 years. Hope this is agreeable.	Please Adhere to RFP terms

	between the parties hereto as follows		
20	**Page No. 55 Annexure-VII** **SERVICE LEVEL AGREEMENT** **(v) ONSITE SUPPORT:** The scope of work of proposed solution is to procure Incident Response Retainer [IRR] Service for 80 hours per year for Cyber Security preparedness and Cyber Security incidents responses of the Bank.	Requested you to explain the 80 Hrs calculation process.	80 Hours will be used as mentioned in the RFP Broad scope of work. For Triage Security issues if any, Incident response preparedness services(IRPS) once in a year, Consulting and Education Services(IR RETAINER SERVICES) as and when required
21	**Page No. 55 Annexure-VII** **SERVICE LEVEL AGREEMENT** **(v) ONSITE SUPPORT:** The service provider also to provide regular threat intelligence on likely threat the bank has and recommend for proactive actions.	Requested you to elaborate this point.	Threat intelligence to be provided by the service provider.
22	**Page No. 55 Annexure-VII** **SERVICE LEVEL AGREEMENT** **(v) ONSITE SUPPORT:** Live response analysis of the systems to identify malicious activity within 4 hours of receipt of information from bank. The incident responder is expected to come online immediately on receipt of information.	As per the RFP you had asked for two on-site Engineers and these services would be provided by Bidder OEM	At least 2 consultants should be available onsite within 24 hours if required excluding travel time.
23	**Page No. 59- Checklist** **S.no 4** Bidder should be providing Security operations Center (SOC) services to at least one BFSI	Bidder should be providing security operations centre (SOC) services to BFSI or enterprise organizations. Since this PO ask includes incident response is totally mandatory OEM offering hence we would appreciate if bank would change the clause that Bidder should	Please refer amendment

	organizations in India.	providing security operations centre (SOC) services to BFSI or enterprise organizations *OEM should be providing Incident Response services to at least one BFSI organizations in India & world. Since Bank is asking for Incident Response services from OEM, we will request Bank to ask OEM for their references	
24	**Additional Clause:**	**Limitation of the Bidder's Liability towards the Purchaser** The Client (and any others for whom Services are provided) shall not recover from the Bidder, in contract or tort, under statute or otherwise, any amount with respect to loss of profit, data or goodwill, or any other consequential, incidental, indirect, punitive or special damages in connection with claims arising out of this Agreement or otherwise relating to the Services, whether or not the likelihood of such loss or damage was contemplated. The Client (and any others for whom Services are provided) shall not recover from the Bidder, in contract or tort, including indemnification obligations under this contract, under statute or otherwise, aggregate damages in excess of the fees actually paid for the Services that directly caused the loss in connection with claims arising out of this Agreement or otherwise relating to the Services	Please Adhere to RFP terms
25	**Additional Clause:**	**Indemnity** The Client shall indemnify and hold harmless the GT Entities and GT Bharat LLP for all Losses incurred in connection with any third-party Claim, except to the extent finally judicially determined to have resulted primarily from the fraud or bad faith of such GT Entity or GT Bharat LLP	Please Adhere to RFP terms
26	**Additional Clause:**	**Non-solicitation** During the Restricted Period, no Engagement Personnel of either party shall solicit for employment any Engagement Personnel of the other party. "Engagement Personnel" shall be defined as only those personnel of either party who a) are directly involved in the provision of Services under the applicable Statement of Work, or b) are the	Please Adhere to RFP terms

		direct recipients of such Services. The "Restricted Period" shall be defined to include a) the Term of the applicable Statement of Work, b) a period of 12 months after the expiration of such Term, and c) for those Engagement Personnel whose involvement as a direct provider or recipient of Services ends prior to the expiration of the Term, for 12 months after such involvement ends. Provided, that this restriction shall not apply to (i) Engagement Personnel of a party who respond to general advertisements for positions with the other party, (ii) Engagement Personnel of either party who come to the other party on their own initiative without direct or indirect encouragement from the other party's Engagement Personnel, or (iii) generic recruiting activities by non-Engagement Personnel, including direct outreach by recruiters of either party who have sourced the individuals in the ordinary course of recruiting through the use of research, agencies, social media and/or other technology or tools	
27	**Additional Clause:**	**Force Majeure** Force Majeure to facilitate remote working. i. To the extent that the provision of the Services is impacted by a pandemic (including COVID19) and any reasonable concerns or measures taken to protect the health and safety interests of either Party's personnel, the Parties will work together to amend the Agreement to provide for the Services to be delivered in an appropriate manner, including any resulting modifications with respect to the timelines, location, or manner of the delivery of Services. ii. Where the Bidder Personnel are required to be present at Client's premises, the Bidder will use reasonable efforts to provide the Services on-site at Client side, provided that, in light of a pandemic the parties agree to cooperate to allow for remote working and/or an extended timeframe to the extent a. any government or similar entity implements restrictions that may interfere with provision of onsite Services; b. either party implements voluntary limitations on travel or meetings that could interfere with provision of onsite Services, orc. an bidder's resource determines that he or she is unable or unwilling to travel in light of a pandemic-related risk.	Please Adhere to RFP terms

28	**Additional Clause:**	**Retention of Copies** Request you to kindly consider the clause as under: The Bidder shall be permitted to retain all information and documents as maybe required for legal or professional regulatory purposes, provided that such retained information remains subject to confidentiality obligations for the entire retention period.	Please Adhere to RFP terms
29	**Additional Clause:**	**Non-Exclusivity** Request you to kindly consider the clause as under: It is agreed that the services are being rendered on a non-exclusive basis and the Bidder shall have the right to pursue business opportunities that it may in its sole discretion deem appropriate.	Please Adhere to RFP terms