



UCO BANK

Department of Information Technology

Request for Proposal (RFP) for “Implementation of Advanced Persistent Threat (APT) device”

RFP REF NO: DIT/BPR & BTB/OA/2241/2018-19 Date: 17/08/2018

Pre-Bid Responses/ Clarifications to Queries raised by the Bidder(s), Amendments, Addendums and Corrigendum's

Sl. No	Page. No.	Clause No	Clause as per RFP	Description of Query/ Clarification sought by Bidder	Bank Response
1	23 & 26	PART – IV SECTION – 1	<p>Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. xxvi The bidder should have a 24x7 365 days support contact center in order to log the calls. The contact center numbers should be provided to the Bank along with the escalation matrix mentioning the contact person's name, number and designation in the company.</p> <p>Scope of Work: 2.6. System Maintenance & Support Services: Point no. a: 24 x 7 online support</p>	<ul style="list-style-type: none"> • Can bidder propose 24x7 support contact center from OEM along with OEM escalation matrix? • Can bidder propose 24x7 online supports from OEM? 	<p>Bank will make direct correspondence with the bidder only.</p> <p>The bidder should have back to back arrangement with the OEM so that bank will be able to log a call with the OEM directly.</p>

2	24	PART – IV SECTION – 1	Scope of Work: POC (Proof of Concept)	Does the POC needs to be done at UCO bank premises or can it be performed from OEM POC setup?	Clause stands as per RFP.
3	25	PART – IV SECTION – 1	Scope of Work: 2.6. System Maintenance & Support Services: Point no.1: Monitoring & Log Analysis Services On server and consoles.	Can bidder perform monitoring and log analysis services through remote session?	It has to be onsite only as and when required.
4	42	PART-V	3. Delivery and Installation Point no. 3.1: Deliveries of the equipment, installation and operationalization of complete solution at all locations should be made within 4 weeks from the date of purchase order.	We request to change the clause to "Deliveries of the equipment, installation and operationalization of complete solution at all locations should be made within Twelve Weeks from the date of acceptance of PO"	Clause stands as per RFP.
5	46	PART-V	10. Warranty Point no. 10.2: The warranty period will be 36 months from date of successful deployment of APT at the respective location/s and 3 years of Support and warranty period.	We request to change the clause to "The warranty period will be 36 months from date of issue of PO".	Clause stands as per RFP.
6	9 & 58	Part – I 3. Eligibility Criteria & Annexure – B Eligibility Criteria compliance	Point no.6: The bidder must have implemented at least two APT solutions in a BFSI / E-Commerce environment or at Banks in India. Documents to be submitted: PO / Invoice and satisfactory certificate from client to be submitted. Details to be furnished along with the references.	<ul style="list-style-type: none"> We request to change the clause to "PO / Invoice or satisfactory certificate from client to be submitted. Details to be furnished along with the references". Relevant PO or declaration letter mentioning APT is under implementation at least two APT solutions in a BFSI / Ecommerce Environment or at Banks in India. Can you please include bidder / OEM. Requesting to modify the clause as below. "The bidder / OEM must have implemented at least two APT solutions in a BFSI / E-Commerce environment or at Banks in India." 	<p>The modified clause to be read as under:</p> <p>Point no.6: The bidder must have implemented at least one APT solution in a BFSI / E-Commerce environment or at Banks in India. Documents to be submitted: PO / Invoice and satisfactory certificate from client to be submitted. Details to be furnished along with the references.</p>

				<p>Or</p> <p>"The bidder must have implemented at least one APT solution in a BFSI / E-Commerce environment or at Banks in India."</p> <p>Or</p> <p>"The bidder must have implemented at least two APT solutions, one of which should be in a BFSI / E-Commerce environment or at Banks in India."</p>	
7	63	Annexure – E Technical Bill of Material	Sl. No. 1: Advanced Persistent Threat Prevention (APT) device with 3 years warranty QTY-2	Does bidder has to propose 2 appliances in HA at DC or is it standalone appliances in DC & DR each?	Two standalone appliances at DR.
8	28	PART – IV SECTION – 2 1. TECHNICAL REQUIREMENTS	Clause no. 4: Sandboxing capabilities of following Operating Systems (32 and 64 bit) : Win XP, Win7, Win8.x, Win10.x, Server 2008 R2, 2012 R2, Linux, Unix and MAC OS, all industry standard OS	<ul style="list-style-type: none"> This point is specific to a particular vendor. We request to modify the clause as "Sandboxing capabilities of following Operating Systems (32 and 64 bit) : Win XP, Win7, Win8.x, Win10.x, Server 2008 R2, 2012 R2 and should be able to perform static analysis for Linux, MAC OS or any x86 platform". Please specify the need for Linux /Unix Sandbox. The Hypervisor used by sandboxing solution must not be an OEM solution such as from VM Ware, Hyper V, Virtual Box, RHEV etc. however it should be a custom Hypervisor purpose built for sandboxing requirement. Contradictory to the clause of OS Agnosticism mentioned in clause number 18. We request to delete the clause 	<p>The modified clause to be read as under:</p> <p>PART – IV: SECTION – 2</p> <p>1. TECHNICAL REQUIREMENTS:</p> <p>As per the RFP clause no.4, page no 28, Sandboxing capabilities of following Operating Systems (32 and 64 bit): Win XP, Win7, Win8.x, Win10.x, Server 2008 R2, and 2012 R2. In addition to the requirement static analysis for Linux, MAC OS or any x86 platform by the solution is preferable.</p>

				<ul style="list-style-type: none"> • Sandboxing is asked to be agnostic of OS and thus this clause is contradictory to clause 18. Request to remove Linux, UNIX and MAC OS sandboxing as clause asks for OS agnosticism. <p>Only one Anti-APT solution vendor have MAC OS sandbox capability, Only one have Linux sandboxing capability but no vendor have UNIX sandboxing capability. As you cannot buy WinXP now because Microsoft declared the same as EOL. So most of the sandbox solution cannot give WinXP environment too. - Sandboxing capabilities of following Operating Systems (32 and 64 bit) : Win7, Win8.x, Win10.x, Server 2008 R2, 2012 R2 etc. all industry standard OS</p> <ul style="list-style-type: none"> • Sandboxing capabilities of following Operating Systems (32 and 64 bit) : Win7, Win8.x, Win10.x, Server 2008 R2, 2012 R2 etc. all industry standard OS • We request to delete the clause. 	
9	28	PART – IV SECTION – 2 1. TECHNICAL REQUIREMENTS	Clause no. 16: Solution/appliance must have RAID redundancy (for hard drives), network redundancy (for management network interfaces), power Supply and Fan module redundancy.	<ul style="list-style-type: none"> • Request to modify the clause as "Solution/appliance must have RAID redundancy (for hard drives), power Supply and Fan module redundancy. • Management solution does not need to be dedicated and can be performed over management IP addresses connected to redundant 	Clause stands as per RFP.

				switches in the datacenter. Request to modify the clause as "Solution/appliance must have RAID redundancy (for hard drives), power Supply and Fan module redundancy.	
10	28	PART – IV Section – 2	1. Technical Requirements & 2. Technical Specifications	Kindly clarify the specifications to be followed for the APT solution	Clause stands as per RFP.
11	28	PART – IV Section – 2	1. Technical Requirements & 2. Technical Specifications	Kindly clarify whether the APT solution is to be sized to handle more than 10,000 users.	Clause stands as per RFP.
12	23	PART – IV SECTION – 1	Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. xv: The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance.	Kindly clarify the overall bandwidth to be handled by the APT solution per each interface like internet, DMZ, WAN etc.	At least 1gbps bandwidth to be handled by the APT solution in total.
13	24	PART – IV SECTION – 1	Scope of Work: POC (Proof of Concept): Technically qualified bidders should conduct POC (Proof of Concept) within 1 week (7 working days from the date of mail sent to the technically qualified bidders)	Kindly clarify the scope of the POC like functionalities to be tested, exploit simulation and blocking, reports and integration capabilities with the existing environment, etc.	Technical POC as per industry standard.
14	24	PART – IV SECTION – 1	Scope of Work: POC (Proof of Concept): Technically qualified bidders should conduct POC (Proof of Concept) within 1 week (7 working days from the date of mail sent to the technically qualified bidders)	<ul style="list-style-type: none"> Kindly extend the duration of providing the appliance from 7 days to 21 days as this would involve logistics dependency and regulatory permissions to be obtained - if needed. We request the tendering committee to extend POC timeline to 3 weeks (21 days) from the date of email. 	The modified clause to be read as under: PART – IV: Section – 1 Scope of Work: POC (Proof of Concept): Technically qualified bidders should conduct POC (Proof of Concept) within 10 working days from the date of mail sent to the technically qualified bidder.

				<ul style="list-style-type: none"> • Kindly clarify whether the POC needs to be conducted on the live environment or separate testing environment. Kindly also clarify the details of the requirement to be demonstrated. Request to extend the duration specified to start the POC from the date of mail sent as it involves multiple formalities to be executed. • Kindly provide the scope of work of the POC and request to extend the date to at least 15 days for completion of the POC. • POC appliance arrangement - Kindly extend the duration of providing the appliance from 7 days to atleast three weeks. 	
15	42	PART-V	<p>2. Performance Bank Guarantee</p> <p>The successful bidder shall be required to provide a Bank Guarantee for 10% of the Total Order Value issued by any scheduled commercial bank (other than UCO Bank) valid for 39 months (36+3 months claim period), from the issuance of Purchase Order (PO), indemnifying any loss to the Bank, as per the format of Annexure – J. The bank guarantee shall be provided to the bank either before or at the time of execution of the Service Level Agreement (SLA). Upon furnishing the Performance Bank Guarantee, the EMD of the selected bidder shall be returned.</p> <p>The Performance Bank Guarantee shall act as a security deposit and either in case the successful bidder is unable to start the project within the stipulated time or start of the project is delayed inordinately beyond the acceptable levels, the Bank reserves the right to forfeit</p>	<p>1. Performance guarantee (PBG) to be provided at 5% of annual contract value and shall be renewed yearly at 5% of relevant subsequent year's contract value.</p> <p>2. Customer shall invoke the PBG only on occurrence of material breach and after providing 30 days cure period to the bidder to rectify the material breach for which the PBG is sought to be invoked.</p>	Clause stands as per RFP.

			<p>the same. Further, the Bank reserves the right to invoke the Performance Bank Guarantee in case the successful bidder is not able to fulfill any or all conditions specified in the document or is unable to complete the project within the stipulated time. This is independent of the LD on Delivery and installation.</p>		
16	43	PART-V	<p>4. Payment Terms:</p> <p>4.1 80% of the order value along with GST and other applicable duties on actual basis will be paid on delivery, installation and acceptance of ordered items, after realizing penalty charges for late delivery and / or late installation, if any. The claim for payment should contain proof of delivery, installation report & User Acceptance Report signed by an authorized official of the bank / branch at the respective sites etc.</p> <p>4.2 The balance 20% of order value will be paid after 3 months of successful running of Advanced Persistent Threat (APT) on submission of the Performance Bank Guarantee (PBG) of the equivalent amount.</p> <p>4.3 In case installation is held up by the Bank for site non-readiness, the payment may be released after 30 days from delivery on production of Site Non-Readiness (SNR) certificate from the competent authority at the delivery site.</p>	<ul style="list-style-type: none"> • Hardware/Software – 100% payment shall be made on delivery. <p>AMC/ATS – Payment shall be made yearly in advance for the subsequent years. Support - Payment shall be made monthly in arrears. Payment shall be made within 30 days from the date of Invoice. Bidder seeks right to terminate the contract in the event of delay in payment of undisputed invoice. Late payment will bear an interest of 2% per month.</p> <ul style="list-style-type: none"> • We request modification of Payment term to: <ol style="list-style-type: none"> 1) 80% of the order value along with GST and other applicable duties on actual basis to be paid on delivery. 2) 15% of the order value to be paid after installation and acceptance of ordered items, after realizing penalty charges for late delivery and / or late installation, if any. 3) The balance 5% of order value to be paid after 3 months of 	<p>Clause stands as per RFP.</p>

				successful running of Advanced Persistent Threat (APT) on submission of the Performance Bank Guarantee (PBG) of the equivalent amount.	
17	44 & 45	PART-V	<p>8. Penalty:</p> <ul style="list-style-type: none"> • If the Vendor fails to maintain guaranteed monthly uptime of 99.5 % of each individual solution, the Bank shall impose penalty as mentioned below on slab basis. • Bank may recover such amount of penalties due to delay in service from any payment being released to the vendor, irrespective of the fact whether such payment is relating to this contract or otherwise. The same may be recovered from the payment due towards the vendor or from the retention money at the end of contract period. 	<ul style="list-style-type: none"> • Maximum SLA Penalties should be capped at 5% of the applicable service fees for that month. • Bidder requests that the Customer be entitled to set-off the penalties due to the Customer only with the amount which is due to bidder under this contract and not any other contract. 	Clause stands as per RFP.
18	45 & 46	PART-V	<p>9. Liquidated Damage:</p> <p>Notwithstanding the Bank's right to cancel the order, liquidated damages at 1% (One percent) of the Total Cost of Ownership (TCO) price per week will be charged for every week's delay in the specified implementation schedule i.e. 4 weeks from the date of issuance of Purchase Order (PO). The Liquidated Damages including Service Level Penalties would be subject to a maximum of 10% of the total project cost. Bank will have right to recover these amounts by any mode such as adjusting from any payments to be made to the selected bidder or from the performance Bank</p>	<ul style="list-style-type: none"> • Liquidated damages should be applicable only in the event of delay in delivery is solely attributable to the Bidder and should be computed at the rate of 0.5% of the value of the affected service or product per week subject to the maximum of 5% of the value of affected service or product. • Liquidated damages should be applicable only in the event of delay in delivery is solely attributable to the Bidder and should be computed at the rate of 0.5% of the value of the affected service or 	Clause stands as per RFP.

			<p>Guarantee. Liquidated damages will be calculated per week basis.</p> <p>The Bidder shall perform its obligations under the agreement entered into with the Bank, in a professional manner. Bank may invoke the Bank Guarantee for further delay in start of the services.</p>	<p>product per week subject to the maximum of 5% of the value of affected service or product. It is recommended that a minimum cure period of 30 days should be provided prior to imposing liquidated damages.</p>	
19	47	PART-V	<p>12. Contract Period:</p> <p>The tenure of the Contract will be for a period of 3 (three) years</p>	<p>The contract tenure of 3 years is including or excluding installation/implementation phase?</p>	<p>Clause stands as per RFP.</p>
20	48	PART-V	<p>12. Contract Period:</p> <p>However, after the completion of initial period of 3 (three) years with warranty, the contract may be extended/renewed for further period on such terms and conditions as would be decided by the Bank.</p>	<p>After the completion of initial period of 3 (three) years with warranty, the contract may be extended/renewed for further period on such terms and conditions as would be decided & agreed upon mutually by both the parties.</p>	<p>Clause stands as per RFP.</p>
21	48, 51 & 53	PART-V	<p>12. Contract Period:</p> <p>The performance of the selected bidder shall be reviewed every quarter and the Bank reserves the right to terminate the contract at its sole discretion by giving 90 days 'notice without assigning any reasons and without any cost or compensation therefor. Any offer falling short of the contract validity period is liable for rejection.</p> <p>22. Exit Option and Contract Re-Negotiation:</p> <p>The Bank reserves the right to cancel the contract in the event of happening one or more of the following Conditions.</p> <p>24. Termination:</p> <p>UCO BANK reserves the right to cancel the work/purchase order or terminate the SLA by giving 90 (ninety) days' prior notice in writing and recover damages, costs and expenses etc., incurred by Bank</p>	<p>Contract shall be terminated only for serious and material breaches and not for minor breaches/delays or for convenience. We further request that the bidder should be allowed a cure period of a minimum of 30 days prior to issuance of notice of default for termination of the contract.</p> <p>Bank shall make all the payments for products / services delivered by the Bidder and any liability towards the third party vendors till the date of termination. Bank shall also be liable to pay stranded cost to the bidder in case of termination.</p>	<p>Clause stands as per RFP.</p>

			under the following circumstances.		
22	51	PART-V	22. Exit Option and Contract Re-Negotiation: The Bank will reserve a right to re-negotiate the price and terms of the entire contract with the Selected Bidder at more favorable terms in case such terms are offered in the industry at that time for projects of similar and comparable size, scope and quality.	Any re-negotiation of price & terms of the contract shall be mutually discussed and agreed upon between both the parties.	Clause stands as per RFP.
23	64 & 66	Annexure – F & Annexure – G	Masked commercial format & Commercial format	There is no placeholder to provide the 3 years support cost. Please clarify.	Bidder should quote 2 numbers of Advanced Persistent Threat Prevention (APT) device with 3 years warranty which covers repair, replace and support services.
24	76 & 77	Annexure – K PRE CONTRACT INTEGRITY PACT	Point no. 7. 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	<ul style="list-style-type: none"> Request for deletion of this clause. Alternatively, the Bidder requests the bank to replace the existing language with this suggested language. "The BIDDER undertakes that it has not supplied/is not supplying same product/systems or subsystems as a whole solution with same scope and terms and conditions, within a period of 1 year prior to the bid submission date, at a price lower than that offered in the present bid in respect of any other Public Sector Banks in India and if it is found within one year after the signing of contract that same product/systems or subsystems as a whole solution with same scope and terms and conditions was supplied by the BIDDER to any other Public Sector Bank in India at a lower price within a period of one year before the bid	Clause stands as per RFP.

				<p>submission date, 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 adjusted by the BIDDER in its invoices to the BUYER, if the contract has already been concluded."</p> <ul style="list-style-type: none"> • Price is always dependent on various factors and some of them are identified below. The integrity pact is for ensuring that bidders don't indulge in unethical behavior and ensuring competitiveness. The undertaking above shall not be applicable and we request that this clause is deleted. If Bank is not keen to delete the clause we kindly request the Bank to clarify: <ul style="list-style-type: none"> i) that the undertaking above is only applicable if all other factors are identical. <ul style="list-style-type: none"> a) payment terms (advance or arrears or 30 days to 90 days payment terms) b) supply on best effort basis as against supply with liquidated damages and the rate of LD c) commercial and legal risk elements in contract d) place of supply (supply in centralized model as against decentralized model or supply in metros as against remote location) e) volume f) discount offered by OEM 	
--	--	--	--	---	--

				<p>ii) that in the event the bidder doesn't have a control over price due to reason beyond its control (percentage of discount provided by OEM) the same shall be taken into account.</p> <p>iii) that in case bidder doesn't have a tracking mechanism for tracking price, bidder shall be allowed to make such declaration.</p> <p>iv) that the clause shall only be effective prospectively and not retrospectively.</p> <p>v) that this kind of undertaking may have adverse impact on competition and in the event this is treated as anti-competitive the bidder shall not be liable.</p>	
25	12	Part – II: INVITATION FOR BIDS AND INSTRUCTIONS TO BIDDERS	<p>Clause 4: Earnest Money Deposit</p> <p>The Earnest Money Deposit may be forfeited under the following circumstances:</p> <p>The bidder violates any of the provisions of the terms and conditions of this tender specification.</p> <p>In case of the successful bidder, if the bidder fails: To sign the contract in the form and manner to the satisfaction of UCO BANK.</p>	<p>We request that this sub-clause while specifies forfeiture of EMD if bidder is in "violation of any provisions" should be deleted.</p> <p>Please clarify whether inclusion of deviations in the bid proposal could also result in forfeiture of the EMD.</p>	Clause stands as per RFP.
26	13	Part – II: INVITATION FOR BIDS AND INSTRUCTIONS TO	<p>5. Rejection of the Bid:</p> <p>Bidder should comply with all the points mentioned in the RFP. Noncompliance of any point will lead to rejection of the bid.</p>	<p>We request that this RFP be permitted to be a deviation bid. We submit that the contract to be signed between the Bank and the bidder should be a</p>	Clause stands as per RFP.

		BIDDERS		mutually acceptable agreement, incorporating the terms of bidder's proposal.	
27	15	Part – II: INVITATION FOR BIDS AND INSTRUCTIONS TO BIDDERS	15. Acceptance of Terms: A Recipient will, by responding to Bank RFP, be deemed to have accepted the terms as stated in the RFP.	We request that the bidder be permitted to submit deviations to the bid. We submit that the contract to be signed between the Bank and the bidder should be a mutually acceptable agreement, incorporating the terms of bidder's proposal.	Clause stands as per RFP.
28	18	Part – II: INVITATION FOR BIDS AND INSTRUCTIONS TO BIDDERS	23. Submission of offer – Three Bid System Note vi. The Bank reserves the right to modify any terms, conditions or specifications for submission of bids and to obtain revised Bids from the bidders due to such changes, if any, at any time prior to completion of evaluation of technical / eligibility bids from the participating bidders.	Please confirm that this right is limited only till the last date of submission of the proposal. If the terms are revised after the submission, we request that the bidder be given the right to revise its technical and commercial proposal to the extent to accommodate the changes / revisions made by the Bank in its requirements.	Clause stands as per RFP.
29	22	Part IV: Section – I	2. Scope of Work	Bidder requests that the scope of work should be mutually discussed and agreed to between the parties.	Clause stands as per RFP.
30	27	Part IV: Section – I	5. Acceptance Test: Power on Self-Test (POST) will be conducted by Bidder at the site in presence of UCO Bank officials and /or nominated person. Installation report (IR) should be submitted a complete implementation of systems. UCO Bank will take over the system on successful completion of above acceptance test.	We suggest that the acceptance test and associated criteria for each milestone should be mutually decided. Once the installation cum acceptance test is carried out as per the acceptance criteria, the acceptance test shall be complete.	Clause stands as per RFP.
31	42	PART-V	3. Delivery and Installation: Point no. 3.4: All the equipment supplied by the Bidder shall be legal and Bidder shall give indemnity to that effect.D40	Indemnity should be restricted to third party claims for infringement of intellectual property rights only. Accordingly, we request that this clause should be deleted.	Clause stands as per RFP.
32	44	PART-V	7. Service Level Agreement: Point no. 7.6: The purchaser may without	The Bidder requests that a minimum cure period of 30 days should be	Clause stands as per RFP.

			<p>prejudice to its right to effect recovery by any other method, deduct the amount of penalty from any money belonging to the bidder in its hands (which includes the purchaser's right to claim such amount against bidder's Bank Guarantee) or which may become due to the Bidder. Any such recovery of penalty shall not in any way relieve the Bidder from any of its obligations to complete the works/services or from any other obligations and liabilities under the Contract.</p>	<p>provided prior to invoking any SLAs. Further invoking of PBG should be restricted to material breach of terms and conditions of this Agreement.</p>	
33	46	PART-V	<p>10. Warranty:</p> <p>Point no. 10.1 The Bidder further represents and warrants that all licenses delivered / rendered under and in accordance with contract shall have no defect, arising from design or from any act, error/defect or omission of the Bidder.</p> <p>Point no. 10.2 The warranty period will be 36 months from date of successful deployment of APT at the respective location/s and 3 years of Support and warranty period</p>	<ul style="list-style-type: none"> • Bidder submits that warranties related to any third party software and hardware will be as per the warranty terms of the original OEM. Any exclusion to such warranty will be applicable to the Bank and if any work is done by the Bidder for services which are excluded from warranty, they will be additionally charged to the Bank. <p>Bidder will rectify any defects free of costs, provided the defects are not due to reasons attributable to the Bank, e.g., if the system is not used in a manner and for purpose as agreed the agreement, it is combined with other system, if there are any unauthorized modifications, if there is any productive use of the system before the go-live period.</p> <p>Bidder submits that Bidder cannot reasonably foresee the regulatory changes that may be required by the govt. and the estimated effort of such requirements. Any such requirements</p>	<p>Clause stands as per RFP.</p>

				<p>will be carried out by the Bidder as part of Change Requests and will be additionally charged as mutually agreed between the parties. Kindly make this change.</p> <p>Enhancements and customization cannot be part of the warranty or AMC. Any enhancements requested by the Customer will be taken up as Change Requests and will be additionally charged.</p> <ul style="list-style-type: none"> • Requesting you to add 4weeks extra in warranty period, which also proposed as implementation timeline. 	
34	47	PART-V	<p>12. Contract Period:</p> <p>The tenure of the Contract will be for a period of 3 (three) years with warranty effective from the date of execution of the Service Level Agreement (SLA) unless <u>terminated earlier by the Bank by serving 90 days prior notice in writing to the selected bidder at its own convenience without assigning any reason and without any cost or compensation therefor.</u> However, after the completion of initial period of 3 (three) years with warranty, the contract may be extended/renewed for further period on such terms and conditions as would be decided by the Bank.</p> <p>The performance of the selected bidder shall be reviewed every quarter and the Bank <u>reserves the right to terminate the contract at its sole discretion by giving 90 days 'notice without assigning any reasons and without any cost or</u></p>	<p>Bidder submits that the tenure of Contract shall be effective from the date of execution of the mutually agreed Contract between the Bidder and the Bank.</p> <p><u>Underlined Portion:</u> Also, the Contract shall be terminated only for <u>serious and material breaches</u> and not for minor breaches/delays or for convenience. We further request that the bidder should be allowed a cure period of a minimum of 30 days prior to issuance of notice of default for termination of the contract.</p> <p>Any further renewal of the contract shall be on such terms and conditions as mutually decided between the Bank and the Bidder.</p>	Clause stands as per RFP.

			compensation therefor. Any offer falling short of the contract validity period is liable for rejection.		
35	48	PART-V	<p>14. Acceptance Tests:</p> <p>The Bank will carry out the acceptance tests as per Scope of work Part IV supplied & implemented by the selected bidder as a part of the Project. The Vendor shall assist the Bank in all acceptance tests to be carried out by the Bank. The provisioned items will be deemed accepted only on successful acceptance of those products and the vendor would need to provision insurance of those items till successful acceptance. The Bank at its discretion may modify, add or amend the acceptance tests which then will have to be included by the vendor. The Vendor shall arrange for the tests at the relevant sites in the presence of the officials of the Bank. The Vendor should ensure that the tests will involve trouble-free operation of the complete system apart from physical verification and testing and that there shall not be any additional charges payable by the Bank for carrying out this acceptance test.</p>	<p>We suggest that the acceptance test and associated criteria for each milestone should be mutually decided. Once the installation cum acceptance test is carried out as per the acceptance criteria, the acceptance test shall be complete.</p>	<p>Clause stands as per RFP.</p>
36	48-49	PART-V	<p>15. Order Cancellation:</p> <p>The Bank reserve its right to cancel the order in the event of one or more of the following situations, that are not occasioned due to reasons solely and directly attributable to the Bank alone:</p> <ul style="list-style-type: none"> • Delay in commissioning / implementation / testing beyond the specified period. • Serious discrepancy in the quality of service expected during the 	<ul style="list-style-type: none"> • Bidder requests that the right to cancel / terminate the contract / order be available only in case of material breach by the Bidder. Bank may terminate the Contract, provided the Customer has given a cure period of 30 days, and the Bidder has not rectified the breach within the cure period. Accordingly, we request that the reasons for cancellation of order as specified in 	<p>Clause stands as per RFP.</p>

			<p>implementation, rollout and subsequent maintenance process.</p> <ul style="list-style-type: none"> • In case of cancellation of order, any payments made by the Bank to the Vendor would necessarily have to be returned to the Bank, further the Vendor would also be required to compensate the Bank for any direct loss suffered by the Bank due to the cancellation of the contract/purchase order and any additional expenditure to be incurred by the Bank to appoint any other Vendor. This is after repaying the original amount paid. • Vendor should be liable under this section if the contract/ purchase order has been cancelled in case sum total of penalties and deliveries equal to exceed 10% of the TCO. 	<p>Clause 15 should be deleted and restricted to material breach only.</p> <p>We request that any compensation to be paid by the vendor to the Bank would be established post a reasonable due – diligence of the re-procurement cost to be incurred and shall not exceed @ 5% of the value of the undelivered services which the Bank re-procures from third party.</p> <ul style="list-style-type: none"> • Termination should be only for material breach of the contract. Bidder should not be asked to compensate as bidder is already paying agreed liquidated damages. Kindly amend the clause accordingly. 	
37	49	PART-V	<p>16. indemnity:</p> <p>The selected Bidder agrees to indemnify and keep indemnified the Bank against all losses, damages, costs, charges and expenses incurred or suffered by the Bank due to or on account of any claim for infringement of intellectual property rights.</p> <p><u>The selected Bidder agrees to indemnify and keep indemnified the Bank against all losses, damages, costs, charges and expenses incurred or suffered by the Bank due to or on account of any breach of the terms and conditions contained in this RFP or Service Level Agreement to be executed.</u></p> <p><u>The selected Bidder agrees to indemnify and keep indemnified Bank at all times</u></p>	<p>Bidder agrees provided that such third party claims are for infringement of their intellectual property rights arising out of use of the software provided by the Bidder only and, provided and to the extent such infringement does not result from any act or omission of Customer or third parties authorized by Customer. Rest of the losses and damages due to third party claims are covered and claimable under the contractual remedies for breach of contract by Bidder. Kindly make this amendment.</p> <p>Customer would promptly notify Bidder when it is informed of any claims against it. Bidder will be entitled to sole right of defense and for settling such claims.</p>	Clause stands as per RFP.

			<p><u>against all claims, demands, actions, costs, expenses (including legal expenses), loss of reputation and suits which may arise or be brought against the Bank, by third parties on account of negligence or failure to fulfill obligations by the selected bidder or its employees/personnel.</u></p> <p><u>All indemnities shall survive notwithstanding expiry or termination of Service Level Agreement and the Vendor shall continue to be liable under the indemnities.</u></p> <p><u>Selected Bidder is required to furnish a separate Letter of Indemnity (Format whereof to be supplied by the Bank) in Bank's favor in this respect before or at the time of execution of the Service Level Agreement.</u></p>	<p>Indemnification is the sole and exclusive right and remedy of indemnified party for the losses arising out of IPR infringement.</p> <p>Indemnities are provided for direct damages only and must be mutual in nature.</p> <p><u>Underlined Portion:</u> Bidder submits that Indemnification obligation be limited to third party claims for IPR infringement only. Customer has other remedies available under the contract to recover all losses and damages due to defaults, delays and breaches caused by Bidder and its subcontractors'. Bidder requests that this requirement be deleted.</p> <p>We request that indemnity be restricted to a contractual obligation (covered in the contract to be signed between the Bank and the Bidder) and there should be no requirement to submit an additional letter of indemnity.</p>	
38	50	PART-V	<p>20. Guarantee:</p> <p>Selected bidder should guarantee that all the material as deemed suitable for the delivery and management of the Implementation of Advanced Persistent Threat (APT) device. All hardware and software must be supplied with their original and complete printed documentation.</p>	<p>Bidder submits that guarantees related to any third party software and hardware will be as per the terms of the EULA to be signed between the Bank and the Third Party OEM.</p>	<p>Clause stands as per RFP.</p>
39	51	PART-V	<p>22. Exit Option and Contract Re-negotiation:</p> <p>The Bank reserves the right to cancel the</p>	<p>Bidder requests that the right to cancel/terminate the contract/order be available only in case of <u>material</u></p>	<p>Clause stands as per RFP.</p>

		<p>contract in the event of happening one or more of the following Conditions:</p> <ul style="list-style-type: none"> • Failure of the Selected bidder to accept the contract / purchase order and furnish the Performance Guarantee within 30 days of receipt of purchase contract; • Delay in offering; • Delay in commissioning project beyond the specified period; • Delay in completing commissioning / implementation and acceptance tests / checks beyond the specified periods; • Serious discrepancy in project noticed during the testing; • Serious discrepancy in functionality to be provided or the performance levels agreed upon, which have an impact on the functioning of the Bank. • Serious discrepancy in completion of project. • Serious discrepancy in maintenance of project. • In addition to the cancellation of purchase contract, Bank reserves the right to appropriate the damages through encashment of Bid Security / Performance Guarantee given by the Selected Bidder. <p><u>The Bank will reserve a right to re-negotiate the price and terms of the entire contract with the Selected Bidder at more favorable terms in case such terms are offered in the industry at that time for projects of similar and comparable size, scope and quality.</u></p> <p>The Bank shall have the option of</p>	<p>breach by the Bidder. Bank may terminate the Contract, provided the Customer has given a cure period of 30 days, and the Bidder has not rectified the breach within the cure period.</p> <p>Accordingly, we request that the reasons for cancellation of contract as specified in Clause 22 should be deleted and shall be restricted to material breach only.</p> <p>We request that the Performance Bank Guarantee shall be invoked for material breach only.</p> <p>Kindly clarify option will be exercised only before the award of the Contract. Bidder has to enter into a contract with the hardware manufacturer, incase Bank opts to procure hardware from the Bidder. Bidder cannot cancel this contract with the manufacturer once it has entered into the subcontract with the OEM.</p>	
--	--	--	---	--

			<p>purchasing the equipment from third-party suppliers, in case such equipment is available at a lower price and the Selected Bidder's offer does not match such lower price. Notwithstanding the foregoing, the Selected Bidder shall continue to have the same obligations as contained in this scope document in relation to such equipment procured from third-party suppliers.</p>		
40	53	PART-V	<p>24. Termination: UCO BANK reserves the right to cancel the work/purchase order or terminate the SLA by giving 90 (ninety) days' prior notice in writing and <u>recover damages, costs and expenses etc.</u>, incurred by Bank under the following circumstances:-</p> <p>a) The selected bidder commits a breach of any of the terms and conditions of this RFP or the SLA to be executed between the Bank and the selected Bidder.</p> <p>b) The selected bidder goes into liquidation, voluntarily or otherwise.</p> <p>c) The selected bidder violates the Laws, Rules, Regulations, Bye-Laws, Guidelines, and Notifications etc.</p> <p>d) An attachment is levied or continues to be levied for a period of seven days upon effects of the bid.</p> <p>e) The selected bidder fails to complete the assignment as per the time lines prescribed in the Work Order/SLA and the extension, if any allowed.</p> <p>f) Deductions on account of liquidated damages exceed more than 10% of the total work order.</p> <p>g) In case the selected bidder fails to deliver the resources as stipulated in the</p>	<p>Bidder requests that the right to cancel/terminate the contract/order be available only in case of material breach by the Bidder. Bank may terminate the Contract, provided the Customer has given a cure period of 30 days, and the Bidder has not rectified the breach within the cure period. Accordingly, we request that sub-clauses (a) to (h) should be deleted.</p> <p><u>Underlined Portion:</u> We request that any compensation to be paid by the vendor to the Bank would be established post a reasonable due – diligence of the re-procurement cost to be incurred and shall not exceed @ 5% of the value of the undelivered services which the Bank re-procures from third party.</p> <p>We further request that the performance bank guarantee shall be invoked for material breaches only.</p> <p>Bidder seeks a right to terminate the contract for material breach (including failure to fulfill payment obligations) by</p>	<p>Clause stands as per RFP.</p>

			<p>delivery schedule, UCO BANK reserves the right to procure the same or similar resources from alternate sources at the risk, cost and responsibility of the selected bidder.</p> <p>h) After award of the contract, if the selected bidder does not perform satisfactorily or delays execution of the contract, UCO BANK reserves the right to get the balance contract executed by another party of its choice by giving one month's notice for the same. <u>In this event, the selected bidder is bound to make good the additional expenditure, which UCO BANK may have to incur in executing the balance contract. This clause is applicable, if the contract is cancelled for any reason, whatsoever.</u></p> <p>i) UCO BANK reserves the right to recover any dues payable by the selected Bidder from any amount outstanding to the credit of the selected bidder, including the adjustment of pending bills and/or invoking the Performance Bank Guarantee under this contract.</p> <p>The rights of the Bank enumerated above are in addition to the rights/remedies available to the Bank under the Law(s) for the time being in force.</p>	<p>the Customer, in the event the Customer does not cure the material breach in 30 days of receipt of notice of breach from the bidder. Kindly include this provision in the Contract.</p>	
41	54	PART-V	<p>26. Effects of Termination:</p> <p>In the event of termination of the Contract due to any reason, whatsoever, [whether consequent to the expiry of stipulated term of the Contract or otherwise], <u>UCO BANK shall be entitled to impose any such obligations and conditions and issue any clarifications as</u></p>	<p>Bidder agrees provided:</p> <ol style="list-style-type: none"> 1. Scope of the exit assistance activities will be pre-determined by the parties upon mutual agreement under an exit plan. 2. Bidder will charge an additional exit assistance charges for providing exit assistance services. 	<p>Clause stands as per RFP.</p>

			<p><u>may be necessary to ensure an efficient transition and effective business continuity of the Service(s) which the Vendor shall be obliged to comply with and take all steps to minimize loss resulting from the termination / breach, and further allow the next successor Vendor to take over the obligations of the erstwhile Vendor in relation to the execution/continued execution of the scope of the Contract.</u></p> <p>In the event that the termination of the Contract is due to the expiry of the term of the Contract and the Contract is not further extended by UCO BANK, the Vendor herein shall be obliged to provide all such assistance to the next successor Bidder or any other person as may be required and as UCO BANK may specify including training, where the successor(s) is a representative/personnel of UCO BANK to enable the successor to adequately provide the Service(s) hereunder, even where such assistance is required to be rendered for a reasonable period that may extend beyond the term/earlier termination hereof.</p> <p>Nothing herein shall restrict the right of UCO BANK to invoke the Performance Bank Guarantee and other guarantees, securities furnished, enforce the Letter of Indemnity and pursue such other rights and/or remedies that may be available to UCO BANK under law or otherwise.</p>		
42	55	PART-V	<p>29. Limitation of Liability: Bidder's aggregate liability under the contract shall be limited to a maximum of</p>	<ul style="list-style-type: none"> • Bidder requests that the total cumulative liability of the Bidder be limited to the amount paid and 	Clause stands as per RFP.

		<p>the contract value. This limit shall not apply to third party claims for</p> <p>a. IP Infringement indemnity.</p> <p>b. Bodily injury (including Death) and damage to real property and tangible property caused by Bidder/s' gross negligence. For the purpose of this section, contract value at any given point of time, means the aggregate value of the purchase orders placed by Bank on the Bidder that gave rise to claim, under this RFP.</p> <p><u>c. Bidder shall be liable for any indirect, consequential, incidental or special damages under the agreement/purchase order.</u></p>	<p>payable by Customer in the last 12 months, before the event that gave rise to the liability occurs.</p> <p><u>Underlined Portion:</u></p> <p>Notwithstanding anything to the contrary contained anywhere in the tender document, no party will be liable for any indirect, incidental and consequential damages, including loss of business, revenue, goodwill or profits, even if the party has been advised of the possibility of such damages.</p> <ul style="list-style-type: none"> • To make the contract feasible for business we request Liability should be limited up to the extent mentioned below: Neither party shall, in any event, regardless of the form of claim, be liable for any indirect, special, punitive, exemplary, speculative or consequential loss or damages. Subject to the above and to the extent allowed by local laws, the maximum aggregate liability of each party under this proposal/Contract/PO for any claim or series of claims regardless of the form of claim, damage and legal theory shall not exceed the annual value of the Contract. • We propose the following clause to replace the current clause "NOTWITHSTANDING ANY OTHER PROVISION HEREOF, NEITHER PARTY SHALL BE LIABLE FOR (A) ANY 	
--	--	--	--	--

				<p>INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES OR (B) ANY DAMAGES FOR LOST PROFITS, LOST REVENUES, LOSS OF GOODWILL, LOSS OF ANTICIPATED SAVINGS, LOSS OF CUSTOMERS, LOSS OF DATA, INTERFERENCE WITH BUSINESS OR COST OF PURCHASING REPLACEMENT SERVICES, ARISING OUT OF THE PERFORMANCE OR FAILURE TO PERFORM UNDER THIS AGREEMENT, WHETHER OR NOT CAUSED BY THE ACTS OR OMISSIONS OR NEGLIGENCE (INCLUDING GROSS NEGLIGENCE OR WILLFUL MISCONDUCT) OF ITS EMPLOYEES OR AGENTS, AND REGARDLESS OF WHETHER SUCH PARTY HAS BEEN INFORMED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES. IN NO EVENT BIDDER SHALL BE LIABLE IN AN AMOUNT THAT EXCEEDS, IN THE AGGREGATE FOR ALL SUCH LIABILITIES, THE MOST RECENT TWELVE (12) MONTHS OF CHARGES COLLECTED BY BIDDER FROM THE BANK PURSUANT TO THE APPLICABLE PURCHASE ORDER GIVING RISE TO THE LIABILITY. "</p>	
43	56	Annexure – A Tender Offer Forwarding letter	<p>We agree to abide by the terms and conditions of this tender and our offer shall remain valid 180 days from the date of commercial bid opening and our offer shall remain binding upon us which may be accepted by The Bank any time before expiry of 180 days.</p>	<p>Bidder requests that certain deviations to the Contract terms be permitted and the Contract to be signed between Customer and Bidder should be a mutually acceptable agreement. Bidder submits that the response to RFP shall be deemed acceptance of the RFP terms except for such specific sections against which deviations are</p>	<p>Clause stands as per RFP.</p>

				proposed by Bidder. Kindly confirm acceptance of this intent. Accordingly, we request that this sub-clause should be deleted from the Annexure.	
44	61	Annexure – D Format of Bank Guarantee (EMD)	<p>The Bid security for which this guarantee is given is liable to be enforced/ invoked:</p> <ol style="list-style-type: none"> 1. If the Bidder withdraws his proposal during the period of the proposal validity; or 2. If the Bidder, having been notified of the acceptance of its proposal by the Bank during the period of the validity of the proposal fails or refuses to enter into the contract in accordance with the Terms and Conditions of the RFP or the terms and conditions mutually agreed subsequently. 	Bidder requests that certain deviations to the Contract terms be permitted and the Contract to be signed between Customer and Bidder should be a mutually acceptable agreement. Bidder submits that the response to RFP shall be deemed acceptance of the RFP terms except for such specific sections against which deviations are proposed by Bidder. Kindly confirm acceptance of this intent.	Clause stands as per RFP.
45	65	Annexure – F Masked Commercial Format	<p>We have not added or modified any clauses / statements / recordings / declarations in the commercial offer, which is conditional and / or qualified or subjected to suggestions, which contain any deviation in terms & conditions or any specification.</p> <ul style="list-style-type: none"> • We have understood that in case of non-adherence to any of the above, our offer will be summarily rejected. • Please note that any commercial offer which is conditional and / or qualified or subjected to suggestions will also be summarily rejected. This offer shall not contain any deviation in terms & condition or any specifications, if so such offer will be summarily rejected. 	Bidder requests that certain deviations to the Contract terms be permitted and the Contract to be signed between Customer and Bidder should be a mutually acceptable agreement. Bidder submits that the response to RFP shall be deemed acceptance of the RFP terms except for such specific sections against which deviations are proposed by Bidder. Kindly confirm acceptance of this intent. Accordingly, we request that this sub-clause should be deleted from the Annexure.	Clause stands as per RFP.
46	68	Annexure – H DECLARATION- CUM- UNDERTAKING	We do also hereby irrevocably and unconditionally agree and undertake to save and keep the Bank, including its respective directors, officers, and	We request that indemnity obligations of the Bidder shall be restricted to providing indemnity for third party claims arising due to infringement of	Clause stands as per RFP.

			employees and keep them harmless from and against any claim, demand, losses, liabilities or expenses of any nature and kind whatsoever and any damage caused from and against all suits and other actions that may be instituted taken or preferred against the Bank by whomsoever and all losses, damages, costs, charges and expenses arising out of non-compliance with or non-adherence to any statutory/regulatory requirements and/or any other law for the time being in force.	Intellectual Property Rights. Accordingly, we request that this sub-clause should be deleted.	
47	70	Annexure – J PROFORMA FOR PERFORMANCE GUARANTEE	We, [indicate the name of the bank ISSUING THE BANK GUARANTEE] (Hereinafter referred to as "Bank") at the request of [VENDOR] do hereby undertake to pay to Purchaser an amount not exceeding Rs. against any loss or damage caused to or suffered or would be caused to or suffered by Purchaser by reason of any breach by the said VENDOR of any of the terms or conditions contained in the said Agreement.	We request that the PBG shall be invoked for material breaches only. A minimum cure period of 30 days should be permitted prior to invoking of the PBG.	Clause stands as per RFP.
48	77	Annexure – K Pre- Contract Integrity Pact	7. Fall Clause: Point no. 7.1 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 PS U 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 at a lower	<ul style="list-style-type: none"> • We request that the fall clause should be deleted. • It is not practical to implement therefore, please take out this clause from the RFP 	Clause stands as per RFP.

			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.		
49	79	Annexure – L Undertaking Letter to the Bank on the vendor's letterhead	We hereby agree to comply with all the terms and conditions / stipulations as contained in the RFP and the related addendums and other documents including the changes made to the original tender documents if any, issued by the Bank. The Bank is not bound by any other extraneous matters or deviations, even if mentioned by us elsewhere either in our proposal or any subsequent deviations sought by us, whether orally or in writing, and the Bank's decision not to accept any such extraneous conditions and deviations will be final and binding on us.	Bidder requests that certain deviations to the Contract terms be permitted and the Contract to be signed between Customer and Bidder should be a mutually acceptable agreement. Bidder submits that the response to RFP shall be deemed acceptance of the RFP terms except for such specific sections against which deviations are proposed by Bidder. Kindly confirm acceptance of this intent. Accordingly, we request that this sub-clause should be deleted from the Annexure.	Clause stands as per RFP.
50	80	Annexure – M Undertaking for Non-Blacklisting / Non-Debarment of the bidder	Further, we hereby undertake and agree to abide by all terms and conditions and guidelines stipulated by the Bank. We understand that any deviation may result in disqualification of our bid.	Bidder requests that certain deviations to the Contract terms be permitted and the Contract to be signed between Customer and Bidder should be a mutually acceptable agreement. Bidder submits that the response to RFP shall be deemed acceptance of the RFP terms except for such specific sections against which deviations are proposed by Bidder. Kindly confirm acceptance of this intent. Accordingly, we request that this sub-clause should be deleted from the Annexure.	Clause stands as per RFP.
51	84	Annexure – P NON-DISCLOSURE AGREEMENT	1. Confidential Information: "Confidential Information" shall mean and include any information which relates to the financial and/or business	Please clarify that the definition of Confidential Information does not include sensitive personal data of individuals.	Clause stands as per RFP.

			<p>operations of each Party, including but not limited to, specifications, drawings, sketches, models, samples, reports, forecasts, current or historical data, computer programs or documentation and all other technical, financial or business data, <u>information related to each Party's customers</u>, products, processes, financial condition, employees, intellectual property, manufacturing techniques, experimental work, trade secrets.</p> <p>The Receiving Party shall indemnify the Bank and hold the Bank harmless against any loss caused to it as a result of the non-performance or improper performance of this Agreement by the Receiving Party, or its servants or agents to perform any aspect of its obligations forming part of the subject matter of this Agreement.</p>	<p>Indemnity obligation under this agreement shall be limited to the liability cap as specified in the contract between the Bank and the Bidder.</p>	
52		General		<p>IPR Clause:</p> <p>We suggest inclusion of IPR clause with following points. Note that verbiage would be drafted during contract negotiation.</p> <ol style="list-style-type: none"> 1. Any existing IP and its modifications will remain with the party that it belongs to. 2. Any deliverables and intellectual property developed or created by DXC during the performance of the contract will vest in DXC except created exclusively for OBC and agreed between the parties. 3. Ownership and IPR in any processes, methodologies or techniques, improvements developed by DXC 	Not accepted.

				<p>before or during the provision of the services will remain with DXC.</p> <p>4. OBC shall use the products in accordance with the license terms and restrictions specified by the OEM to be applicable for the use of such products.</p> <p>5. Hardware warranty if any will be passed on as provided by the OEM and software license will be subject to licensing terms issued by the licensor.</p>	
53			No Deviation Template Provided	<p>We request the bank to kindly allow bidders to provide alternate clauses/Suggestions or Deviations to the RFP Clauses as it will be difficult to comply to all terms as is:</p> <p>Request you to kindly provide us an opportunity to submit the same. Kindly share with us a template or annexure for the same.</p>	Not accepted.
54	23	PART – IV SECTION – 1	<p>Scope of Work:</p> <p>2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following:</p> <p>Point no. xxiv:</p> <p>Licenses should be considered based on registered asset to console at any given point of time if applicable.</p>	<p>Should have more option for licensing.</p> <p>Licenses should be considered based on registered asset to console or volume of traffic handled OR number of file processed at any given point of time if applicable.</p>	Clause stands as per RFP.
55	28	PART – IV SECTION – 2 1. TECHNICAL REQUIREMENTS	<p>Point no. 5:</p> <p>Solution should be able to detect the persistent threats which come through executable files, PDF files, Flash files, RTF files, any type of file.</p>	<p>All type of files should not be supported in all sandboxes.</p> <p>Solution should be able to detect the persistent threats which come through executable files, PDF files, Flash files, RTF files, any type of office files.</p>	Clause stands as per RFP.
56	34	PART – IV SECTION – 2 2. TECHNICAL SPECIFICATIONS	<p>Point no. 30: DGA/Domain Flux identification</p> <p>A solution should identify Domain Generation Algorithm (DGA)-based crime ware.</p>	<p>Mainly the DGA job is for IPS & perimeter NGFW.</p> <p>So make it optional or remove the point.</p>	Clause stands as per RFP.

57	35	PART – IV SECTION – 2 2. TECHNICAL SPECIFICATIONS	<p>Point no. 44: Battle-Simulation</p> <p>A solution should perform dynamic analysis of files outside of an organization's network, in a –space where malware files cannot evade detection. Specifically, malware files should be processed in a dedicated –dirty spacell, with full Internet access that allows bare metal analysis of the malware, to counter VM and Internet aware malware as well as implement other controls (such as time dilation, key stroke counts, varying software configuration, etc.).</p>	<ul style="list-style-type: none"> • Language clarity required. A solution should perform dynamic analysis of files securely inside of an organization's network, in a –space where malware files cannot evade detection. Specifically, malware files should be processed in a dedicated –dirty spacell, with full Internet access that allows bare metal analysis of the malware, to counter VM and Internet aware malware as well as implement other controls (such as time dilation, key stroke counts, varying software configuration, etc.) • A solution should perform dynamic analysis of files securely inside of an organization's network, in a –space where malware files cannot evade detection. Specifically, malware files should be processed in a dedicated – dirty spacell, with full Internet access that allows bare metal analysis of the malware, to counter VM and Internet aware malware as well as implement other controls (such as time dilation, key stroke counts, varying software configuration, etc.) 	Clause stands as per RFP.
58	31 & 39	PART – IV SECTION – 2 2. TECHNICAL SPECIFICATIONS	<p>Point no. 75: DNS Redirects</p> <p>A solution should be able to perform DNS redirection for malicious DNS queries, to prohibit infections from communicating with cyber criminals.</p> <p>Point no. 3</p> <p>Implementation and configuration:</p> <p>A solution must possess an architecture that should works in offline Mode/SPAN/</p>	<ul style="list-style-type: none"> • The point needs to be changed. If the solution sits in SPAN mode then it cannot perform the DNS re-direction. A solution should be able to identify malicious DNS queries, to prohibit infections from communicating with cyber criminals. • Please clarify why email monitoring 	It should be deployed in line but should have the capability to be deployed in SPAN/TAP mode.

			Mirror Traffic	should not be in MTA mode. Also, the solution should be deployed preferably in Inline blocking mode rather than having capability to be deployed in SPAN/TAP mode	
59	9 & 58	Annexure – B Eligibility Criteria Compliance	<p>Point no. 5: The bidder should provide the list of clients for APT solution Implemented during last five years up-to 30.06.2018.</p> <p>Documents to be submitted: Relevant PO / client satisfactory letter regarding successful implementation of APT solution is to be submitted.</p>	<ul style="list-style-type: none"> • Relevant PO or declaration letter mentioning APT is under implementation till submission date of tender. • Clause is not quantifying the no of customer (We request you to pls put bidder to submit 5 customer references either PO or Sign Off) and since the solution required to be implemented at Network/Web We request you to pls change "APT Solution" to Network/Web/Email APT. 	Clause stands as per RFP.
60	22 & 23	PART – IV SECTION – 1	<p>Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. xv The proposed solution should support to monitor traffic from multiple Segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single appliance.</p> <p>Point no. vi Solution shall support unlimited endpoints on a single APT Appliance or multiple or under HA mode or stand-by mode.</p>	<ul style="list-style-type: none"> • Kindly clarify whether the DMZ, Server Farm and MPLS zone to be monitored with the same appliance or it needs separate appliances in order to maintain the physical segregation of the security zones. • Appliance sizing - Kindly clarify whether the DMZ, Server Farm and MPLS zone to be monitored with the same appliance or it needs separate appliances in order to maintain the physical segregation of the security zones. <p>Requesting Bank to clarify if they need the solution in Active Passive HA or in Standalone mode. This will help to create a bench mark for all bidders. Also in "Technical Bill of</p>	<p>The 2 APT Appliance should be able to monitor at least 16 physical (both ingress and outgress) segments at DR side.</p> <p>i.e. per APT should have 8 numbers of physical segments.</p>

				<p>Material" section it is mentioned as Quantity 2.</p> <ul style="list-style-type: none"> • Please confirm the cumulative throughput requirements for all segments. Also, share total no of segments and port requirements. • Kindly mention how many physical segments to be monitored? 	
61			General	<p>Kindly clarify whether the APT solution is to be sized to handle more than 10,000 users.</p>	Clause stands as per RFP.
62			General	<ul style="list-style-type: none"> • Please provide us the following: A) What are the available Operating System for the hosts? • Please provide us the following: A) Firewall- Make, Model and Qty B) IPS- Make, Model and Qty C) Details of equipment which will be integrated with APT D) How many hosts will be connected to the APT? E) Details of solution like Web Proxy, AV, Event Logging, SIEM, SNMP etc. with which APT integration will be done. 	<ul style="list-style-type: none"> • Please refer to Sl.no. 8 of the pre-bid responses. • Successful bidder will be provided with the other details.
63	22	PART – IV SECTION – 1	<p>Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. ii Vendor's expert team will be onsite till complete installation, implementation and project sign-off.</p>	<p>Vendor's expert team OR Vendor's authorized expert team will be onsite till complete installation, implementation and project sign-off.</p>	<p>The modified clause to be read as under: PART – IV: SECTION – 1 Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. ii Vendor's expert team OR Vendor's authorized expert team will be</p>

					onsite till complete installation, implementation and project sign-off.
64	23	PART – IV SECTION – 1	Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. xiii Solution shall support role-based administration such as Administrator, Malware Analyst, Database Reader, and Read-only access users.	Multiple user account with different roles should be supported.	Clause is Self-Explanatory.
65	23	PART – IV SECTION – 1	2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. xiv Licenses should be considered based on registered asset to console at any given point of time if applicable.	Licenses should be considered based on registered asset to console or volume of traffic handled OR number of file processed at any given point of time if applicable.	Clause stands as per RFP.
66	28	PART – IV SECTION – 2 1. TECHNICAL REQUIREMENTS	Clause no. 5 Solution should be able to detect the persistent threats which come through executable files, PDF files, Flash files, RTF files, any type of file	<ul style="list-style-type: none"> • Solution should be able to detect the persistent threats which come through executable files, PDF files, Flash files, RTF files, any type of office files. • Please specify that detection of threats should be available for more than 30+ file types. 	Clause stands as per RFP.
67	30	PART – IV SECTION – 2 1. TECHNICAL REQUIREMENTS	Clause no. 39 Sandboxing File type supports (.doc, .xls, .ppt, .pdf, .exe, .zip, .rar, .tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj, .exe, .dll, .avi, .mpeg, .mp3/4, .jpg, java script, JavaArchive JAR, LNK, .chm, .swf, .sys, .com, .hwp, etc.)	Sandboxing File type supports (.doc, .xls, .ppt, .pdf, .cab, .rar, .arj, .exe, .dll, .avi, .mpeg, .mp3/4, .jpg, java script, JavaArchive JAR, LNK, .chm, .swf, .sys, .com, .hwp, etc.)	Clause stands as per RFP.
68	31	PART – IV SECTION – 2 2. TECHNICAL SPECIFICATIONS	Point no. 9: Hardware redundancy: A solution must have RAID redundancy (for hard drives), network redundancy (for management network interfaces), Power-Supply redundancy.	<ul style="list-style-type: none"> • A solution must have RAID redundancy (for hard drives), network redundancy, Power-Supply redundancy • Management network redundancy 	Clause stands as per RFP.

				won't work in most of the solutions - A solution must have RAID redundancy (for hard drives), network redundancy , Power-Supply redundancy	
69	39	PART – IV SECTION – 2 2. TECHNICAL SPECIFICATIONS	<p>Point no. 75: DNS Redirects: A solution should be able to perform DNS redirection for malicious DNS queries, to prohibit infections from communicating with cyber criminals.</p>	<ul style="list-style-type: none"> • A solution should be able to identify malicious DNS queries, to prohibit infections from communicating with cyber criminals. • The point needs to be changed. If the solution sits in SPAN mode then it cannot perform the DNS re-direction - A solution should be able to identify malicious DNS queries, to prohibit infections from communicating with cyber criminals. 	Clause stands as per RFP.
70	40	PART – IV SECTION – 2 2. TECHNICAL SPECIFICATIONS	<p>Point no. 80: Web Proxy Integration: Automated and Direct Integration with web proxy where web access policies can be implemented based on device state (suspected or infected) information discovered by the solution. (IE: Block) infected assets from communicating to internet and/or high-value assets)</p> <p>Point no. 81: Web Proxy Integration: Automated and Direct Integration with web proxy where ewb access policies can be implemented which blocks active C&C communication attempts identified by the solution</p>	<p>Requested to be modified: Automated and Direct Integration with web proxy.</p>	Clause stands as per RFP.
71	43	PART – V	<p>4. Payment Terms 4.1 80% of the order value along with GST and other applicable duties on actual basis will be paid on delivery, installation and acceptance of ordered items, after realizing penalty charges for late delivery and / or late installation, if any. The claim</p>	80% of the order value along with GST and other applicable duties on actual basis will be paid on delivery, after realizing penalty charges for late delivery, if any. The claim for payment should contain proof of delivery, Report signed by an authorized official of the	Clause stands as per RFP.

			for payment should contain proof of delivery, installation report & User Acceptance Report signed by an authorized official of the bank / branch at the respective sites etc.	bank / branch at the respective sites etc.	
72	9 & 59	PART – I 3. Eligibility Criteria & Annexure – B Eligibility Criteria Compliance	<p>Point no. 8: The Bidder should have all necessary licenses, permissions, consents, no objections, approvals as required under law for carrying out its business as on date of submission of the tender.</p> <p>Documents to be submitted: Copy of the Relevant product license / documents to be submitted.</p>	<ul style="list-style-type: none"> Request you to please clarify the requirement 	Clause is Self-Explanatory.
73	22 & 26	PART – IV SECTION – 1	<p>2. Scope of Work 2.2 Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. ii Vendor's expert team will be onsite till complete installation, implementation and project sign-off.</p> <p>2.6. System Maintenance & Support Services: Direct OEM Service and support should be covered under with dedicated TAM (Technical Account Manager) and onsite support.</p>	<ul style="list-style-type: none"> Team will be available onsite as and when required based on the project plan. To comply the same you need to be quote Professional services cost wise it will be too high. - Vendor's expert team OR Vendor's authorized expert team will be onsite till complete installation, implementation and project sign-off. Kindly clarify if the installation needs to be performed by OEM certified authorized engineer to follow the best practices from the OEM or certified by the OEM TAC. Request to engage OEM or OEM certified professional services for installation in order to maintain the best practice as per the OEM standard. 	Vendor's expert team (OEM / OEM Authorized support engineer) will be onsite till complete installation, implementation and project sign-off.
74	24	PART – IV	2. Scope of Work:	Since APT solution is new edge and	Involvement of OEM professional

		SECTION – 1	2.4 Training Services	advanced technology, kindly clarify whether the training needs to be conducted by the bidder or involve the OEM professional services for the training.	services for the training is desired.
75	28	PART – IV SECTION – 2	1. TECHNICAL REQUIREMENTS & 2. TECHNICAL SPECIFICATIONS	It is assumed that the technical requirements are to be followed for compliance.	Yes. The bidder should comply with all the terms mentioned in the scope of work, technical requirements and technical specifications.
76	28	PART – IV SECTION – 2	1. TECHNICAL REQUIREMENTS & 2. TECHNICAL SPECIFICATIONS	Kindly clarify the solution throughput needed - if any or the parameters of overall interface bandwidth to decide on the solution throughput.	Yes, parameters of overall interface bandwidth to decide on the solution throughput which is at least 4 Gbps per appliance.
77	9	PART – I 3. Eligibility Criteria	Point no. 6: The bidder must have implemented at least two APT solutions in a BFSI / E-Commerce environment or at Banks in India. Documents to be submitted: PO / Invoice and satisfactory certificate from client to be submitted. Details to be furnished along with the references.	Request you to please change the clause as per below: The bidder must have implemented at least one APT solution in a BFSI / E-Commerce environment or at Banks in India.	Clause stands as per RFP.
78	43	PART – V 4. Payment Terms	4.1 80% of the order value along with GST and other applicable duties on actual basis will be paid on delivery, installation and acceptance of ordered items, after realizing penalty charges for late delivery and / or late installation, if any. The claim for payment should contain proof of delivery, installation report & User Acceptance Report signed by an authorized official of the bank / branch at the respective sites etc. 4.2 The balance 20% of order value will be paid after 3 months of successful running of Advanced Persistent Threat (APT) on	Request you to please change the clause as per below - 80% of the order value along with GST and other applicable duties on actual basis will be paid after successful delivery The balance 20% of order value will be paid after 3 months of successful running of Advanced Persistent Threat (APT)	Clause stands as per RFP.

			submission of the Performance Bank Guarantee (PBG) of the equivalent amount.		
79	42	PART – V 3. Delivery and Installation	<p>Point no. 3.1: Deliveries of the equipment, installation and operationalization of complete solution at all locations should be made within 4 weeks from the date of purchase order.</p>	<p>Request you to please change the clause as per below: Deliveries of the equipment, installation and operationalization of complete solution at all locations should be made within 8 weeks from the date of purchase order.</p>	Clause stands as per RFP.
80	8	Part – 1 Overview	<p>An Advanced Persistent Threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data other than to cause damage to the network or organization.</p>	<p>APT solution is not a commodity UTM or Firewall/IPS or Proxy that depends on traditional signature or pattern based detections. This solution needs a holistic and dedicated independent framework and methodology. FireEye has been pioneer in APT and even coined the term APT for industry. We work with major vendors and security regulators to build a framework which helps reduce the impact of Advance attacks on critical organizations. In this project we had suggested to have coverage from all three major APT vectors.</p> <p>Primary APT vectors of infection are Email, Web & Endpoint with Email being 85-90% of all infections. This is corroborated by all industry leading research reports like Ponemon Institute, Verizon Data Breach reports (Frequency of malware vector @page #18) etc. We request to incorporate email vector in monitoring as a solution so that</p>	Clause stands as per RFP.

				<p>coverage for EAPT vectors/channels is taken care of. To further explain the requirement of Email Security for APT solution, it requires a dedicated Email solution rather than monitoring only network based web traffic.</p> <p>Remarks/Change requested: APT platform as a solution cannot be taken in one vector only. It involves, Email, Network & Endpoint vectors and all vectors needs to be given due consideration in order to have a balanced platform.</p>	
81	22	PART – IV SECTION – 1	<p>2. Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. iv: Solution shall monitor, detect, alert, report and provide remediation, recommendation for infections discovered using SPAN or mirror traffic.</p>	<p>As APT threats are mostly zero day of unknown vulnerabilities. The remediation recommendations would not be available for unknown infections. However, as the solution prevents APT infections, such attacks would be prevented. The sizing for APT solution is mandatory and the parameters need to be defined. All three primary sources/vectors of infection require attention to have APT coverage. As a framework, APT solution should work independent of any underlying solution / technology and should be providing the services which help Detect, prevent and respond to advanced threats in a holistic manner. The requirements are missing in the specs which will create ambiguity in the solution sizing and create mismatch in solution architecture design and deliverables. We request and strongly recommend to consider the clause as proposed in column 'E'.</p>	<p>It should be deployed in line but should have the capability to be deployed in SPAN/TAP mode.</p>

				<p>If you are considering APT only at Network layer that means you would again land up in loopholes and would be missing 80% of attack surface which comes through Email and Endpoint channels.</p> <p>Please rephrase the clause as "Network/Web (1.0Gbps), E m a i l (10000 mailboxes) with XXXX incoming emails per day and Endpoints (10000 Endpoints). APT solution shall perform analysis on-premise and no files shall be sent outside the datacenter network. It should be based on the throughput and should not have any other restrictions. All necessary additional devices, licenses required for such configuration should be quoted as part of the solution. The Network / Web solution must be deployed in Inline blocking mode with Hardware bypass built-in. TCP reset is not acceptable form of inline blocking and preferred deployment mode".</p>	
82	22	PART – IV SECTION – 1	<p>2. Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. vi: Solution shall support unlimited endpoints on a single APT Appliance or multiple or under HA mode or stand-by mode.</p>	<p>Please explain if HA is required or optional.</p>	<p>The modified clause to be read as under: PART – IV: SECTION – 1 2. Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. vi: HA is optional. But APT appliance should support HA and without HA mode.</p>
83	22	PART – IV	2. Scope of Work:	Please explain what class of technology	The modified clause to be read as

		SECTION – 1	2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. viii: Solution should have following new class of security technology base for detecting unknown security threats and features.	is being asked for apart from APT	under: PART – IV: SECTION – 1 2. Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. viii: Solution should have the embedded class of technology to update itself automatically to detect latest type of threat propagating through network.
84	28	PART – IV SECTION – 2 1. TECHNICAL REQUIREMENTS	Clause no. 3: Solution should be deployed on premise and along with on premise sandboxing capability	Please specify that Sandboxing capability should be in same appliance and no external device is required.	No device specific but solution should be complete in itself so that no extra device is required by the bank.
85	28	PART – IV SECTION – 2 1. TECHNICAL REQUIREMENTS	Clause no. 10: Detection of C & C and Botnet that are carried by Any protocol	Please specify outgoing CnC connections should be blocked.	Yes.
86	28	PART – IV SECTION – 2 1. TECHNICAL REQUIREMENTS	Clause no. 13: Solution should be capable to integrate with devices like Firewall/IPS to mitigate risk by blocking similar session. (Checkpoint , Cisco)	Solution should have its own blocking capabilities and does not depend on other solutions. TCP reset is not an acceptable mechanism to block the suspected malicious sessions	Solution should have its own blocking capabilities and does not depend on other solutions
87	28	PART – IV SECTION – 2 1. TECHNICAL REQUIREMENTS	Clause no. 17: A solution must support minimum 4X1 GB supported to Copper Gigabit Ethernet (GBE). (4X1Gigabit Fiber (LC) interfaces optional).	Please clarify if (4X1Gigabit Fiber is optional and not to be quoted. Also confirm the total throughput capacity which is to be sized for the proposed appliance	The modified clause to be read as under: Clause no. 17: A solution must support minimum 8X1 GB supported to Copper Gigabit Ethernet (GBE). (4X1Gigabit Fiber (LC) interfaces optional).
88	29	PART – IV SECTION – 2 1. TECHNICAL REQUIREMENTS	Clause no. 22: The solution should be able to inspect and block all network sessions regardless of protocols for suspicious activities or files at various entry/exit sources to the Bank's	The solution would inspect and block monitored traffic at entry/exit sources where it is deployed only	The solution would inspect and block monitored traffic at entry/exit sources for the zone it is monitoring.

			network.		
89	29	PART – IV SECTION – 2 1. TECHNICAL REQUIREMENTS	Clause no. 24: The solution should be able to identify malware present in network file shares and web objects (For Eg: JPEG, doc, docx, exe, gif, hip, htm, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx. etc. and any new formats having vulnerabilities to carry potential malware) and able to quarantine them.	Please clarify if bank is looking for file share APT monitoring solution also.	The solution should Monitor and detect threats due to file shares and web objects within the bank's network.
90	29	PART – IV SECTION – 2 1. TECHNICAL REQUIREMENTS	Clause no. 26: The solution should be able to identify spear phishing email containing malicious URLs and attachments that bypass the anti-spam technologies.	Please specify the Email APT requirements and number of Mailboxes which are to be monitored	Not required.
91	29	PART – IV SECTION – 2 1. TECHNICAL REQUIREMENTS	Clause no. 31: The solution should be able to block the call back tunnel including fast flux connections.	The CnC call back blocking should not be based on fast flushing DNS of TCP reset like workarounds. It should be true blocking	Clause stands as per RFP.
92	30	PART – IV SECTION – 2 1. TECHNICAL REQUIREMENTS	Clause no. 44: Inspect https traffic (Full Deep Packet / Encrypted Traffic Inspection)	Please specify the amount of Https traffic mix is available on the network which needs to be monitored	As per throughput.
93	30 & 40-41	PART – IV SECTION – 2	1. TECHNICAL REQUIREMENTS Clause no. 46: Solution should be capable to integrate with devices like Web proxy to mitigate risk by blocking similar session. 2. TECHNICAL SPECIFICATIONS Point no. 80 Web Proxy Integration: Automated and Direct Integration with web proxy where web access policies can be implemented based on device state (suspected or infected) information discovered by the solution. (IE: Block) infected assets from communicating to	<ul style="list-style-type: none"> Please clarify why should integration with proxy is required to block similar sessions. The blocking of threats should be native to the proposed solution. It seems to give advantage to some proxy OEM to propose their workaround solution which they believe can comply with this requirement. Request to remove this specification as this gives leverage to Proxy vendors to propose their solution and propose a bolt on sandbox to comply. This is not true APT solution 	Solution should be inline in the network with web proxy.

			internet and/or high-value assets)	<ul style="list-style-type: none"> It should be modified. Automated and Direct Integration with web proxy. 	
94	30	PART – IV SECTION – 2 1. TECHNICAL REQUIREMENTS	Clause no. 50: The solution should be able to capture packets for deep dive analysis.	Kindly clarify by Packet capture you mean to have pcap data about the alert which got triggered for sessions which were part of threat detected	Yes, pcap data required only for the threat detected.
95	35	PART – IV SECTION – 2 2. TECHNICAL SPECIFICATIONS	Point no. 36 Inspection of Evidences: A solution support inspection of evidences both per threat and per asset.	Inspection of threats with required specifications would be at network layer and O.S change report for those threats which get detected. Kindly confirm if only network threats are being asked for evidence here.	Clause stands as per RFP.
96	39	PART – IV SECTION – 2 2. TECHNICAL SPECIFICATIONS	Point no. 74 & Point no. 76 Connection termination: A solution should be able to perform TCP RSTs for individual communication sessions with C&Cs to protect against the loss of data.	Query: TCP reset does not provide a fool proof mechanism to mitigate the call back blocking or APT threat prevention. Please ensure TCP reset should not be the method of mitigation. Remarks / change Requested: This needs to be removed as this gives leverage to Firewall vendors to propose their solution and propose a bolt on sandbox to comply. This is not true APT solution.	Clause stands as per RFP.
97	39	PART – IV SECTION – 2 2. TECHNICAL SPECIFICATIONS	Point no. 77 Firewall integration: A solution should integrate with firewall platform for asset quarantine purpose such as Check Point, Cisco firewall.	Query: What is the requirement for integration with firewall to quarantine the asset when the solution should have the capability on box to block the communication. To contain the endpoint, a solution needs to be used which can monitor endpoints regularly and enable to contain the asset from communicating out from network.	Solution should be inline in the network. For asset quarantine the solution should be complete in itself and not depend on other devices.

				Remarks / change Requested: This needs to be removed as this gives leverage to Firewall vendors to propose their solution and propose a bolt on sandbox to comply. This is not true APT solution	
98	40	PART – IV SECTION – 2 2. TECHNICAL SPECIFICATIONS	Point no. 78 Firewall integration: Automated and Direct Integration with Checkpoint firewall where firewall policies can implemented based on device state (suspected or infected) information discovered by the solution. (IE: Block infected assets from communicating to internet and/or high-value assets, enhance logging on suspected assets)	Query: What is the requirement for integration with firewall to quarantine the asset when the solution should have the capability on box to block the communication. To contain the endpoint, a solution needs to be used which can monitor endpoints regularly and enable to contain the asset from communicating out from network. Remarks / change Requested: This needs to be removed as this gives leverage to Firewall vendors to propose their solution and propose a bolt on sandbox to comply. This is not true APT solution	Clause stands as per RFP.
99	40-41	PART – IV SECTION – 2 2. TECHNICAL SPECIFICATIONS	Point no. 82 AV Integration: Automated and Direct Integration with Endpoint AV solution to create / add identified threat's file integrity hash value. The Solution can work in conjunction with ANTIVIRUS but it should not be dependent on it.	Request to remove this specification as this gives leverage to AV platform vendors to propose their solution and propose a bolt-on sandbox to comply. This is not true APT solution. If the existing NGFW/NGAV/NG Proxy solutions could have been effective, why they could not be able prevent the APT threats. They are by design made to work for a specific use case like Firewall/proxy/V and have specific technology being used. To bolt-on a Sandbox on top and comply to APT solution is not true solution but taking leverage of situations.	Solution should be inline in the network with AV.

100			Request to add: Network/Web	The Overall solution sandbox engine must include prepopulated LICENSED copies of Microsoft windows and office images through an agreement with Microsoft to run multiple concurrent executions of Virtual Environment. There should be no requirement for the customer to buy additional Microsoft licenses for sandboxing solution	The solution should contain all the required licenses for all the software/hardware. Bank will not purchase any software and hardware separately.
101			Request to add: Network/Web	Proposed APT solution should be designed as independent solution of other security components proposed as part of RFP such as Firewall, IPS, Proxy, Anti-spam, DLP or Anti-virus. APT should be from different OEM to have an independent layer of protection from advance attacks.	Solution should be inline in the network with AV Firewall , IPS, Proxy, Anti-spam ,DLP etc.
102			Request to add: Network/Web	The proposed solution should have the ability to analyze, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents, common multimedia contents such as JPEG, QuickTime, MP3 and ZIP/RAR/7ZIP/TNEF archives, 3gp, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm to prevent advanced Malware and Zero-day attacks.	Solution should be able to detect the persistent threats which come through executable files, PDF files, Flash files, RTF files, any type of file as mentioned in the RFP.
103			Request to add: Network/Web	The solution must be deployed in Inline blocking mode with bypass .TCP reset is not acceptable form of inline blocking	It should be deployed in line but should have the capability to be deployed in SPAN/TAP mode.
104			Request to add: Network/Web	The solution must utilize purpose built Virtual Machine (on-premise) to	No addition in RFP technical Requirements.

				positively identify malware, including zero-hour vulnerability exploits, polymorphic payloads, and obfuscated java-script. The virtualization solution must not be detectable by malware in order to avoid evasion. Relevant anti VM detection techniques used in the solution must be specified.	
105			Request to add: Endpoint	This solution should integrate with the proposed Advanced Threat Protection Platform for Network to receive Indicators of Compromise for unknown or zero day threats detected by sandboxing behavioral engine within Network Anti-APT solution.	No addition in RFP technical Requirements.
106			Request to add: Endpoint	Servers/Controllers for End Point Security Solution should be deployed on premise and agents should not be managed or controlled by cloud based servers/controllers	No addition in RFP technical Requirements.
107			Request to add: Endpoint	Solution should provide a flexible, data-driven exploit behavioral intelligence .The solution must support exploit detection & prevention capabilities. Exploit detection capability does not depend on signatures like traditional AV solutions and shall minimally support the detection of the following exploit techniques: Return-oriented programming (ROP) attacks, Heap spray attacks, Application crashes caused by exploits, Structured Exception Handling Overflow Protection (SEHOP) corruption, Drive-by downloads of programs, Null page exploits, Microsoft Office macro-based exploits, Java exploits, shell code detection, process injection detection, Access	No addition in RFP technical Requirements.

				token privilege escalation detection, DEP. It shall support commonly exploited applications minimally Office Word, Office Excel, Office Power point, Internet Explorer, Mozilla Firefox, Google Chrome, Java, Adobe Flash, Adobe Reader.	
108			Request to add: Endpoint	The solution must be able to automatically kill exploited applications or automatically prevent any payload from exploited application to run.	No addition in RFP technical Requirements.
109			Request to add: Endpoint	The solution must support the ability to exclude applications or files from exploit detection/prevention.	No addition in RFP technical Requirements.
110			Request to add: Endpoint	End-user shall be notified of automatically killed applications and payloads ensuring seamless user experience.	No addition in RFP technical Requirements.
111			Request to add: Endpoint	The solution must support the recording of recent activities on each endpoint in an indexed and searchable lookback cache, minimally file writes, registry operations, network connections, DNS resolutions, URL collection, process loaded in memory.	No addition in RFP technical Requirements.
112			Request to add: Endpoint	Agent should be lightweight, operating at low priority with virtually no impact to end user	No addition in RFP technical Requirements.
113			Request to add: Endpoint	Solution must be able to drill into system activity during a specific incident time window to determine the source of the threat and possible data exfiltration or lateral movement	No addition in RFP technical Requirements.
114			Request to add: Endpoint	Solution must be able to mitigate the impact of a compromised system with network isolation (i.e. remote containment) using workflow driven	No addition in RFP technical Requirements.

				containment in order to prevent lateral spread.	
115			Request to add: Endpoint	The solution shall support end-user notification when containment is enforced.	No addition in RFP technical Requirements.
116			Request to add: Endpoint	The solution must be able to exclude mission-critical hosts from containment; ensuring enterprise-wide disruptions are minimal.	No addition in RFP technical Requirements.
117			Request to add: Endpoint	The default and custom defined detection policies can be modified to monitor and ignore certain behavior, conditions, or applications.	No addition in RFP technical Requirements.
118			Request to add: Endpoint	Solution must provide an easy to use interface and require no more than an entry level SOC analysts and/or IR responder skillset to operate.	No addition in RFP technical Requirements.
119			Request to add: Endpoint	The solution must offer a built-in graphical triage viewer to ease security operations and require no more than an entry level SOC analysts and/or IR responder skillset to operate.	No addition in RFP technical Requirements.
120			Request to add: Endpoint	Solution should be able to automatically generate forensic package upon detection of a threat or IOC match for deep level forensic by Incident Responders.	No addition in RFP technical Requirements.
121			Request to add: Endpoint	Solution should be able to detect attacks & alert using methodology indicators such as understanding attacks loaded into memory to steal passwords or power shell commands usage with arguments run by attacker for stealing credentials.	No addition in RFP technical Requirements.
122			Request to add: Endpoint	Solution should provide capability to SOC analyst to acquire malicious file remotely for analysis.	No addition in RFP technical Requirements.
123			Request to add:	Solution must provide the following	No addition in RFP technical

			Endpoint	hunting/searching capabilities across all agents:	Requirements.
124			Request to add: Endpoint	-broadly search for known malicious behavior	No addition in RFP technical Requirements.
125			Request to add: Endpoint	proactively "Hunt" for suspicious activity	No addition in RFP technical Requirements.
126			Request to add: Endpoint	-comprehensively investigate compromised endpoints	No addition in RFP technical Requirements.
127			Request to add: Endpoint	search for all evidence of advanced intrusions, not just malware	No addition in RFP technical Requirements.
128			Request to add: Endpoint	The solution must support to search the enterprise endpoint population for malicious activity including metadata on Browser, Cookie, Driver, Executable, File, HTTP Header, IP Connections, Process, Parent process, Port, Registry, Tasks, Services, URLs, Username etc.	No addition in RFP technical Requirements.
129			Request to add: Endpoint	The solution must be capable of detecting attacker lateral movement.	No addition in RFP technical Requirements.
130			Request to add: Endpoint	The solution must be capable of detecting fileless malware.	No addition in RFP technical Requirements.
131			Request to add: Endpoint	The solution must be capable of detecting the execution of post-exploitation tools.	No addition in RFP technical Requirements.
132			Request to add: Endpoint	The solution must be capable of detecting data exfiltration.	No addition in RFP technical Requirements.
133			Request to add: Endpoint	The solution must support Windows & Mac-OS End Points.	No addition in RFP technical Requirements.
134			Request to add: Endpoint	The solution's Infrastructure and Agent shall be easily installed and deployed, lightweight, and operating at low priority with virtually no impact to end user.	No addition in RFP technical Requirements.
135			Request to add: Endpoint	The solution's agent must include policies to maximize performance by controlling the amount of CPU.	No addition in RFP technical Requirements.
136			Request to add: Email Threat Prevention Platform	Proposed Email APT should be deployed independently in MTA mode	No addition in RFP technical Requirements.

				monitoring Email traffic coming from outside and delivering the mails to Email Server on-premise, post quarantine of Advance threats.	
137			Request to add: Email Threat Prevention Platform	The proposed solution should have the ability to be deployed in the following modes: <ul style="list-style-type: none"> • BCC monitoring mode • Inline MTA Block mode 	No addition in RFP technical Requirements.
138			Request to add: Email Threat Prevention Platform	Proposed Email APT solution should accurately detect and immediately stop advanced and targeted attacks, including spear phishing and ransomware targeted email URL's or attachments using signatureless Execution Engine before they enter user environment. The solution should detect such attacks which are missed by Anti-Spam engine	No addition in RFP technical Requirements.
139			Request to add: Email Threat Prevention Platform	Email APT solution must have its own dedicated Virtual Execution Engine (Sandboxing) that inspects suspicious email traffic to identify attacks that evade traditional signature- and policy-based defenses. The Sandboxing engine must detect zero-day, multi-flow and other evasive attacks by using dynamic, signatureless analysis in a safe, virtual environment. The solution sandboxing should not be shared with other vectors for analysis and should have its own environment to function independently.	No addition in RFP technical Requirements.
140			Request to add: Email Threat Prevention Platform	The solution must have ability to protect against e-mail borne spear-phishing & targeted attacks and have ability to analyze/process at least 10000 incoming emails per day (with URLs and	No addition in RFP technical Requirements.

				email attachments of variable sizes) .Solution should be licensed for 1800 number of user mailboxes	
141			Request to add: Email Threat Prevention Platform	The solution must be able to support Windows OS (32 bit, 64 Bit) & Mac OSX OS images profiles on premise for the Dynamic Analysis Engine (VM) all within the single appliance form factor.	No addition in RFP technical Requirements.
142			Request to add: Email Threat Prevention Platform	The proposed solution must have the ability to analyze, detect, quarantine and block malware in common file formats attachment types including, but not limited to: EXE,DLL, PDF, SWF, DOC/ DOCX, XLS/XLSX, PPT/PPTX,JPG, PNG, MP3, MP4 and ZIP/RAR/TNEF archives	No addition in RFP technical Requirements.
143			Request to add: Email Threat Prevention Platform	The virtual execution or sandboxing engine must have pre-shipped guest images supporting wide variety of file types for dynamic sandbox analysis : 3gp, applet, accdb ,asf, avi, chm, csv,com, dll, doc, docx, eeml,eml ,exe, gif, hlp, hta, htm, ico, jar, jpg, mov, mp3, mp4,mpg, msg,midi,msi,pdf, png, ppsx, ppt, pptx, qt, rm, rtf,rmi, swf, tiff, url, vbs, vcf, vcs,xls, xlsx,xdp, bat, cmd, js, wsf, xml, flv, wav, wma ,lnk to prevent advanced Malware and Zero-day attacks.	No addition in RFP technical Requirements.
144			Request to add: Email Threat Prevention Platform	The proposed solution should have the ability to quarantine emails with malicious attachments or URLs locally and have the option to keep a copy of the quarantined emails with malicious attachments for further forensics analysis.	No addition in RFP technical Requirements.
145			Request to add: Email Threat Prevention Platform	Solution should allow to set Congestion Control thresholds and analysis bypass	No addition in RFP technical Requirements.

				threshold to prevent overloading of emails from sender MTA.	
146			Request to add: Email Threat Prevention Platform	Email APT device should have an ability to hold inbound email traffic in MTA Queue until all attachments have been dynamically analyzed within a dynamic execution Environment for malicious behavior.	No addition in RFP technical Requirements.
147			Request to add: Email Threat Prevention Platform	The solution must be able to utilize mandatory and opportunistic TLS connections in order to securely deliver the e-mails.	No addition in RFP technical Requirements.
148			Request to add: Email Threat Prevention Platform	The email APT solution must support Credential Phishing URL and typosquatting attack detection for all sender domain & URL domain in email body	No addition in RFP technical Requirements.
149			Request to add: Email Threat Prevention Platform	Proposed solution must be able to extract malware out of password protected archive files sent as attachments where password is listed in email body and submit malware for sandbox analysis. This is strong evasion technique used by APT threat actors to bypass sandboxing solution. Solution should be resistant to such evasion techniques	No addition in RFP technical Requirements.
150			Request to add: Email Threat Prevention Platform	The solution must support for multi-language password candidate extraction from email body	No addition in RFP technical Requirements.
151			Request to add: Email Threat Prevention Platform	Admin must be able to specify their own list of passwords for extractive documents out of archive files for analysis	No addition in RFP technical Requirements.
152			Request to add: Email Threat Prevention Platform	The solution must support retroactive detection feature that allows to alert on missed objects or previously undetected URLs if they become	No addition in RFP technical Requirements.

				malicious.	
153			Request to add: Email Threat Prevention Platform	The proposed solution should differentiate between riskware vs advance threats and provide separate alerts on riskware to isolate critical threats	No addition in RFP technical Requirements.
154			Request to add: Email Threat Prevention Platform	Proposed solution should be able to scan for malicious URL embedded inside PDF & DOC attachments and block emails with malicious attachments	No addition in RFP technical Requirements.
155			Request to add: Email Threat Prevention Platform	The solution must have capability to integrate with Vendor's Network Based Advance Persistent Threat detection solution to stop blended attacks across multiple vectors by quarantine emails with malicious URLs and trace Web-based attacks back to the original spear-phishing email.	No addition in RFP technical Requirements.
156			Request to add: Email Threat Prevention Platform	Email APT solution must meet the FedRAMP security requirements and complies with SOC 2 Type II certification	No addition in RFP technical Requirements.
157			Request to add: Email Threat Prevention Platform	Dashboard should display following statistics: Email Traffic Message Attachments Top Senders Top Recipients Top Rule Matches Advanced Threats Recent Alerts Threat Map	No addition in RFP technical Requirements.
158			Request to add: Email Threat Prevention Platform	If the URL is detected as malicious, upon click user is redirected to a page indicating that the URL is blocked and that the site contains malicious content.	No addition in RFP technical Requirements.
159			Request to add: Email Threat Prevention Platform	If the URL is detected as suspicious, upon click user is redirected to a page	No addition in RFP technical Requirements.

				informing you that the site might contain malicious content.	
160			Request to add: Email Threat Prevention Platform	If the URL is detected as non-malicious, upon click user can access the original URL in the email message.	No addition in RFP technical Requirements.
161	28	PART – IV SECTION – 2	1. TECHNICAL REQUIREMENTS & 2. TECHNICAL SPECIFICATIONS	The requirement and specification are separately mentioned in two different tables. It is assumed that the technical requirements are to be followed for compliance.	Yes. The bidder should comply with all the terms mentioned in the scope of work, technical requirements and technical specifications.
162	28	PART – IV SECTION – 2	1. TECHNICAL REQUIREMENTS & 2. TECHNICAL SPECIFICATIONS	Appliance sizing Kindly clarify whether the APT solution is to be sized to handle more than 10,000 users.	Clause stands as per RFP.
163	22	PART – IV SECTION – 1	2. Scope of Work 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. v Solution shall use agentless approach for detection of infections via network activities analysis from the endpoints. Point no.vi Solution shall support unlimited endpoints on a single APT Appliance or multiple or under HA mode or stand-by mode.	Kindly verify whether endpoint protection is needed or network protection or both?	Network protection.
164	23	PART – IV SECTION – 1	2. Scope of Work 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. xxviii OEM/ Bidder to provide hardware replacement within 3 days' time if failed as part of RMA replacement policy.	<ul style="list-style-type: none"> How you are expecting 99.5% uptime with 3 days replacement procedure, kindly clarify? Do Bank mean 3 business days please clarify. 	The modified clause to be read as under: PART – IV SECTION – 1 2. Scope of Work 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. xxviii The bidder should maintain 99.5 % uptime within the SLA. During any

					fault of equipments non-availability of the services will be treated as downtime.
165	42 & 43	Part – V	<p>2. Performance Bank Guarantee The successful bidder shall be required to provide a Bank Guarantee for 10% of the Total Order Value issued by any scheduled commercial bank (other than UCO Bank) valid for 39 months (36+3 months claim period), from the issuance of Purchase Order (PO), indemnifying any loss to the Bank, as per the format of Annexure – J.</p> <p>4. Payment Terms 4.2 The balance 20% of order value will be paid after 3 months of successful running of Advanced Persistent Threat (APT) on submission of the Performance Bank Guarantee (PBG) of the equivalent amount.</p>	<p>Under PBG: This clause suggest PBG of 10% of Total Order Value for 39 months</p> <p>Under payment terms: This clause suggests 20% of order value would be paid on submission of PBG of equivalent amount.</p> <p>Query: Both the clauses highlighted have different values of Performance Bank Guarantee and hence we request bank to modify the payment terms as under to bring standardization.</p> <p>Payment Terms: 1. 90% of order value to be paid on delivery of products, installation, commissioning of solution along with User Acceptance Testing 2. 10% of order value to be paid after submitting Performance Bank Guarantee of equivalent amount as highlighted under Pg.42 - Part V - Clause 2.</p>	Clause stands as per RFP.
166		General	Indemnity	We request that the clarity be provided in the RFP that - Indemnity shall only be restricted to third party claim for (i) IPR Infringement indemnity, and (ii) bodily injury and death and tangible property damage due to gross negligence and willful misconduct. The process of indemnification shall provide the requirement of notice, right to defend and settle, and the concept of	Clause stands as per RFP.

				apportionment (liable only to the extent of its claim), mitigation and carve-outs.	
167	9	Eligibility Criteria	<p>Point no. 6: The bidder must have implemented at least two APT solutions in a BFSI / E-Commerce environment or at Banks in India.</p> <p>Documents to be submitted: PO / Invoice and satisfactory certificate from client to be submitted. Details to be furnished along with the references.</p>	We request Bank to change "APT solution" to "Network/Web/Email APT Solution" as the RFP is to implement Network APT	Clause stands as per RFP.
168	24	PART – IV SECTION – 1	<p>2. Scope of Work 2.4 Training Services: a. The Vendor/Bidder shall provide training at Kolkata location or any other location as specified by Bank to the number of personnel identified by UCO Bank on functional, operational and reporting aspects of the entire APT solution.</p>	<p>1) Requesting to confirm the Training location at least City name instead of "any other location". 2) Request you to mention the Maximum no of participants per batch for the training.</p>	<p>Training location will be Kolkata at Bank's premises. Two (2) batches with each of 10 participants.</p>
169	24	PART – IV SECTION – 1	<p>2. Scope of Work 2.4 Training Services: b. The Bidder/ Vendor shall provide training to at-least two batches of UCO Bank officials for the following each type of training. i. User Training. ii. System Administration training. iii. Top executive awareness program.</p> <p>d. Training deliverables shall be i. User Training Plan. ii. Training Material in English. iii. Exercises with Sample Test Cases.</p>	<ul style="list-style-type: none"> As per understanding total 6Nos of trainings requested. Kindly confirm the timeline to complete those trainings. Request you to confirm the training timeline and kindly keep this training post Project sign-off. 	Within three month of success full running.
170	24	PART – IV SECTION – 1	<p>2. Scope of Work 2.4 Training Services: c. Training shall be for Two days per batch</p>	Request you to mention the Maximum no of participants per batch for the training.	Maximum no of participants per batch for the training is 20.

			with a batch size as mutually agreed by the UCO Bank and Vendor/Bidder.		
171	26	PART – IV SECTION – 1	2. Scope of Work 2.7 Schedule: The Vendor/Bidder shall implement the solution /Service(s) as per the schedule specified below: a. Technical Support services period will be for 3 years. (from deployment day till end of 3rd year) b. The period of contract shall be extendable, based on mutually agreed terms and conditions.	Requesting you to mention the Installation timeline/schedule as well in this section.	Please refer to the addendum of the pre-bid responses.
172	42	PART – V	3. Delivery and Installation: Point no. 3.1 Deliveries of the equipment, installation and operationalization of complete solution at all locations should be made within 4 weeks from the date of purchase order.	Requesting you to segregate the product delivery and implementation timeline. We propose as per below: 1) Delivery of the HW/SW/Lic within 8 Weeks from the PO. 2) Installation of the supplied HW/SW/Lic within 4 weeks from the delivery of the products.	Clause stands as per RFP.
173	43	PART – V	4. Payment Terms 4.1 80% of the order value along with GST and other applicable duties on actual basis will be paid on delivery, installation and acceptance of ordered items, after realizing penalty charges for late delivery and / or late installation, if any. The claim for payment should contain proof of delivery, installation report & User Acceptance Report signed by an authorized official of the bank / branch at the respective sites etc. 4.2 The balance 20% of order value will be paid after 3 months of successful running of Advanced Persistent Threat (APT) on submission of the Performance Bank Guarantee (PBG) of the equivalent	Requesting you to change the payment terms as per below: 1) 70% of the order value will be released post-delivery to the HW/SW/Lic. 2) 20% of the order value will be released post implementation. 3) 10% of the order value will be released after 3months post installation. Note: Bank will release the full payment if any delay happened from Bank end post timeline mentioned above.	Clause stands as per RFP.

			amount.		
174	15	Part – II: INVITATION FOR BIDS AND INSTRUCTIONS TO BIDDERS	17. RFP Response Validity Period RFPs response will remain valid and open for evaluation according to their terms for a period of at least 6 months from the time the RFP response submission process closes.	Bidder proposed the RFP response to be valid for 120 days from the submission date.	Clause stands as per RFP.
175	51	PART – V	22. Exit Option and Contract Re-Negotiation: The Bank will reserve a right to re-negotiate the price and terms of the entire contract with the Selected Bidder at more favourable terms in case such terms are offered in the industry at that time for projects of similar and comparable size, scope and quality.	The prices for any alteration in the requirements will be mutually discussed and agreed between TCL and UCO Bank.	Clause stands as per RFP.
176	51	PART – V	22. Exit Option and Contract Re-Negotiation: The Bank shall have the option of purchasing the equipment from third-party suppliers, in case such equipment is available at a lower price and the Selected Bidder's offer does not match such lower price. Notwithstanding the foregoing, the Selected Bidder shall continue to have the same obligations as contained in this scope document in relation to such equipment procured from third-party suppliers.	Bidder proposes to remove this clause.	Clause stands as per RFP.
177	49	PART – V	16. Indemnity The selected Bidder agrees to indemnify and keep indemnified the Bank against all losses, damages, costs, charges and expenses incurred or suffered by the Bank due to or on account of any claim for infringement of intellectual property rights. The selected Bidder agrees to indemnify	We propose the following clause to replace the current clause "Each Party shall indemnify the other from and against any claims by third parties (including any governmental authority) and expenses (including legal fees and court costs) arising from damage to tangible property, personal injury or death caused by such Party's	Clause stands as per RFP.

			<p>and keep indemnified the Bank against all losses, damages, costs, charges and expenses incurred or suffered by the Bank due to or on account of any breach of the terms and conditions contained in this RFP or Service Level Agreement to be executed.</p> <p>The selected Bidder agrees to indemnify and keep indemnified Bank at all times against all claims, demands, actions, costs, expenses (including legal expenses), loss of reputation and suits which may arise or be brought against the Bank, by third parties on account of negligence or failure to fulfill obligations by the selected bidder or its employees/personnel.</p> <p>All indemnities shall survive notwithstanding expiry or termination of Service Level Agreement and the Vendor shall continue to be liable under the indemnities.</p> <p>Selected Bidder is required to furnish a separate Letter of Indemnity (Format whereof to be supplied by the Bank) in Bank's favour in this respect before or at the time of execution of the Service Level Agreement.</p>	negligence or willful misconduct."	
178	53	PART – V	<p>24. Termination</p> <p>a) The selected bidder commits a breach of any of the terms and conditions of this RFP or the SLA to be executed between the Bank and the selected Bidder.</p>	Termination should be only for material breach of the contract.	Clause stands as per RFP.
179	53	PART – V	<p>24. Termination</p>	Bidder should not be asked to bear	Clause stands as per RFP.

			<p>h) After award of the contract, if the selected bidder does not perform satisfactorily or delays execution of the contract, UCO BANK reserves the right to get the balance contract executed by another party of its choice by giving one month's notice for the same. In this event, the selected bidder is bound to make good the additional expenditure, which UCO BANK may have to incur in executing the balance contract. This clause is applicable, if the contract is cancelled for any reason, whatsoever.</p> <p>i) UCO BANK reserves the right to recover any dues payable by the selected Bidder from any amount outstanding to the credit of the selected bidder, including the adjustment of pending bills and/or invoking the Performance Bank Guarantee under this contract.</p>	expenditure as bidder is already paying agreed liquidated damages. Kindly amend the clause accordingly.	
180	54	PART – V	<p>26. Effect of termination: Nothing herein shall restrict the right of UCO BANK to invoke the Performance Bank Guarantee and other guarantees, securities furnished, enforce the Letter of Indemnity and pursue such other rights and/or remedies that may be available to UCO BANK under law or otherwise.</p>	Please take out indemnity provision from this clause	Clause stands as per RFP.
181	86	Annexure – P Non-Disclosure Agreement	<p>9. Arbitration and Equitable Relief (d) Indemnification The Receiving Party shall indemnify the Bank and hold the Bank harmless against any loss caused to it as a result of the non-performance or improper performance of this Agreement by the Receiving Party, or its servants or agents to perform any aspect of its obligations forming part of</p>	This clause is open ended and exposes the party to unlimited liability therefore, please take out this clause from the RFP	Clause stands as per RFP.

			the subject matter of this Agreement.		
182	23	PART – IV SECTION – I	<p>Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. xxv The bidder should have back to back arrangement with the OEM so that bank will be able to log a call with the OEM directly.</p>	Is that Bank needs to book ticket with Bidder as well as OEM. Also how Bank will determine which tickets to be booked with OEM and which to be booked with Bidder. Please clarify.	Bank will inform the bidder. Bidder will make arrangement for the bank to log a call with the OEM.
183	23	PART – IV SECTION – I	<p>Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. xxvi The bidder should have a 24x7 365 days support contact center in order to log the calls. The contact center numbers should be provided to the Bank along with the escalation matrix mentioning the contact person's name, number and designation in the company. The selected bidder has to supply, install and configure the hardware and software provided as per the timelines and SLA levels prescribed in the RFP.</p>	Understand the bidder is responsible for supply, install and configure the hardware and software. What is the support expectation from Bidder or is any day to day management is required from the bidder.	Apart from supply, install and configure, trouble shooting of the hardware/software support and as per the clause 2.6(Page no 23).
184	23	PART – IV SECTION – I	<p>Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. xxvii Technical support shall be for 3 (Three) years (from deployment day till end of 3rd year).</p>	Is it the OEM support which Bank is required.	Bidder support along with arrangement for the bank to log a call with the OEM.
185	47	PART – V 10. Warranty	During the warranty period, the vendor will have to undertake comprehensive maintenance of the entire hardware, hardware components, software, services and accessories supplied by the vendor. This service is to be provided on all the working days of the Bank notwithstanding	The replacement policy contradicts the Warranty terms. As per replacement policy 3 days is the TAT for RMA. Please clarify on the same.	Please refer to Sl. No. 171 of the pre-bid responses.

			the fact whether on such days the selected vendor's office remains closed or not. The request for support shall have to be attended by the vendor even if the request is made over telephone / SMS or by e-mail / fax by the respective sites, as per SLA. The entire equipment should be repaired within 24 hours (Resolution time). In case of vendor failing above standards, a standby arrangement should be provided till the machine is repaired.		
186	24	PART – IV SECTION – I	2. Scope of Work 2.4 Training Services:	Bank to arrange the venue or Bidder to arrange the venue for training.	Training location will be Kolkata at Bank's premises.
187	45	PART – V 8. Penalty	Bidder will provide on-site support for addressing Software/application related issues.	Does the Bank require a dedicated on-site resource for this or is it required on need basis only?	Need basis only for addressing Software/application related issues.
188	45	PART – V 8. Penalty	Reports: Reports of availability, performance, incident of Advanced Persistence Threat (APT) Management solutions if any, shall be submitted on monthly basis to Bank. Quarterly review shall be conducted for all Service Level requirements.	What is the expectation / scope of work from bidder post implementation after 100% payment?	As per the clause 2.6. Part 4, Section- 1 Of RFP.
				Who would own the service requests and security incident management post implementation?	Service requests are according to Part 4, Section- 1 and clause 2.6. Of RFP and security incident management will be done by Bank post implementation.
189	9	PART – I 3. Eligibility Criteria	Point no. 6 The bidder must have implemented at least two APT solutions in a BFSI / Ecommerce environment or at Banks in India. Documents to be submitted: PO / Invoice and satisfactory certificate from client to be submitted. Details to be furnished along with the references.	Please relax the clause to one APT solution in a BFSI / Ecommerce environment or at Banks in India.	Clause stands as per RFP.
190	28	PART – IV Section – 2 1. Technical Requirements	Point no. 16 Solution/appliance must have RAID redundancy (for hard drives), network redundancy (for management network interfaces), power Supply and Fan	Management solution does not need to be dedicated and can be performed over management IP addresses connected to redundant switches in the datacenter. - Request to modify the	Clause stands as per RFP.

			module redundancy.	clause as "Solution/appliance must have RAID redundancy (for hard drives), power Supply and Fan module redundancy.	
191	28	PART – IV SECTION – 1 & SECTION – 2	1. Technical Requirements & 2. Technical Specifications	Appliance sizing - Kindly clarify whether the APT solution is to be sized to handle more than 10,000 users.	Clause stands as per RFP.
192	23	PART – IV SECTION – 1	Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. xiii Solution shall support role-based administration such as Administrator, Malware Analyst, Database Reader, and Read-only access users.	The roles cannot be as mentioned in the RFP in practical world. - Multiple user account with different roles should be supported.	Clause is Self-Explanatory.
193	23	PART – IV SECTION – 1	Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. xxiv Licenses should be considered based on registered asset to console at any given point of time if applicable.	Should have more option for licensing. - Licenses should be considered based on registered asset to console or volume of traffic handled OR number of file processed at any given point of time if applicable.	Clause stands as per RFP.
194	23	PART – IV SECTION – 1	Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. xxviii OEM/ Bidder to provide hardware replacement within 3 days' time if failed as part of RMA replacement policy.	Very less time for Hardware replacement. - OEM/ Bidder to provide hardware replacement within 45 days' time if failed as part of RMA replacement policy.	Clause stands as per RFP.
195	30	PART – IV Section – 2 1. Technical Requirements	Point no. 39: Sandboxing File type supports (.doc, .xls, .ppt, .pdf, .exe, .zip, .rar, .tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj, .exe, .dll, .avi, .mpeg, .mp3/4, .jpg, java script, JavaArchive JAR, LNK, .chm, .swf, .sys, .com, .hwp, etc.)	Some file types can be supported only in Linux & Unix systems. - Sandboxing File type supports (.doc, .xls, .ppt, .pdf, .cab, .rar, .arj, .exe, .dll, .avi, .mpeg, .mp3/4, .jpg, java script, JavaArchive JAR, LNK, .chm, .swf, .sys, .com, .hwp, etc.)	Clause stands as per RFP.

Addendum

Part – IV, Section – 1: Scope of Work

2.7 Schedule:

c. Deliveries of the equipment, installation and operationalization of complete solution at all locations should be made within 4 weeks from the date of purchase order.

Corrigendum

Sl. No.	Existing Clauses	Modified Clauses
1	<p>Part – I: 3. Eligibility Criteria & Annexure – B: Eligibility Criteria Compliance Point no.6 The bidder must have implemented at least two APT solutions in a BFSI / E-Commerce environment or at Banks in India.</p> <p>Documents to be submitted: PO / Invoice and satisfactory certificate from client to be submitted. Details to be furnished along with the references.</p>	<p>Part – I: 3. Eligibility Criteria & Annexure – B: Eligibility Criteria Compliance Point no.6 The bidder must have implemented at least one APT solution in a BFSI / E-Commerce environment or at Banks in India.</p> <p>Documents to be submitted: PO / Invoice and satisfactory certificate from client to be submitted. Details to be furnished along with the references.</p>
2	<p>PART – IV: SECTION – 2 1. TECHNICAL REQUIREMENTS: Clause no. 4: Sandboxing capabilities of following Operating Systems (32 and 64 bit) : Win XP, Win7, Win8.x, Win10.x, Server 2008 R2, 2012 R2, Linux, Unix and MAC OS, all industry standard OS</p>	<p>PART – IV: SECTION – 2 1. TECHNICAL REQUIREMENTS: As per the RFP clause no.4, page no 28, Sandboxing capabilities of following Operating Systems (32 and 64 bit): Win XP, Win7, Win8.x, Win10.x, Server 2008 R2, and 2012 R2. In addition to the requirement static analysis for Linux, MAC OS or any x86 platform by the solution is preferable.</p>
3	<p>PART – IV: Section – 1 Scope of Work: POC (Proof of Concept): Technically qualified bidders should conduct POC (Proof of Concept)</p>	<p>PART – IV: Section – 1 Scope of Work: POC (Proof of Concept): Technically qualified bidders should conduct POC (Proof of Concept) within</p>

	within 1 week (7 working days from the date of mail sent to the technically qualified bidders)	10 working days from the date of mail sent to the technically qualified bidder.
4	PART – IV: SECTION – 1 Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. ii Vendor's expert team will be onsite till complete installation, implementation and project sign-off.	PART – IV: SECTION – 1 Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. ii Vendor's expert team OR Vendor's authorized expert team will be onsite till complete installation, implementation and project sign-off.
5	Part – IV: Section – 2 1. Technical Requirements Clause no. 17: A solution must support minimum 4X1 GB supported to Copper Gigabit Ethernet (GBE). (4X1Gigabit Fiber (LC) interfaces optional).	Part – IV: Section – 2 1. Technical Requirements Clause no. 17: A solution must support minimum 8X1 GB supported to Copper Gigabit Ethernet (GBE). (4X1Gigabit Fiber (LC) interfaces optional).
6	PART – IV: SECTION – 1 2. Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. vi: Solution shall support unlimited endpoints on a single APT Appliance or multiple or under HA mode or stand-by mode.	PART – IV: SECTION – 1 2. Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. vi: HA is optional. But APT appliance should support HA and without HA mode.
7	PART – IV: SECTION – 1 2. Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. viii: Solution should have following new class of security technology base for detecting unknown security threats and features.	PART – IV: SECTION – 1 2. Scope of Work: 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. viii: Solution should have the embedded class of technology to update itself automatically to detect latest type of threat propagating through network.
8	PART – IV: SECTION – 1 2. Scope of Work 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. xxviii OEM/ Bidder to provide hardware	PART – IV: SECTION – 1 2. Scope of Work 2.2. Solution for the Advanced Persistent Threat (APT) broadly covers the following: Point no. xxviii The bidder should maintain 99.5 % uptime within the SLA. During any fault of

	replacement within 3 days' time if failed as part of RMA replacement policy.	equipments non-availability of the services will be treated as downtime.												
9	<p>Part – IV : Section – 1</p> <p>2.6. System Maintenance & Support Services</p> <p>Support – Terms and Conditions: System Maintenance & Support services will include the following activities. The vendor is required to execute APT solution & support services with UCO Bank covering all terms and conditions of this tender.</p> <table border="1"> <thead> <tr> <th>Sl. No.</th><th>Service Area</th><th>Service Level</th></tr> </thead> <tbody> <tr> <td>1</td><td>Monitoring & Log Analysis Services On server and consoles.</td><td> <ul style="list-style-type: none"> • Event / log monitoring the first week of every month. • Availability of relevant logs for last 3 months. • Standard / Exception reports. </td></tr> <tr> <td>2</td><td>Server Management (System performance, Policy fine tune and Threat Analysis)</td><td>Monthly check in the first week of every month.</td></tr> <tr> <td>3</td><td>Reports & Dashboard</td><td>Dashboard should give online view of threat identified with their status.</td></tr> </tbody> </table> <p>System Maintenance & Support services will include the following</p>	Sl. No.	Service Area	Service Level	1	Monitoring & Log Analysis Services On server and consoles.	<ul style="list-style-type: none"> • Event / log monitoring the first week of every month. • Availability of relevant logs for last 3 months. • Standard / Exception reports. 	2	Server Management (System performance, Policy fine tune and Threat Analysis)	Monthly check in the first week of every month.	3	Reports & Dashboard	Dashboard should give online view of threat identified with their status.	<p>Part – IV : Section – 1</p> <p>2.6. System Maintenance & Support Services</p> <p>Support – Terms and Conditions: System Maintenance & Support services will include the following activities. The vendor is required to execute APT solution & support services with UCO Bank covering all terms and conditions of this tender.</p> <p>System Maintenance & Support services will include the following activities-</p> <ol style="list-style-type: none"> 24 x 7 online support Issue resolution / Onsite Visits Issue resolution / remote desktop support Issue resolution / telephonic support <p>Any problems/Issues due to APT appliance and console malfunctioning issue and virus outbreak issue identified and reported to the Vendor and if the successful bidder is not able to resolve, then penalty will be imposed on the basis of SLA.</p> <ul style="list-style-type: none"> •The maintenance support should be (24x7x365days) including product upgrades and updates. •The support should be for unlimited requests. It may be provided on email / Telephone /Online. •Direct OEM Service and support should be covered under with dedicated TAM (Technical Account Manager) and onsite support.
Sl. No.	Service Area	Service Level												
1	Monitoring & Log Analysis Services On server and consoles.	<ul style="list-style-type: none"> • Event / log monitoring the first week of every month. • Availability of relevant logs for last 3 months. • Standard / Exception reports. 												
2	Server Management (System performance, Policy fine tune and Threat Analysis)	Monthly check in the first week of every month.												
3	Reports & Dashboard	Dashboard should give online view of threat identified with their status.												

	<p>activities-</p> <p>a. 24 x 7 online support</p> <p>b. Issue resolution / Onsite Visits</p> <p>c. Issue resolution / remote desktop support</p> <p>d. Issue resolution / telephonic support</p> <p>Any problems/Issues due to APT appliance and console malfunctioning issue and virus outbreak issue identified and reported to the Vendor and if the successful bidder is not able to resolve, then penalty will be imposed on the basis of SLA.</p> <ul style="list-style-type: none"> •The maintenance support should be (24x7x365days) including product upgrades and updates. •The support should be for unlimited requests. It may be provided on email / Telephone /Online. •Direct OEM Service and support should be covered under with dedicated TAM (Technical Account Manager) and onsite support. 	
10	<p>Part – II : Invitation for Bids and Instructions to bidders</p> <p>Detail guidelines for MSME bidders:</p>	Please refer to the enclosed Annexure – Q

Annexure – Q

Guidelines for MSME bidders in tenders

The default clauses at MSME site:

- Exemption from submission of EMD shall be given to bidders who are Micro, Small & Medium Enterprises (MSME) and are registered with National Small Scale Industrial Corporation Ltd. (NSIC) under its "Single Point Registration Scheme". The bidder has to submit necessary document issued by NSIC to avail the exemption. To qualify for EMD exemption, firms should necessarily enclose a valid copy of registration certificate issued by NSIC which are valid on last date of submission of the tender documents. MSME firms who are in the process of obtaining NSIC registration will not be considered for EMD exemption. **(Traders are excluded who are engaged in trading activity without value addition/branding/packing. In such a case they will have to submit EMD and Tender Cost).**
- As per Government of India guidelines, there is a special provision for Micro & Small Enterprises owned by Scheduled Castes & Schedule Tribes. Out of 20% target of

annual procurement from Micro & Small Enterprises, a sub-target of 20% (i.e., 4% out of above 20%) shall be earmarked for procurement from Micro & Small Enterprises owned by Scheduled Castes & Schedule Tribe entrepreneurs. Provided that, in the event of failure of such Micro & Small Enterprises to participate in the tender process or meet tender requirements and L1 price, 4% sub-target for procurement earmarked for procurement from Micro & Small Enterprises owned by Scheduled Castes & Schedule Tribe entrepreneurs shall be met from other Micro & Small Enterprises.

(It is clarified that necessary & valid documents should be submitted by the Micro & Small Enterprises and SC/ST Micro & Small Enterprises owners to avail the preference).

Bids received without EMD for bidders not having valid NSIC registered documents for exemption will not be considered.

However, Performance Bank Guarantee has to be submitted by the bidder under any circumstance.

Note:

All other terms and conditions, clauses of the subject RFP remain unchanged. The reply to pre-bid queries responses / clarifications / corrigendum / addendum & changes in the RFP clause mentioned herein above will be part & parcel of the RFP.

Place: Kolkata

Date: 13/09/2018

-----XXX-----