UCO BANK

Department of Information Technology

Request for Proposal (RFP) For RFP for Implementation of Anti-Phishing Managed Services RFP REF NO: UCO/DIT/ANTI-PHISHING /139/2016-17 Date 30/04/2016 Pre-Bid Responses/ Clarifications to Queries raised by the Bidder(s), Amendments, Addendums and Corrigendum's

SL. No.	Page no	Clause No	Terms& Conditions as per RFP	Queries/Suggestions by the Bidder (s)	Bank's Response (s)
1		Part 1. General		What platform needs to be monitored (Web site, cell phone, apps?)	The detailed scope along with web sites are to be given in RFP document.
2	16	Part II: 2.1 Eligibility Criteria	The bidder should be registered as a company in India as per Company Act 1956.	Since the OEM is an international company can we have consortium and bid.?	Clause stands as per RFP
3	16	Part II: 2.1 Eligibility Criteria	The Bidder should have provided Anti-Phishing Managed Services in at least one scheduled commercial bank in India during the last three years. The solution offered should be currently running successfully.	Since the OEM is an international company can we show our global experience	Clause stands as per RFP

4	16	Part II: 2.1 Eligibility Criteria	The bidder should own full-fledged Security Operations Center (SOC) which is operational in India with minimum one active customer for last 1 year as of date of the RFP.	Since the OEM is an international company can an international SOC be accepted?	Clause stands as per RFP
5	16	Part II: 2.1 Eligibility Criteria	The bidder should own full-fledged Security Operations Center (SOC) which is operational in India with minimum one active customer for last 1 year as of date of the RFP.	Is it acceptable to propose Amazon Web Services cloud offering SOC running our cloud solution based in India. Or you would definitely need the bidder/ISV/OEM to have their own SOC in India.	Clause stands as per RFP
6	19	PART – IV: Scope Of Work	Track hosting of phishing sites through digital watermark.	Please clarify point	Phishing sites must be tracked using digital watermark
7	20	PART – IV: Scope Of Work	Monitor Spam traps to detect phishing mails	Do you need a fail proof automated discarding of phishing email spoofing you domain? do you definitely want to stop the delivery of the spoofed emails to your customers mailbox.	The requirement is self - explanatory.
8	20	PART – IV: Scope Of Work	Selected bidder should benchmark Bank's website (3 sites) and suggest controls required to minimize impact from phishing attacks.	What are the 3 sites? Are they primary domains?	Details will be shared with selected bidders
9	20	PART – IV: Scope Of Work	Selected bidder should assist the Bank for coordination with law enforcement agencies like CERT-IN, Banking Ombudsman etc.	What would be the required action?	Clause stands as per RFP

10	20	PART – IV: Scope Of Work	Brand abuse cases	Please clarify? What media would you like us to survey under brand intelligence Any specifics?(LinkedIn, FaceBook, etc ?)	Clause stands as per RFP
11	20	PART – IV: Scope Of Work	The vendor should provide anti malware services for UCO Bank's websites (Twenty sites) to promptly detect the insertion of malicious codes in Bank's web pages. This will include.	What are the 20 sites? Primary domains? Domains that have a login page? Please mentions how many of the domains have login page?	Details will be shared with selected bidders
12	20	PART – IV: Scope Of Work	The Solution should monitor Website for 24x7 basis for any breach of (Confidentiality & Integrity).	Please clarify? Does this mean you need Defacement monitoring?	The requirement is self - explanatory.
13	20	PART – IV: Scope Of Work	24x7 monitoring / scanning of web pages for real-time detection of malware Injection. No skipping of page scanning.	Would you agree in to placing a java code emended inside your web page?	The requirement is self-explanatory.
14	20	PART – IV: Scope Of Work	Real-time alert via tel. call / SMS and Email in case of Malicious Mobile Code (MMC)attack /defacement.	Please Clarify	The requirement is self - explanatory.
15	49	Ann-I	Take down charges per site shall be arrived by dividing the rates quoted in item no. 3 above by 150.	We understand that there is a requirement for 150 take-downs. Please confirm that is per year? Please can you also confirm if this is an estimate or what you currently use?	The number of 150 sites will be consider for calculation. Actual site may vary.

16	19	4.1.1	Selected Bidder should have 24x7 support to protect Banks Internet Banking customers from "Phishing" on Real time basis. Bidder should alert the Bank immediately in the event of Phishing attacks. The selected bidder should respond within 15 min upon detection of phishing attack and should work to shut down/take down the phishing site, anywhere in the world, within reasonable time and submit the report to the Bank.	This is contradicting with the query over the line •" Page 29 section 5.16 Resolution of the incident within 180 minutes" over reasonable time frame Please confirm as no OEM is providing SLA for takedown time	There is 15 Minute (response time) and 60 Minutes(Resolution time) take down time.
17	19	4.1.2	The bidder should ensure bringing down the reactivated phishing site at earliest which was earlier detected as phishing site. If the same site becomes active again within a period of 180 days of its taking down, it should not be treated as a new incident and should be taken down as part of original incident.	Assumption is "same site" refers to the same URL as previously detected. Please confirm.	RFP Clause is self-explanatory
18	19	4.1.19	Monitor spoofed email ids that may be used for sending emails to the customers of the Bank	Please confirm if this means that the service provider has to identify the email address used for sending spam emails to the customer. This is primarily catered by Anti-Spam solution and falls beyond the scope of Anti-Phishing.	Clause stands as per RFP

19	20	4.1.17	Brand Abuse cases	Our assumption is the brand abuse is relative to the Phishing websites where UCO Bank's brand is represented. Please confirm.	Clause stands as per RFP
20	20	4.1	There is no confirmation on number of domain to be under anti-phishing	Please confirm the exact number of domain	Please refer the RFP document
21	44	Annexure G , Point 1	Bidder should possess experience in 24x7x365 Phishing monitoring and implementation of real time detection mechanisms and alerts, during the last three years in 3 financial institutions in India, of which one should be a scheduled commercial bank in India.	Request to consider experience of non Financial Institutions also with atleast 1 Schedule Bank. Hence the clause may be diluted as: Bidder should possess experience in 24x7x365 Phishing monitoring and implementation of real time detection mechanisms and alerts, during the last three years in 3 public/private company/ institutions in India, of which one should be a scheduled commercial bank in India.	Clause stands as per RFP
22	44	Annexure G, point 2	Bidder should have experience in taking down Phishing sites anywhere in the world, during the last three years in 3 financial institutions in India, of which one should be a scheduled commercial bank in India.	Request to consider experience of non Financial Institutions also with atleast 1 Schedule Bank. Hence the clause may be diluted as: Bidder should have experience in taking down Phishing sites anywhere in the world, during the last three years in 3 public/private company/ institutions in India, of which one should be a scheduled commercial bank in India.	Clause stands as per RFP

23	44	Annexure G , Point 3	Should possess experience in implementation of referrer log analysis of web server, monitoring similar domain name registration and monitoring spam traps for detecting phishing mails, during the last three years in 3 financial institutions in India, of which one should be a scheduled commercial bank in India.	Request to consider experience of non Financial Institutions also with atleast 1 Schedule Bank. Hence the clause may be diluted as:Should possess experience in implementation of referrer log analysis of web server, monitoring similar domain name registration and monitoring spam traps for detecting phishing mails, during the last three years in 3 public/private company/ institutions in India, of which one should be a scheduled commercial bank in India.	Clause stands as per RFP
24	18	3.1.2	The bidder needs to achieve a cut-off score of 100 % marks in order to qualify for the commercial evaluation stage.	What is the Cut-off marks to be obtained by the bidder? Request you to consider 60% of cut-off	Clause stands as per RFP
25	44-46	3.1.2	…..three years in 3 financial institutions in India……	Request to dilute the clause to: in 3 public/private company/ institutions in India	Clause stands as per RFP
26		**Corrigendum**	**Last date of Bid Submission is on 20/05/2016 at 03:00 PM and opening of Technical Bid is on 20/05/2016 at 03:30 PM.**		**Last date of Bid Submission date is extended upto 24/05/2016 at 03:00 PM and opening of Technical Bid is on 24/05/2016 at 03:30 PM.**