Selection of vendor for implementation & support of End User Security(DLP / Encryption & Email Security) - RFP NO: CO: BFSL/SYS RFP/20-21/04

Dated : 4th Aug, 2020

Pre-Bid Responses Dated 28.08.2020

Sr. No.	Pg No	Point No	BFSL Clause	Clarification	Request for Change / Modification / Addition / Deletion	BFSL Comments/Clarification
1	10	3.0 Scope of Work	Email Protection : Solution which will prevents email spam, viruses via email, malware, malicious links, phishing attacks, spoofing and other email borne malicious threats and visibility into all messages. Outbound controls include encryption and data loss prevention, while continuity capabilities ensure business communications can continue as normal in the event of an email outage. Robust reporting and email tracking/tracing. For detailed requirement refer Annexure E	What is the email solution used , is it Office 365 / Exchange or both. Request you to clarify the same so that we will accordingly design the solution and right product	NA	Office 365 Enterprise
2	10	3.0 Scope of Work	Encryption Solution : Tool capable to encrypt content immediately as it is created.Synchronized Encryption proactively will protects our data by continuously validating the user, application, and security integrity of a device before allowing access to encrypted data. Full disk encryption using Windows BitLocker. Seamlessly manage keys and recovery functions. Intended to use only on laptops at our locations to secure sensitve data. For detailed requirement refer Annexure G	Please clarify the following: 1. Encryption solution is required only for Laptops or any other technologies such as Database, Storage etc.. 2. It is mentioned that Device integrity also needs to be checked, this cannot be achieved through the encryption solution. Please let us know if we need to provision other solution than Encryption		Encryption is only required on the laptops and the count for 1st year to be considered as 350 / 2nd year 550 / 3rd Year 725. Please refer Addendum 04.
3	10	3.0 Scope of Work	Annexure E,F G have been referred in Scope of work	Annexure E,F & G details are not present in the RFP documents	Annexure E,F & G details	Point to be ignored
4	23	7.9 Submission of Bids	All envelopes with RFP response should be submitted to the authorized person at the address given in Section 1.4–Important Details (Schedule of Events, contact & communication details etc.)	Requesting you to consider softcopy submission via email considering the COVID crises	Requesting you to consider softcopy submission via email considering the COVID crises	Please refer Addendum 03 towards Guidelines for submitting online bids
5	6	1.7 Important Details	Last date & time for submission of Bids : 25th Aug 2020, 3 PM	Requesting you to consider submission timelines as 31st Aug	Requesting you to consider submission timelines as 31st Aug	Request rejected as of now
6	1	Annexure 02 – Credential Strengths	d. Credentials for under implementation projects will not be considered	Requesting you to consider credentials for ongoing projects as we will have implementation support for longer duration for 3 years	Requesting you to consider credentials for ongoing projects as we will have implementation support for longer duration for 3 years	Rejected
7		1.7 Important Details	EMD	Requesting you to share NEFT account number for DD		Please refer Addendum 03 towards Guidelines for submitting online bids

8	9	2.1 Application	The scope of works in the Request for Proposal (RFP) for the [RFP for Selection of vendor for implementation & support of End User Security (DLP / Encryption & Email Security)] would include but not be limited to providing service/solution for [RFP for Selection of vendor for implementation & support of End User Security (DLP / Encryption & Email Security)] and its maintenance and support for the tenure of the Contract.	Detailed Scope of Work not inlcuded in RFP	Kindly share the detailed SOW included in this project	Expectation from Bidder 1) L1 resource 2) 3 Years Managed Support 3) End to End Management. We are looking complete Managed Services for end user security , bidder are responsible for complete management of All Security tools should be managed Properly and a dash board to be shared to Management , Bidder need to put one resource at Bob Financial SIte with additional Cost along with Back to back L2 and L3 Support .
9	10	2.4 Training	The Vendor is required to provide training to the Company's [Please include details of the team requiring Training] teams on the proposed [RFP for Selection of vendor for implementation & support of End User Security (DLP / Encryption & Email Security)], provide a training schedule and furnish training details as per the RFP requirements at all major locations.	Kindly confirm the detail Agenda of Training . Also confirm the locatio of training and no of people join the training	Training will be done on a "Train the Trainer" concept. This will be done to only the Trainer team, if online or at the BOB Head office. Also Bank has to clarify on how many days of effort this will take (need to include any reserve trainings if needed). How many people will involved in Training.	Agenda will be operational knowhow/Finetuning/Product Features of the products and KT for first level trouble shooting. Helpdesk Team & BFSL IT Team members
10	15	6.2	The prices and other terms offered by vendors must be firm for an acceptance period of 180 days from the opening of the commercial bid.	Please make the period as 90 days	The prices and other terms offered by vendors must be firm for an acceptance period of 90 days from the opening of the commercial bid.	Rejected
11	31	9	Payment terms	Payment terms are not mentioend clearly	Kindly clarify on how the payment will be release. The percentage of payment release as per task. 100% payment should be released for licenses agains the delivery of licenses.	Payment of 60 % Upon delivery of the product software/Licenses and remaining on completion of implementation. This will be applied to every individual product being procured

12	17	6.5	By submitting the bid, the Bidder represents and acknowledges to the Company that it possesses necessary experience, expertise and ability to undertake and fulfill its obligations, under all phases involved in the performance of the provisions of this RFP. The Bidder represents that all services supplied in response to this RFP shall meet the proposed RFP for Selection of vendor for implementation & support of End User Security (DLP / Encryption & Email Security) requirements of the Company. The Bidder shall be required to independently arrive at a Solution, which is suitable for the Company, after taking into consideration the effort estimated for implementation of the same. If any services, functions or responsibilities not specifically described in this RFP are an inherent, necessary or customary part of the deliverables or services and are required for proper performance or provision of the deliverables or services in accordance with this RFP, they shall be deemed to be included within the scope of the deliverables or services, as if such	Bidder will execute the task as per mentioned in the SOW and Projest Scope. Anything apart from SOW and Project Scopw will be chargeable at actuals.	Bidder will execute the task as per mentioned in the SOW and Projest Scope. Anything apart from SOW and Project Scopw will be chargeable at actuals.	Accepted. Read it as any additional requirement of manpower/Licenses & Software apart from the existing RFP requirements will be out of scope and seperately chargeable.
13	19-20	6.6-9	Right to Alter requirements – Company reserves the right to alter the requirements specified in the RFP. Company also reserves the right to delete one or more items from the list of items specified in the RFP. Company will inform all Bidders about changes, if any. The Bidder agrees that Company has no limit on the additions or deletions on the items for the period of the contract. Further the Bidder agrees that the prices quoted by the Bidder would be proportionately adjusted with such additions or deletions in quantities. The Company will have the right to increase or decrease any quantities in the bid and the unit/pro-rata rates would be applicable for such alterations in quantities till the period of the contract.	The Prices we will quote depend upon the qty mentioend in the RFP. IN case the Qty chenges or alter, it will also affet the pricing of the product	The Prices we will quote depend upon the qty mentioend in the RFP. IN case the Qty changes or alter, it will also affect the pricing of the product	Rejected. Also have shared that since this is pandemic situation we cannot commit for additional or 2nd & 3rd Year requirement. Details for the mentioned period are estimates.The first Year count given will be confirmed at the time of order release and Bidder will be given PO as Mention in the List however 2nd and 3r year will be on need basis there is no Commitment

14	23	7.6	The bids shall remain valid for a period of 180 days from the last date of submission of bids. All responses including commercial and technical bids would be deemed to be irrevocable offers/proposals from the Bidders and shall, if accepted by Company, form part of the final contract between Company and the selected Bidder. Company may seek further extensions of the bid validity, if required.	Please make the validity period as 90 days	The bids shall remain valid	Rejected
15		General	Regarding the Payment of Tender fee and EMD/BG	Please clarify if online payment us possible and share the Account details with IFSC Code and Beneficialry name to make online transfer of Tender fee and EMD/BG amount	Considering the Pandemic situation, please share the please give us an option of online money trasfer. Please share the Account details with IFSC Code and Beneficialry name to make online transfer of Tender fee and EMD/BG amount	Please refer Addendum 03 towards Guidelines for submitting online bids
16		General	Regarding the Delivery timeline of Project	Delivery time of project is not mentioned in the RFP/	Please clarify on the licenses delivery timeline and project delivery timline.	T + 6 Weeks
17	Appendix1(DLP)	1	The agent should Monitor content traversing across the endpoint by I/O channel (bus, Bluetooth, LPT, etc.)	Need to know why LPT is required. Does the bank use LPT port printers ??	Request to modify this point & remove LPT if not required.	LPT not to be considered
18	Appendix1(DLP)	22	It should have the ability to disover data in online and offline mode	Need clarity on what is meant by online & offiline discovery mode. Does this relate to discovery when agent is connected or in a disconnected state ??		Currently we are not implementing DFA, however the tool should have a discovery capablity and suggested to have it in online and offline mode.
19	Appendix1(DLP)	25	The solution should have the capability to do OCR detection & prevention for Email & Web	What is the proxy solution that the bank is using ?? Does is support ICAP.		Fortifgate FW using as proxy. ICAP supports.
20	Appendix1(DLP)	27	The solution should be capable of extending to the cloud if required without deploying full CASB.	What are the cloud applications that the bank is looking to extend the DLP to. Pls provide full details of the same.		No Cloud Application as of now. CASB not required
21	Appendix1(DLP)	28	The solution should be supported to be deployed in IAAS rather then on-prem if required.	What IAAS platform does the bank plan to use ??		No Plan to use IAAS
22	Appendix1(DLP)	41	Solution should have capability to integrate with data classification and tagging solutions such as Titus, Boldon James and other natively available in cloud services such as Box and Office365.	Request the bank to mention if possible the classification solution that needs to be integrated with.		DFA is not to be implemented in the first phase but the solution should have capability
23	Appendix1(Email Security)	3	Solution should possibly be able integrate with MS O365 seamlessly for implementing the Email Security/Email DLP Solution.	The bank will have to provide infra in azure. Is the flexible at doing the same		This is opex based hence any infra cost required should for procurement and maintenance should be borne by Bidder

24	Appendix1(Email Security)	5	Solution should have option to Delete/ Quarantine or Move detected emails to Junk Folder	Once the email is quarantined, the user is notified & the end user has the option to release the email	Request to remove this point & make it optional to move the mail to the Junk folder. Important is to quarantine & provide the capability to access/realease email which is provided. Moving it to junk folder is a risky action.	Emails should be Quarantined
25	Appendix1(Email Security)	6	Solution should have complete analysis and reasoning of spear phishing email and why it is detected by the solution	Request bank to provide clarity on what is required as part of analysis & reasoning details here.	The Solution detects phishing email. There is no reason provided, request to remove this point. However we can provide end user education on phishing emails.	The bidder should provide all required details for Investigation purpose as and when required
26	Appendix1(Email Security)	25	In case of incidents like security breaches, the solution should support to notify Bank on real time basis	Need expectation as what is expected as part of the realtime notification.	Alerts, notifications around the availability of the cloud service are available to the customer. What is extra required apart from this.	H1/L1 Bidder will share the additional cost of L1 support who will be placed at BFSL premises for the contract service period and L2/L3 support will be provided by the OEM or SME Team. L1 will be responisible for monitoring alerts/incidents on all the products put together. Also read the read the statement as "Security Incidents" instead of "Security Breaches".
27	Appendix1(Email Security)	26	No data should be kept outside the boundaries of India at any point of time.	As part of the solution, only user information from the AD is synced back to the cloud service??	Is the bank fine with sending this data outside of india. This is non financial data.	Data center should be in India for services from where services being availed for product
28	Appendix1(Email Security)	26	No data should be kept outside the boundaries of India at any point of time.	The Email is quarantined & then is destroyed when the quarantine mail is released.	Is the bank find with this approach?? Apart from this there is no email data stored on the cloud service.	Data center should be in India for services from where services being availed for product
29	Appendix1(Email Security)	27	A clear demarcation should be available for the data hosted by the Bank in the cloud, with the data of other organizations/customers.	How is the cloud service provider expected to show this demarcation	Pls provide the required clarity	Data center should be in India for email Gateway
30	Appendix1(Email Security)	26	No data should be kept outside the boundaries of India at any point of time.	The Email is quarantined & then is destroyed when the quarantine mail is released.	Is the bank open to using on-prem email security solution if even AD data & quarantined mail should not be taken outside of India?? Pls provide the required clarity	Data center should be in India for services from where services being availed for product
31	Appendix1(Email Security)	31	The solution should Conform to Bank's IT/IS policy guidelines, RBI Cyber Security Policy & other relevant Guidelines, IDRBT & Cert-In recommendations/ guidelines during the entire Contract Period.	Banks needs to share this point & a blanket compliance cannot be agreed to. Request to remove this point.	Request to mention this points in the RFP as blanket conformation to regulations cannot be practically be provided	Accepted to remove partially. Except sections of ISO27001 policies and configuration needs to be carried out by the partner once the policy framework is ready.
32	Appendix1(Email Security)	33	Bank has right to audit the data centres/premises where-in the proposed solution is hosted or bank's data is kept/to seek latest IT/IS audit reports /audit certificates by reputed Security auditors / regulators.	OEM maintains its certifications as per their security requirements whichh are published & updated from time to time. We ask to remove this point of physical audit.	Is the bank fine with this approach?	The required certification should be available from the bidder as and when required.

33	Appendix1(Email Security)	35	Allow the Reserve Bank of India or persons authorized by it online/ in person to access the bank's documents, records of transactions, and other necessary information given to, stored or processed by the service provider within a reasonable time. This includes information maintained in paper and electronic formats with prior permission of the Bank.	Most of the information is in electronic format & maintained by the bank itself	What additional information is required?	The required certification should be available from the bidder as and when required.
34	SLA (Page no 13)	4	The bank has asked for the resolution time SLA	While the response time can be provided. Resolution cannot be guaranteed	Request the bank to edit this point & remove the SLA resolution time requirement.	99% for Platform Availability and Notification Systems SLA
35	Payment Terms(Pno 31)			Need Clarification on Payment terms	90% payment to be made against delivery and remaining 10% against installation and Sign Off	Payment of 60 % Upon delivery of the product software/Licenses and remaining on completion of implementation. This will be applied to every individual product being procured
36	Eligibility Criteria		The Bidder should have at least One year' experience in implementation/support of end user security solutions and should have implemented End User Security (DLP / Encryption & Email Security) in one Bank / Financial Institutions in India	Please clarify in End user security Solutions whether the RFP ask is either DLP or Encryption or Email Security.	The bids shall remain valid for a period of 90 days from the last date of submission of bids. All responses including commercial and technical bids would be deemed to be irrevocable offers/proposals from the Bidders and shall, if accepted by Company, form	The bidder should have experience in all three technology at least 2 in BFSI segment
37	General Queries			Please advise whether the said solution can be deployed centrally.Whether BOB Financial will provide central console to deploy the solution centrally.		Remotle implementation will be done by remote tools available with BFSL , In case issue hands and legs support will be provided by BFSL
38	General Queries			Whether onsite engineer is required for Facility Management		H1/L1 Bidder will share the additional cost of L1 support who will be placed at BFSL premises for the contract service period and L2/L3 support will be provided by the OEM or SME Team. L1 will be responisible for monitoring alerts/incidents on all the products put together. Also read the read the statement as "Security Incidents" instead of "Security Breaches".
39	General Queries			HW for deploying the licenses of the said solution if required will be provided by BOB Financial or Bidder needs to incorporate in the solution		Partner to take care of cost of support and also take care of maintenance of any additional resources
40	6	1.7 Important Details (Schedule of Events, contact & communication details etc.)	10. Bid document cost (non-refundable) - INR 5000/-	As per MSME/NSIC, exemptions are given to MSME bidders on Bid cost	We request you to provide exemptions on bid cost for MSME bidders as this clause is not applicable to us.	Accepted as per MSME Exemption

41	7	1.7 Important Details (Schedule of Events, contact & communication details etc.)	Bid Security (EMD) INR 200000/-	As per MSME/NSIC exemptions are given for MSME bidders on EMD	We request you to provide exemptions on bid cost for MSME bidders as this clause is not applicable to us.	Accepted as per MSME Exemption but No exemption on PBG.
42		ANNEXURE A1 – ELIGIBILITY CRITERIA, (B) Bidder Qualification Criteria, (B1)	The bidder should be a Company Registered under Company act and should be in business for at least five (5) years as on March 31, 2020.		We request you to revise it to 4 years 5 months. However the company is encororporated in 2003, later it converted into Pvt ltd and completed 5 years on 4th Aug 2020 i.e on the same day this RFP published on your portal. Additionally as per MSME clause and start up logevity of business is excluded	Accepted basis of review of MSMSE document
43		ANNEXURE A1 – ELIGIBILITY CRITERIA, (B) Bidder Qualification Criteria, (B2)	The bidder should have a minimum average annual turnover of at least Rs.50 Lacs over the last three (3) years	We have more turnover than expected in the RFP but as MSME/NSIC/GOI MSME exempted from turnover criteria.	We have more turnover than expected in the RFP but as MSME/NSIC/GOI MSME exempted from turnover criteria.	Accepted basis of review of MSMSE document
44		ANNEXURE A1 – ELIGIBILITY CRITERIA, (B) Bidder Qualification Criteria, (B3)	The Bidder should have at least One year' experience in implementation/support of end user security solutions and should have implemented End User Security (DLP / Encryption & Email Security) in one Bank / Financial Institutions in India		We request you revise the clause as below: 1) The Bidder or OEM, should have at least One year' experience in implementation/support of end user security solutions and should have implemented End User Security (DLP / Encryption & Email Security) in one Bank / Financial Institutions in India. 2) As per MSMED act 2006/NSIC/IOE/DPIIT exemptions granted under MSME by govt we are exempted from any prior experience, so this clause is not applicable to us. 3) In order to substantiate our claim we have attached the related documents for your reference.	No Change in the RFP terms for MSME exemption will be applicable on submission of documents.

45		ANNEXURE A1 – ELIGIBILITY CRITERIA - Additional clause or suggestion:			As per public procurement policy 2017, 2019 and DPIIT revised norms any tender which is below 200 cr published in India should deal and give preference to MSME and Made In India Product/Solution. Therefore we request you to add Make In India Clause in addendum/corrigendum.	We require License
46		ANNEXURE A1 – ELIGIBILITY CRITERIA - Additional clause or suggestion:			At any point of time if BFSL need any documents in order to substantiate our claims please let us know so we can provide the same from PSU/Banks/Govt/private entities	OK
47	31	9.0. Payment Terms		Payment release period is mentiond under payment terms.	Payment release period is mentiond under payment terms.	Payment of 60 % Upon delivery of the product software/Licenses and remaining on completion of implementation. This will be applied to every individual product being procured
48	10	3.0. Scope of Work		Please suggest timelines of implementation	Please suggest timelines of implementation	T + 6 Weeks
49	Appendix1(DLP)	1	The agent should Monitor content traversing across the endpoint by I/O channel (bus, Bluetooth, LPT, etc.)	Need to know why LPT is required. Does the bank use LPT port printers ??	Request to modify this point & remove LPT if not required.	LPT not to be considered
50	Appendix1(DLP)	22	It should have the ability to disover data in online and offline mode	Need clarity on what is meant by online & offiline discovery mode. Does this relate to discovery when agent is connected or in a disconnected state ??		Currently we are not implementing DFA, however the tool should have a discovery capablity and suggested to have it in online and offline mode.
51	Appendix1(DLP)	25	The solution should have the capability to do OCR detection & prevention for Email & Web	What is the proxy solution that the bank is using ?? Does is support ICAP.		Fortifgate FW using as proxy. ICAP supports.
52	Appendix1(DLP)	27	The solution should be capable of extending to the cloud if required without deploying full CASB.	What are the cloud applications that the bank is looking to extend the DLP to. Pls provide full details of the same.		No Cloud Application as of now. CASB not required
53	Appendix1(DLP)	28	The solution should be supported to be deployed in IAAS rather then on-prem if required.	What IAAS platform does the bank plan to use ??		No Plan to use IAAS
54	Appendix1(DLP)	41	Solution should have capability to integrate with data classification and tagging solutions such as Titus, Boldon James and other natively available in cloud services such as Box and Office365.	Request the bank to mention if possible the classification solution that needs to be integrated with.		DFA is not to be implemented in the first phase but the solution should have capability
55	Appendix1(Email Security)	3	Solution should possibly be able integrate with MS O365 seamlessly for implementing the Email Security/Email DLP Solution.	The bank will have to provide infra in azure. Is the flexible at doing the same		This is opex based hence any infra cost required should for procurement and maintenance should be borne by Bidder

56	Appendix1(Email Security)	5	Solution should have option to Delete/ Quarantine or Move detected emails to Junk Folder	Once the email is quarantined, the user is notified & the end user has the option to release the email	Request to remove this point & make it optional to move the mail to the Junk folder. Important is to quarantine & provide the capability to access/realease email which is provided. Moving it to junk folder is a risky action.	Emails should be Quarantined
57	Appendix1(Email Security)	6	Solution should have complete analysis and reasoning of spear phishing email and why it is detected by the solution	Request bank to provide clarity on what is required as part of analysis & reasoning details here.	The Solution detects phishing email. There is no reason provided, request to remove this point. However we can provide end user education on phishing emails.	The bidder should provide all required details for Investigation purpose as and when required
58	Appendix1(Email Security)	25	In case of incidents like security breaches, the solution should support to notify Bank on real time basis	Need expectation as what is expected as part of the realtime notification.	Alerts, notifications around the availability of the cloud service are available to the customer. What is extra required apart from this.	H1/L1 Bidder will share the additional cost of L1 support who will be placed at BFSL premises for the contract service period and L2/L3 support will be provided by the OEM or SME Team. L1 will be responisible for monitoring alerts/incidents on all the products put together. Also read the read the statement as "Security Incidents" instead of "Security Breaches".
59	Appendix1(Email Security)	26	No data should be kept outside the boundaries of India at any point of time.	As part of the solution, only user information from the AD is synced back to the cloud service??	Is the bank fine with sending this data outside of india. This is non financial data.	Data center should be in India for services from where services being availed for product
60	Appendix1(Email Security)	26	No data should be kept outside the boundaries of India at any point of time.	The Email is quarantined & then is destroyed when the quarantine mail is released.	Is the bank find with this approach?? Apart from this there is no email data stored on the cloud service.	Data center should be in India for services from where services being availed for product
61	Appendix1(Email Security)	27	A clear demarcation should be available for the data hosted by the Bank in the cloud, with the data of other organizations/customers.	How is the cloud service provider expected to show this demarcation	Pls provide the required clarity	Data center should be in India for email Gateway
62	Appendix1(Email Security)	26	No data should be kept outside the boundaries of India at any point of time.	The Email is quarantined & then is destroyed when the quarantine mail is released.	Is the bank open to using on-prem email security solution if even AD data & quarantined mail should not be taken outside of India?? Pls provide the required clarity	Data center should be in India for services from where services being availed for product
63	Appendix1(Email Security)	31	The solution should Conform to Bank's IT/IS policy guidelines, RBI Cyber Security Policy & other relevant Guidelines, IDRBT & Cert-In recommendations/ guidelines during the entire Contract Period.	Banks needs to share this point & a blanket compliance cannot be agreed to. Request to remove this point.	Request to mention this points in the RFP as blanket conformation to regulations cannot be practically be provided	Accepted to remove partially. Except sections of ISO27001 policies and configuration needs to be carried out by the partner once the policy framework is ready.
64	Appendix1(Email Security)	33	Bank has right to audit the data centres/premises where-in the proposed solution is hosted or bank's data is kept/to seek latest IT/IS audit reports /audit certificates by reputed Security auditors / regulators.	OEM maintains its certifications as per their security requirements whichh are published & updated from time to time. We ask to remove this point of physical audit.	Is the bank fine with this approach?	The required certification should be available from the bidder as and when required.

65	Appendix1(Email Security)	35	Allow the Reserve Bank of India or persons authorized by it online/ in person to access the bank's documents, records of transactions, and other necessary information given to, stored or processed by the service provider within a reasonable time. This includes information maintained in paper and electronic formats with prior permission of the Bank.	Most of the information is in electronic format & maintained by the bank itself	What additional information is required?	The required certification should be available from the bidder as and when required.
66	SLA (Page no 13)	4	The bank has asked for the resolution time SLA	While the response time can be provided. Resolution cannot be guaranteed	Request the bank to edit this point & remove the SLA resolution time requirement.	99% for Platform Availability and Notification Systems SLA
67	Appendix1(DLP)	1	The agent should Monitor content traversing across the endpoint by I/O channel (bus, Bluetooth, LPT, etc.)	Need to know why LPT is required. Does the bank use LPT port printers ??	Request to modify this point & remove LPT if not required.	LPT not to be considered
68	Appendix1(DLP)	22	It should have the ability to disover data in online and offline mode	Need clarity on what is meant by online & offiline discovery mode. Does this relate to discovery when agent is connected or in a disconnected state ??		Currently we are not implementing DFA, however the tool should have a discovery capablity and suggested to have it in online and offline mode.
69	Appendix1(DLP)	25	The solution should have the capability to do OCR detection & prevention for Email & Web	What is the proxy solution that the bank is using ?? Does is support ICAP.		Fortifgate FW using as proxy. ICAP supports.
70	Appendix1(DLP)	27	The solution should be capable of extending to the cloud if required without deploying full CASB.	What are the cloud applications that the bank is looking to extend the DLP to. Pls provide full details of the same.		No Cloud Application as of now. CASB not required
71	Appendix1(DLP)	28	The solution should be supported to be deployed in IAAS rather then on-prem if required.	What IAAS platform does the bank plan to use ??		No Plan to use IAAS
72	Appendix1(DLP)	41	Solution should have capability to integrate with data classification and tagging solutions such as Titus, Boldon James and other natively available in cloud services such as Box and Office365.	Request the bank to mention if possible the classification solution that needs to be integrated with.		DFA is not to be implemented in the first phase but the solution should have capability
73	Appendix1(Email Security)	3	Solution should possibly be able integrate with MS O365 seamlessly for implementing the Email Security/Email DLP Solution.	The bank will have to provide infra in azure. Is the flexible at doing the same		This is opex based hence any infra cost required should for procurement and maintenance should be borne by Bidder
74	Appendix1(Email Security)	5	Solution should have option to Delete/ Quarantine or Move detected emails to Junk Folder	Once the email is quarantined, the user is notified & the end user has the option to release the email	Request to remove this point & make it optional to move the mail to the Junk folder. Important is to quarantine & provide the capability to access/realease email which is provided. Moving it to junk folder is a risky action.	Emails should be Quarantined
75	Appendix1(Email Security)	6	Solution should have complete analysis and reasoning of spear phishing email and why it is detected by the solution	Request bank to provide clarity on what is required as part of analysis & reasoning details here.	The Solution detects phishing email. There is no reason provided, request to remove this point. However we can provide end user education on phishing emails.	The bidder should provide all required details for Investigation purpose as and when required

76	Appendix1(Email Security)	25	In case of incidents like security breaches, the solution should support to notify Bank on real time basis	Need expectation as what is expected as part of the realtime notification.	Alerts, notifications around the availability of the cloud service are available to the customer. What is extra required apart from this.	H1/L1 Bidder will share the additional cost of L1 support who will be placed at BFSL premises for the contract service period and L2/L3 support will be provided by the OEM or SME Team. L1 will be responisible for monitoring alerts/incidents on all the products put together. Also read the read the statement as "Security Incidents" instead of "Security Breaches".
77	Appendix1(Email Security)	26	No data should be kept outside the boundaries of India at any point of time.	As part of the solution, only user information from the AD is synced back to the cloud service??	Is the bank fine with sending this data outside of india. This is non financial data.	Data center should be in India for services from where services being availed for product
78	Appendix1(Email Security)	26	No data should be kept outside the boundaries of India at any point of time.	The Email is quarantined & then is destroyed when the quarantine mail is released.	Is the bank find with this approach?? Apart from this there is no email data stored on the cloud service.	Data center should be in India for services from where services being availed for product
79	Appendix1(Email Security)	27	A clear demarcation should be available for the data hosted by the Bank in the cloud, with the data of other organizations/customers.	How is the cloud service provider expected to show this demarcation	Pls provide the required clarity	Data center should be in India for email Gateway
80	Appendix1(Email Security)	26	No data should be kept outside the boundaries of India at any point of time.	The Email is quarantined & then is destroyed when the quarantine mail is released.	Is the bank open to using on-prem email security solution if even AD data & quarantined mail should not be taken outside of India?? Pls provide the required clarity	Data center should be in India for services from where services being availed for product
81	Appendix1(Email Security)	31	The solution should Conform to Bank's IT/IS policy guidelines, RBI Cyber Security Policy & other relevant Guidelines, IDRBT & Cert-In recommendations/ guidelines during the entire Contract Period.	Banks needs to share this point & a blanket compliance cannot be agreed to. Request to remove this point.	Request to mention this points in the RFP as blanket conformation to regulations cannot be practically be provided	Accepted to remove partially. Except sections of ISO27001 policies and configuration needs to be carried out by the partner once the policy framework is ready.
82	Appendix1(Email Security)	33	Bank has right to audit the data centres/premises where-in the proposed solution is hosted or bank's data is kept/to seek latest IT/IS audit reports /audit certificates by reputed Security auditors / regulators.	OEM maintains its certifications as per their security requirements whichh are published & updated from time to time. We ask to remove this point of physical audit.	Is the bank fine with this approach?	The required certification should be available from the bidder as and when required.
83	Appendix1(Email Security)	35	Allow the Reserve Bank of India or persons authorized by it online/ in person to access the bank's documents, records of transactions, and other necessary information given to, stored or processed by the service provider within a reasonable time. This includes information maintained in paper and electronic formats with prior permission of the Bank.	Most of the information is in electronic format & maintained by the bank itself	What additional information is required?	The required certification should be available from the bidder as and when required.
84	SLA (Page no 13)	4	The bank has asked for the resolution time SLA	While the response time can be provided. Resolution cannot be guaranteed	Request the bank to edit this point & remove the SLA resolution time requirement.	99% for Platform Availability and Notification Systems SLA
85	RFP	14	Penalty Capping	The penalty shall be calculated on total quarterly payment The total quarterly deduction should not exceed 7%	Request you to cap the penalty at 5%	Rejected

86	RFP	31	Payment Terms	The commercial bid submitted by the bidder must be in conformity with the payment terms proposed by the Company	Kindly specify the payment terms or confirm that the payment terms proposed by vendor would be accepted	Payment of 60 % Upon delivery of the product software/Licenses and remaining on completion of implementation. This will be applied to every individual product being procured
87	Encryption	4	The Product should allow the administrator to customize the Pre-Boot environment to tailor the UI to, for example, corporate graphics and/or custom messages.	We use Windows native encryption to authenticate the user. Using Native encryption does not allow to change or modify the UI and any other authentication process. Native Encryotion is the fastest as it is windows native service	Request you to delete the clause	Clause can be removed
88	Encryption	5	The Solution should features a boot manager that can be enabled from the administrative console, thus allowing the user to choose which partition to boot from.	Need clarification. Full disk encryption encrypts entire drive. Our solution automcatically detects the boot partition and encrypts the data and no manual intervention is needed	Request you to ammend it to "The Solution should features a boot manager that can be enabled from the administrative console"	No change
89	Encryption	9	The product should have achieved EAL 4 certification along with FIPS 140-1 and 140-2 validations.	EAL4+, FIPS are certication mostly for hardware based Soltuion. Encryption is complete Software and does not to be Common Criteria certified	EAL4+, FIPS are certication mostly for hardware based Soltuion. Encryption is complete Software and does not to be Commin Criteria certified	Good to have option
90	Encryption	14	The Solution should support for multifactor authentication, including: smart-cards, biometrics, and RSA tokens for the use in end user authentication	Authentication is enabled for POA. Additionally the user also has to enter his domain credentials to accrss the data. 2FA is already a part of login process	Request you to ammend it to "The Solution should support for multifactor authentication like POA & Windows authentication"	Good to have option
91	Encryption	15	The Solution should support for the encryption of removable media. (floppy disks, CD/DVDs, flash drives, external hard drives, etc).	Removable Media is blocked in all the organizations today. Allowing removable media possess a risk for the threat to get in the network. Additionally DLP monitors, block all sensitve data to removable drives, so encryption of removable media does not play a vital role for USB's CD's etc	Request you to delete the clause	No change
92	Encryption	16	Full disk encryption (FDE) software should be FIPS 140-2 compliant, or FIPS certified.	EAL4+, FIPS are certication mostly for hardware based Soltuion. Encryption is complete Software and does not to be Common Criteria certified	EAL4+, FIPS are certication mostly for hardware based Soltuion. Encryption is complete Software and does not to be Commin Criteria certified	Good to have option
93	Encryption	17	Full disk encryption (FDE) software should be EAL L4 compliant.	EAL4+, FIPS are certication mostly for hardware based Soltuion. Encryption is complete Software and does not to be Common Criteria certified	EAL4+, FIPS are certication mostly for hardware based Soltuion. Encryption is complete Software and does not to be Commin Criteria certified	Good to have option
94	Encryption	18	The product should prevent access to cached passwords, SAM file, temporary files, and other OS Files at Boot up.	Need clarification. The point does not look like Encryption feature point	Request you to delete the clause	Clause can be removed
95	Encryption	22	The product should provide any form of password synchronization with domains, or to simplify having accounts on multiple machines	Need Clarifcation.		The Product should be synchronized with ADS

96	Email Security	5	Solution should have option to Delete/ Quarantine or Move detected emails to Junk Folder	This feature is provided by the Email hosting provider. We can quarantine/delete or highlight suspected / confirm spam	Request you to ammend the point to "The solution should allow options to Quarintine, deliver, delete, tag subject line for mails identified as confirmed, Bulk or suspected spam emails"	Emails should be Quarantined
97	Email Security	15	Solution should have option to customize the email Alert template	Email alert has a defined format and cannot be customized. The email alertt has all the major information which is not recommended to tamper as it has information related to various attack vectors	Request you to delete the clause	Good to have option
98	Email Security	26	No data should be kept outside the boundaries of India at any point of time.	All the vendors with sandboxing has to share the zero day paylods and the files having no footprint on the cloud - Most of them are outside India. These files generally are the ones with vilnerabiltiy and nothing related to bank data	Request you to ammend it t o "No banking related data should be kept outside the boundaries of India at any point of time"	Data center should be in India for services from where services being availed for product
99	DLP	5	Solution should have option to Delete/ Quarantine or Move detected emails to Junk Folder	This feature is provided by the Email hosting provider. We can quarantine/delete or highlight suspected / confirm spam	Request you to ammend the point to "The solution should allow options to Quarintine, deliver, delete, tag subject line for mails identified as confirmed, Bulk or suspected spam emails"	Emails should be Quarantined
100	DLP	15	Solution should have option to customize the email Alert template	Email alert has a defined format and cannot be customized. The email alertt has all the major information which is not recommended to tamper as it has information related to various attack vectors	Request you to delete the clause	Good to have option
101	DLP	26	No data should be kept outside the boundaries of India at any point of time.	All the vendors with sandboxing has to share the zero day paylods and the files having no footprint on the cloud - Most of them are outside India. These files generally are the ones with vilnerabiltiy and nothing related to bank data	Request you to ammend it t o "No banking related data should be kept outside the boundaries of India at any point of time"	Data center should be in India for services from where services being availed for product
102	16	6.4	EMD 2Lakh need to be submitted	Would there be an exemption of EMD for companies registered with NSIC (The National Small Industries corporation Limited)	Request for an Exemption of EMD for companies registered with NSCI (The National Small Industries corporation Limited)	MSME Exemption
103	Encryption	4	The Product should allow the administrator to customize the Pre-Boot environment to tailor the UI to, for example, corporate graphics and/or custom messages.	We use Windows native encryption to authenticate the user. Using Native encryption does not allow to change or modify the UI and any other authentication process. Native Encryotion is the fastest as it is windows native service	Request you to delete the clause	Clause can be removed

104	Encryption	5	The Solution should features a boot manager that can be enabled from the administrative console, thus allowing the user to choose which partition to boot from.	Need clarification. Full disk encryption encrypts entire drive. Our solution automcatically detects the boot partition and encrypts the data and no manual intervention is needed	Request you to ammend it to "The Solution should features a boot manager that can be enabled from the administrative console"	No change
105	Encryption	9	The product should have achieved EAL 4 certification along with FIPS 140-1 and 140-2 validations.	EAL4+, FIPS are certication mostly for hardware based Soltuion. Encryption is complete Software and does not to be Common Criteria certified	EAL4+, FIPS are certication mostly for hardware based Soltuion. Encryption is complete Software and does not to be Commin Criteria certified	Good to have option
106	Encryption	14	The Solution should support for multifactor authentication, including: smart-cards, biometrics, and RSA tokens for the use in end user authentication	Authentication is enabled for POA. Additionally the user also has to enter his domain credentials to accrss the data. 2FA is already a part of login process	Request you to ammend it to "The Solution should support for multifactor authentication like POA & Windows authentication"	Good to have option
107	Encryption	15	The Solution should support for the encryption of removable media. (floppy disks, CD/DVDs, flash drives, external hard drives, etc).	Removable Media is blocked in all the organizations today. Allowing removable media possess a risk for the threat to get in the network. Additionally DLP monitors, block all sensitve data to removable drives, so encryption of removable media does not play a vital role for USB's CD's etc	Request you to delete the clause	No change
108	Encryption	16	Full disk encryption (FDE) software should be FIPS 140-2 compliant, or FIPS certified.	EAL4+, FIPS are certication mostly for hardware based Soltuion. Encryption is complete Software and does not to be Common Criteria certified	EAL4+, FIPS are certication mostly for hardware based Soltuion. Encryption is complete Software and does not to be Commin Criteria certified	Good to have option
109	Encryption	17	Full disk encryption (FDE) software should be EAL L4 compliant.	EAL4+, FIPS are certication mostly for hardware based Soltuion. Encryption is complete Software and does not to be Common Criteria certified	EAL4+, FIPS are certication mostly for hardware based Soltuion. Encryption is complete Software and does not to be Commin Criteria certified	Good to have option
110	Encryption	18	The product should prevent access to cached passwords, SAM file, temporary files, and other OS Files at Boot up.	Need clarification. The point does not look like Encryption feature point	Request you to delete the clause	Clause can be removed
111	Encryption	22	The product should provide any form of password synchronization with domains, or to simplify having accounts on multiple machines	Need Clarifcation.		The Product should be synchronized with ADS
112	Email Security	5	Solution should have option to Delete/ Quarantine or Move detected emails to Junk Folder	This feature is provided by the Email hosting provider. We can quarantine/delete or highlight suspected / confirm spam	Request you to ammend the point to "The solution should allow options to Quarintine, deliver, delete, tag subject line for mails identified as confirmed, Bulk or suspected spam emails"	Emails should be Quarantined

113	Email Security	15	Solution should have option to customize the email Alert template	Email alert has a defined format and cannot be customized. The email alertt has all the major information which is not recommended to tamper as it has information related to various attack vectors	Request you to delete the clause	Good to have option
114	Email Security	26	No data should be kept outside the boundaries of India at any point of time.	All the vendors with sandboxing has to share the zero day paylods and the files having no footprint on the cloud - Most of them are outside India. These files generally are the ones with vilnerabiltiy and nothing related to bank data	Request you to ammend it t o "No banking related data should be kept outside the boundaries of India at any point of time"	Data center should be in India for services from where services being availed for product
115	DLP	5	Solution should have option to Delete/ Quarantine or Move detected emails to Junk Folder	This feature is provided by the Email hosting provider. We can quarantine/delete or highlight suspected / confirm spam	Request you to ammend the point to "The solution should allow options to Quarintine, deliver, delete, tag subject line for mails identified as confirmed, Bulk or suspected spam emails"	Emails should be Quarantined
116	DLP	15	Solution should have option to customize the email Alert template	Email alert has a defined format and cannot be customized. The email alertt has all the major information which is not recommended to tamper as it has information related to various attack vectors	Request you to delete the clause	Good to have option
117	DLP	26	No data should be kept outside the boundaries of India at any point of time.	All the vendors with sandboxing has to share the zero day paylods and the files having no footprint on the cloud - Most of them are outside India. These files generally are the ones with vilnerabiltiy and nothing related to bank data	Request you to ammend it t o "No banking related data should be kept outside the boundaries of India at any point of time"	Data center should be in India for services from where services being availed for product