Information Technology Division, HO, 5, Sansad Marg, New Delhi – 110 001
Email: itdhw@pnb.co.in Tel: 011-23311452

Response to pre bid queries of RFP for Office 365 Email Security Solutions including Email gateway, Email DLP and Email ATP

Sr. No.	RFP Page No.	RFP Clause Name & No.	RFP Clause	Bidder's Query/Suggestion/Remarks	Bank's Response/clarification
1	10	Email Security & 6	The solution should have features to build scenarios for actions on emails.	Please clarify the scenario meaning , as its generic . Our understanding is different types of filters, Is our understanding correct ?	It is clarified, Scenario means all possible outcomes of situations.
2	10	Email Security & 7	The Solution should have IPV4 and IPV6 dual stack Compatibility.	As the solution will be delivered from the IAAS setup , so IPv4 or IPv6 should not be criteria for network conenction , modify the same to "The Solution should have IPV4 or IPV6 Compatibility"	It is clarified, the access to neither IPV4 nor IPV6 traffic should be dropped, due to incompatibility in the infrastructure. Please be guided by RFP.
3	10	Email Security & 8	The Solution should have APIs/ Connectors / scripts for integration with various security solutions in the bank like ADDM, SMS, SOAR, SIEM, Firewall etc. as applicable and bidder shall enable the requested integration without any additional cost to Bank.	Every OEM will have the integration points "The Solution should have APIs/ Connectors / scripts for integration with various security solutions in the bank like SIEM etc. as applicable and bidder shall enable the requested integration. Also for any specific integration need to be discuss and factor in PS cost"	Please be guided by RFP
4	10	Email Security & 11	The solution should be integrated with the case management solution and incident management solution of the bank.	Each OEM has its own way of integration in our case email notifications can be sent to incident management and case management solution for generating the tickets. Also request you to please provide the details of the Case Management & Incident Management solution used by the bank.	It is clarified, the solution should be integrated with the SIEM so that features of case management and incident management is available through the same for the incidents related to email security.
5	10	Email Security & 16	The Solution should have DR capabilities and functionalities so that the email security can be	Each OEM has its own way of setting the DR capability, This clause is limiting our	The solution should have DR capabilities and functionalities so that the email security is not impacted

			implemented even if email solution is shifted from one setup to another setup. This should be properly configured during implementation.	participation, Hence request you to please amend this clause as: The Solution should have DR capabilities and functionalities so that the email security is not impacted even if email solution is shifted from one setup to another setup. This should be properly configured during implementation.	even if the email or the email security solution is shifted from one set up to another set up. This should be properly configured during the implementation.
6	11	Email Security & 22	The solution virus engine should support scanning by inbound, outbound and internal direction and configure the policy per direction.	Internal Mail scanning requires visiability of email via a MTA and in that case Mail Solution has to route the emails to Mail Security solution via MTA. Kindly confirm if Bank mail solution can do the routing of internal domain mails, if not then please remove the Internal direction from the clause & amend as : The solution virus engine should support scanning by inbound, outbound and configure the policy.	It is clarified, please be guided by Microsoft Office 365 email architecture. The solution virus engine should support scanning by inbound, outbound direction and configure the policy per direction. Bidder should provide suitable solution for scanning internal emails in addition to above, if it is not handled at the gateway. Further, Please be guided by Microsoft Office 365 email architecture
7	11	Email Security & 35	The solution should be able to restrict incoming, outgoing and internal mails based on file types, file size and also by file name and also through a combination of them.	Internal Mail scanning requires visiability of email via a MTA and in that case Mail Solution has to route the emails to Mail Security solution via MTA. Kindly confirm if Bank mail solution can do the routing of internal domain mails, if not then please remove the Internal mails from the clause & amend as : The solution should be able to restrict incoming and outgoing mails based on file types, file size and also by file name and also through a combination of them.	The solution should be able to restrict incoming, outgoing and internal mails based on file types, file size and also by file name and also through a combination of them if it is routed through the Gateway.
8	11	Email Security & 36	The solution should provide the local domain identification and should drop any email with source email ID not exist.	Ask is not clear however, local domain is the protected domain for which the mails will be accpeted and if sender address is blank it will be dropped. Hope our understanding is correct, please confirm.	Please be guided by RFP
9	13	Email Security & 75	The Proposed solution should provide capabilities for end users to search on quarantined messages specific to them. The solution should allow end users to release mails from quarantine if approved.	For wider participation, please amend the clause as : The Proposed solution should provide capabilities for end users to search on quarantined messages specific to them. The solution should allow end users to release mails from quarantine	The proposed solution should provide capabilities for defined users (like Helpdesk, Administrators etc) to search on quarantined messages and release emails as required
10	13	Email DLP & 5	The solution should support Email DLP deployment on cloud for Office 365. All licenses required for the same should be included and management should be from the same centralized management platform	Request for Clarification that cloud mentioned can be referred as hosted deployment as well like mentioned in Email Security Clause 1, Hence request you to please amend the clause as : The solution should support Email DLP deployment on cloud/ hosted environmnet for Office 365. All licenses required for the same should be included and	The solution should support Email DLP deployment on cloud for Office 365. All licenses required for the same should be included and management should be from the centralized management platform

				management should be from the same centralized management platform	
11	13	Email DLP & 6	The solution should have features for masking of email ids of customers/ third parties mentioned in the email being forwarded to service providers etc. In case situation is not having this feature then it should be customize for our Bank before UAT sign off.	We can rewrite the emails in envolpe to hide the original emails. While this point is specifically inclined towards OEM – Broadcom here. Also masking the email also create a data risk as it can change the meaning of email if not correctly defined Hence request you to please amend this clause as : "The solution should have features for masking in reporting of PII , PCI and other email ids attribute of customers/third parties mentioned in the email being forwarded to service providers etc."	It is clarified, these are regulatory guidelines which need to be handled.
12	13	Email DLP & 11	The solution should be integrate with external data storage for the forensics over path to Big Data Lake/Data ware house as required.	Specify the data warehouse integration reuqired , we currently support the DLP integration with expoert to AWS and Azure for the log management POV for the datalake. Moreover any shared path can be configured in Centralised DLP Manager (Hot Cold Standby for DC/DR) to store the forensics	Please be guided by RFP
13	15	Email DLP & 34	Integration with Security Datalake to be implemented in future will be got done without extra	Need to understand the use case however forensics and arhive locations can be shared path.	Integration will be in respect of Data / logs which are generated from the email security solutions.
14	15	Email DLP & 42	The reports should be exported to at least CSV, PDF, HTML formats	Request you to please amend the clause as : The reports should be exported to at least CSV and PDF formats	Please be guided by RFP
15	16	Email DLP & 52	Features for disabling or modifying default rules, scenarios, and configurations should be available	Word Scenarios is making the clasue look ambigious, hence request you to please amend the clause as : Features for disabling, modifying default rules, scenarios with bolean logic , configurations should be available.	It is clarified, Scenario means all possible outcomes of situations.
16	63 &64	Email APT & 8	Solution to support below files for execution: Portable Document: PDF Document: DOC, DOCX, DOT, DOCM, DOTX, DOTM, HWP, ODT, PUB, RTF, WPD, XML, XPS and other file type. Spreadsheet: CSV, ODS, SYLK, XLT, XLS, XLM, XLTX, XLSM, XLTM, XLSB, XLA, XLAM, XLL, XLSX and other file type. PowerPoint: ODP, PPS, PPT, PPTX, PPTM, POTX, POTM, PPAM and other file type. Executable: BAT, COM, DLL, EXE, HTA, JS, MACH- O, MSI, PIF, PL, PS1, PY, SCR, SH, SYS, VB, WSF and other file type. Archive File: 7Z, ACE, APK, ARJ, BZIP, CAB, CHM, DMG, GZ, ISO, JAR, LHA, LZMA,, NUPKG, RAR, TAR,	Most of the important file formats are already covered in the mentioned clause, but adding any "other file type" makes the clause open ended and no OEM will be able to comply to this clause technically. Hence request you to please drop the phrase : "and other file type" from complete section.	It is clarified, other file type is deleted. Incase bank desires any other file format, then the same is to be customized by the successful bidder without any additional cost to the Bank

			TARGZ, TNEF, WAR, XAR, XZ, ZIP, ZIPX and other file type. Media: ODG, SVG, SWF, TIFF and other file type. Misc: CLASS, EML, HTML, IQY, PCAP, URL and other file type.		
17	64	Email APT & 9	The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal.	For wider participation, request you to please amend this clasue as : The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families	The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families
18	64	Email APT & 15	Solution should have Content disarm and reconstruction (CDR) capability, which protects against exploits and weaponized content that have not been seen before	OEM Specific Clause, request you to please delete this clause or make it optional for wider participation	Please be guided by RFP
19	64	Cloud Access Security Broker (CASB) & 16	The bidder should also implement a CASB solution to enable role based access to identify application including email by enforcing amalgamated policies for access through cloud from anywhere.	Need to understand the use case. CASB is a separate solution itself. Please share the complete list of detailed Specification of CASB along with Use cases or Request you to please drop the CASB from the scope of this RFP.	The reference to CASB is in respect of the email security solution which will be interacting with the email solution in cloud.
20	37	ANNEXURE-III-ELIGIBILITY CRITERIA OF THE BIDDER & 4	The OEM must have successfully implemented Email Security Solutions including Email gateway and Email DLP/ Email ATP in at least two PSU/ Government Organizations/ BFSI/ Private Sector in India, during last three years as on date of submission of Bid with a size of at least 35,000 email users in each.	For wider participation, request you to please amend the clause as: The OEM must have successfully implemented Email Security Solutions including Email gateway / Email DLP/ Email ATP in at least two PSU/ Government Organizations/ BFSI/ Private Sector in India, During last three years as on date of submission of Bid with a size of at least 35,000 email users in each.	**Please refer Corrigendum 1.1**
21	37 & 38	ANNEXURE-III-ELIGIBILITY CRITERIA OF THE BIDDER & 11	The OEM must have successfully implemented Email Security Solutions including Email gateway and Email DLP/ Email ATP on cloud.	For wider participation, request you to please amend the clause as : The OEM must have successfully implemented Email Security Solutions including Email gateway / Email DLP/ Email ATP on hosted cloud	Please be guided by RFP

Sr. No.	RFP Page No.	RFP Clause Name & No.	RFP Clause	Bidder's Query/Suggestion/Remarks	Bank's Response/clarification
1	9	Scope of Work	The scope of work includes Email Security Solution having following services for Punjab National Bank either On-Premises or on Cloud or both as applicable:	Clarification This clause is opposite to the entire technical specifications where the ask is to deliver the	Please be guided by RFP.

				solution using a cloud. Is the Bank looking for a on prem solution or cloud or we can provide any option? Please clarify ?	
2	10,55	1	The proposed email security solution should software/virtual based and can be hosted over any cloud.	The proposed email security solution should software/virtual based and can be hosted over any cloud OR should be hardware appliance/service built on purpose built email gateway appliance. This clause is opposite to the entire technical specifications where the ask is to deliver the solution using a cloud. Is the Bank looking for a on prem solution or cloud or we can provide any option? Please clarify ?	Please be guided by RFP
3	10,55	11	The solution should be integrated with the case management solution and incident management solution of the bank.	Clarification Such integration are API based. Proposed solution API is a representational state transfer (REST) based set of operations that provide secure and authenticated access to the reports, report counters, tracking, quarantine, and configuration. You can retrieve the appliance reporting, tracking, and quarantine data using the API. We understand that this will meet the ask however also share the case management solution and incident management solution used by Bank.	It is clarified, the solution should be integrated with the SIEM so that features of case management and incident management is available through the same for the incidents related to email security.
4	10,55	12	The solution should provide analytical reports based on the emails processed by the system between two periods to enable fine tuning of policies.	Clarification From the ask we understand that solution should be able to provide interactive reporting to capture contextual data, analysis of which will help admins to do fine tuning of different parameters if required. Interactive email reporting provides filtering based on several types of criteria, including the following: IP address, Domain, Internal user, Destination domain, Internal sender domain, Internal sender IP address, Incoming TLS domain, Outgoing TLS domain,SHA-256 etc.	Please be guided by RFP
5	10,11 ,56	15,25	Solution should protect against URL-based threats and should have lookalike domain detection capability	Clarification We understand that ask is for protection against highly targeted, socially engineered email attacks coming from lookalike domains. That can be delivered with DMARC verification which is a much powerful feature to fight against “Direct Domain Spoofing” and also includes “Display Name” & “Brand Impersonation” attacks. DMARC ties in information	It is clarified, bidder to provide suitable functionalities as per RFP

				authenticated with SPF or DKIM (sending domain source, or signature) with what is presented to the end-recipient in the "From" header and ascertains that SPF and/or DKIM identifiers are aligned with the FROM header identifier. Also Forged Email Detection (FED) is another important line of defense against email spoofing also Dictionary of cousin domains or look-alike domains, based on your own domain by using DNSTWIST (https://github.com/elceef/dnstwist) to match against look-alike domain spoofing. Please confirm if the understanding is correct.	
6	11,56	31	The solution should have at least 1500+ pre-defined content rules inbuilt with Email Security & embedded in the product	The solution should have at least 1500+ pre-defined content rules inbuilt with Email Security & embedded in the product OR should provide the capability to define custom content filter based on the BANK requirement All the incoming and outgoing mails pass through a set of policies if all 1500 content rules will be inspected against each and every message then it will introduce a delivery delay and built up the queue for messaging. So request you to consider option to define the customer filter as per the requirement of bank instead of pre-built list of rules.	It is clarified, the Bidder should provide the predefined / default content rules available in the system. The bank should have the facility to retain or delete specific rules. New rules/modified rules as required by the bank should be configured in the system before or during the implementation.
7	12,57	45	The solution must have directory harvesting and DoS prevention capabilities.	The solution must have protection against directory harvesting attacks. DOS is more applicable to network traffic that can be protected by gateways firewalls or IPS and should not be the capability of the email gateway solutions.	**Please refer Corrigendum 1.2**
8	12,58	57	The Solution must support quarantine administrator role. Thus only the delegated administrator is allowed to access the message in specific queue.	Clarification Administrator assigned with custom role to quarantine will get access to quarantine queue please confirm if the ask is same Proposed solution supports custom roles to allow delegated administrators to access the following All reports (optionally restricted by Reporting Group) Mail Policy reports (optionally restricted by Reporting Group) DLP reports (optionally restricted by Reporting Group) Message Tracking	It is clarified, the solution should support different roles as required for managing the email security besides specific roles for operational support.

				Quarantines Log Subscription	
9	12,58	60	The solution should allow where Administrator can specify which queues can be accessed by end user.	Request to remove this clause The ask is contradicting with clause number 57 where only delegated administered is authorized for quarantine queue access and also giving quarantine queue access to user posses a high risk as if any user released his/her mail without checking the threat context may lead to a threat entry into the PNB network.	**Please refer Corrigendum 1.3**
10	12,58	62	The Proposed solution should allow email reply to release the email quarantined by solution.	Request to remove this clause The ask is contradicting with clause number 57 where only delegated administered is authorized for quarantine queue access and also giving quarantine queue access to user posses a high risk as if any user released his/her mail without checking the threat context may lead to a threat entry into the PNB network.	Please be guided by RFP
11	13,59	78	The Proposed Solution should the configuration of workflow. End user's manager should be able to release the quarantined email via replying to the notification email from his inbox	Request to remove this clause The ask is contradicting with clause number 57 where only delegated administered is authorized for quarantine queue access and also giving quarantine queue access to user posses a high risk as if any user released his/her mail without checking the threat context may lead to a threat entry into the PNB network.	Please be guided by RFP
12	16,63	2	The Solution should have multiple AV/APT engines for anti-virus and malware scanning. Solution should provide on cloud AV/APT service from day1	The Solution should have multiple AV/APT engines for anti-virus and malware scanning. Solution should provide on cloud AV/APT service from day1 or should be hardware appliance/service built on purpose built appliance. "Ask is for a end to end solution that meets the objective instead of the form factor. Same is mentioned at multiple points in RFP. "The scope of work includes Email Security Solution having following services for Punjab National Bank either On-Premises or on Cloud or both." "The Proposed solution should be able to consolidate reports from multiple boxes for centralized logging and reporting."	Please be guided by RFP

13	16,63	6	It should support execution of OS X files and Android applications.	Request to remove this clause The ask is contradicting with clause number 5 where ask is "Sandbox Service should have Kernel visibility with minimal OS version dependencies" Bank supported this ask in "RFP for procurement of Network Anti- Advanced Persistent Threat (N/w-Anti-APT) and Deception/Decoy Solutions." published in 2019 for maximum participation and the point was read as "Solution should be deployed on premise and along with on premise sandboxing capability where the objectionable content may be executed and inspected, of the Windows Operating Systems (32 and 64 bit) This requirement should be based on virtual execution and should not be Hardware or chip based function" after corrigendum 1.	It is clarified, it should support execution of OS Xfiles and android applications if such functionalities of mobile platform support are included in email security solution provided.
14	16,63	8	Solution to support below files for execution: Portable Document: PDF Document: DOC, DOCX, DOT, DOCM, DOTX, DOTM, HWP, ODT, PUB, RTF, WPD, XML, XPS and other file type. Spreadsheet: CSV, ODS, SYLK, XLT, XLS, XLM, XLTX, XLSM, XLTM, XLSB, XLA, XLAM, XLL, XLSX and other file type. PowerPoint: ODP, PPS, PPT, PPTX, PPTM, POTX, POTM, PPAM and other file type. Executable: BAT, COM, DLL, EXE, HTA, JS, MACH-O, MSI, PIF, PL, PS1, PY, SCR, SH, SYS, VB, WSF and other file type. Archive File: 7Z, ACE, APK, ARJ, BZIP, CAB, CHM, DMG, GZ, ISO, JAR, LHA, LZMA,, NUPKG, RAR, TAR, TARGZ, TNEF, WAR, XAR, XZ, ZIP, ZIPX and other file type. Media: ODG, SVG, SWF, TIFF and other file type. Misc: CLASS, EML, HTML, IQY, PCAP, URL and other file type.	Solution to support below files for execution: Portable Document: PDF Document: DOC, DOCX, DOT, DOCM, DOTX, DOTM, HWP, ODT, PUB, RTF, XML, XPS and other file type. Spreadsheet: CSV, ODS, XLT, XLS, XLM, XLTX, XLSM, XLTM, XLSB, XLA, XLAM, XLL, XLSX and other file type. Executable: BAT, COM, DLL, EXE, HTA, JS, MSI, PIF, PS1, SCR, SYS, VB, WSF and other file type. Archive File: CAB, CHM, ISO, JAR and other file type. Media: SWF and other file type. Misc: EML, HTML, IQY, URL and other file type. PNB needs protection against the dynamic threats which is a never-ending battle against malware. So this should not be only limited to certain extension but should be based on the dynamic context information against which each new sample is analyzed. Malware changes over time; we have records of those changes. You can perform thorough retrospective remediation following a security breach. You can prepare more effective defences against the next generation of malware attacks. The list of extensions may not be tally with all the OEM's and restrict the participation.	It is clarified, other file type is deleted. Incase bank desires any other file format, then the same is to be customized by the successful bidder without any additional cost to the Bank

15	16,64	13	The solution should have option to store email or file in queue in case the similar file with same hash value receive in the given timespan then the action should be followed.	Request to remove this clause This will not improve any threat efficacy objective should be to automate the removal of emails with files that become malicious after the initial point of inspection. Retrospective events	Please be guided by RFP
16	16,64	16	The bidder should also implement a CASB solution to enable role based access to identify application including email by enforcing amalgamated policies for access through cloud from anywhere.	Request to remove this clause Cloud-native cloud access security broker (CASB) that helps customers move to the cloud safely. It protects your cloud users, data, and apps. uses open, and automated approach uses APIs to manage the risks in your cloud app ecosystem. Proposed solution complies to FedRAMP,SSAE16 – SOC 2 Type 2 Certified,SOC 3 Certified – Trust Services Report for Service Organizations,TRUSTe,Cloud Security Alliance Security, Trust & Assurance Registry (STAR) However CASB shares the metadata in cloud which may not be localized in geographical boundaries. This is independent solution for protection of cloud based SAAS applications and not part of Email Security.	It is clarified, the reference to CASB is in respect of the email security solution which will be interacting with the email solution in cloud.
17	36	Eligibility Criteria of the Bidder	Firm should be prime bidder and no consortium is allowed for the solution/ services to be offered	Bidder should provide the solution fully compliant as asked by the Bank. Bidder may choose single OEM or multiple OEM to arrive at the solution. This is restricting the bid to a single OEM and is also not allowing the Bank to get the best of the solution. We request the bank to allow multiple OEMs to provide a solution for Bank's requirement.	It is clarified, Bidder can opt for multiple OEM to arrive at Solution. However, each OEM should comply with eligibility Criteria defined in RFP. Additionally, there should be synergy among the products of different OEMs and should be compliant as per RFP
18	36	Eligibility Criteria of the Bidder	The bidder should have Support centres in India.	The Bidder and OEM should have support centres in India. We feel that the OEM must also have support centres in India and must be asked by the Bank. Otherwise in normal business hours Bank will struggle for support from global centres and also would have local language challenges. Almost all Government RFPs ask for OEM support centre in India.	**Please refer Corrigendum 1.13**
19	46	MAF	In case of default/unable to comply with above at the time of delivery or during implementation or customization, for the software already billed, we agree to take back the supplied items without	Kindly remove.	Please be guided by RFP

			demur, if already supplied and replace it with an Original &Latest product/component. We also take full responsibility of the Solution& Service SLA as per the content even if there is any defect by our authorized Service Centre / Reseller / SI etc.		

Sr. No.	RFPPage No.	RFP Clause Name & No.	RFP Clause	Bidder's Query/Suggestion/Remarks	Bank's Response/clarification
1	36	Annexure - III Eligibility Criteria of the Bidder - Clause 3	The Bidder must have successfully implemented Email Security Solutions including Email gateway and Email DLP/ Email ATP in at least one PSU/ Government Organizations / BFSI / Private Sector in India, during last three years as on date of submission of Bid with a size of at least 20,000 email users	Request clause to be changed to read as: Bidder/OEM should have implemented Email Security Solutions including Email Gateway/Email DLP/ Email ATP in at least one PSU/ Government Organizations / BFSI / Private Sector in India, during last three years as on date of submission of Bid with a size of at least 20,000 email users. Or The Bidder must have successfully implemented Email Security Solutions including Email gateway /Email DLP/ Email ATP in at least one PSU/ Government Organizations / BFSI / Private Sector in India with a size of at least 7500 email users. We request you to not attach anytimeline as the gestation period for such projects are too long.	**Please refer Corrigendum 1.4**
2	28	**Annexure -I Terms and Conditions Caluse - 6 Delivery /Activation**	Bidder shall be responsible for delivery/activation of the complete solution/Service as per the Bank's requirement within 4 weeks from the date of Purchase order. Implementation Period will be 6 weeks. The date on which the complete system is installed will be taken as the date of activation. In case of part activation of the solution/Service, the date of last service enablement will be taken as the date of activation.	Request clause to be changed to read as: We Request you to kindly amend the timelines for delivery from 4 to 6 weeks from PO date & Implementation timeline to be 8 weeks after the delivery timeline i.e. 4 to 6 weeks from PO.	**Please refer Corrigendum 1.5**
3	28	Annexure -I Terms and Conditions Caluse -8 Payment, Penalty, Delivery and Timelines	Payment will be made quarterly in arrears for On-Site Support (for line item no. 4 in indicative commercial offer), excluding the payment terms for one-time purchase (for line item no. 1,2 and 3 in indicative commercial offer) which will be against receipt of bank guarantee.	We request you to kindly amend the payment terms to be - 1. Product/Licences Payment - 100% payment of Product/Licences on Delivery. 2. Implementation Payment - This payment should be slab based i.e. 100% payment for completion of implementation of 10000 licenses. 3. Onsite Support Payment - Payment will be made quarterly in arrears for On-Site Support. 4. Penalty- The Maximum Penalty should not be more than 10% of the total Contract Value.	Please be guided by RFP
4	48	Annexure - XII Indicative	If support is not provided onsite for any reason and is provided on work from anywhere basis, the	We Request you to kindly Amend the clause as below -If support is not provided onsite for any	Please be guided by RFP

		Commercial Offer . Notes Point No 11	applicable support charges will be reduced to 75% of onsite support charges as agreed upon after rate finalization as per RFP	reason and is provided on work from anywhere basis, the applicable support charges will be reduced to 90% of onsite support charges as agreed upon after rate finalization as per RFP.	
5	48	Annexure - XII Indicative Commercial Offer . Notes Point No 12	For additional Licenses over and above 30,000, bank will place the order as per unit cost per license in multiple of 1000 derived after Reverse Auction and subsequent negotiations, if any.	To best to our understanding Bank will purchase 30,000 Licences in one go initially & subsequent to that Bank will place order as and when required but minimum quantity would not be less than 1000 Licences .	Please be guided by RFP
6	8	Important Instruction for Submission of Bid	The technical bid should be submitted in a single hard-bound file with not more than 250 pages. No loose pages must be submitted.	Request clause to be change to read as: We request you to kindly delete this clause because we received multiple documents from OEM.	It is clarified, only documents relevant as per RFP should be provided in the Technical Bid documents.
7		Additional		All the delivery and implementation time lines will be agreeable subject to Pre requisites and other dependencies on bank are taken care in stipulated time.	Please be guided by RFP
8	10	SCOPE OF WORK: Email Security & Point 1	The proposed email security solution should software/virtual based and can be hosted over any cloud.	Please clarify cloud hosting infra will be provided by PNB or bidder has to factor the same.	It is clarified, Bidder has to factor for the same.
9		Additional		Please clarify Email Security, ATP and DLP should be from same OEM or can be any combination?	Please be guided by RFP and clarifications provided.
10	10	Email Security & 6	The solution should have features to build scenarios for actions on emails.	Please clarify the scenario meaning , as its generic . Our understanding is different types of filters, Is our understanding correct ?	It is clarified, Scenario means all possible outcomes of situations.
11	10	Email Security & 7	The Solution should have IPV4 and IPV6 dual stack Compatibility.	As the solution will be delivered from the IAAS setup , so IPv4 or IPv6 should not be criteria for network conenction , modify the same to "The Solution should have IPV4 or IPV6 Compatibility"	It is clarified, the access to neither IPV4 nor IPV6 traffic should be dropped, due to incompatibility in the infrastructure. Please be guided by RFP.
12	10	Email Security & 8	The Solution should have APIs/ Connectors / scripts for integration with various security solutions in the bank like ADDM, SMS, SOAR, SIEM, Firewall etc. as applicable and bidder shall enable the requested integration without any additional cost to Bank.	Every OEM will have the integration points "The Solution should have APIs/ Connectors / scripts for integration with various security solutions in the bank like SIEM etc. as applicable and bidder shall enable the requested integration. Also for any specific integration need to be discuss and factor in PS cost"	Please be guided by RFP
13	10	Email Security & 11	The solution should be integrated with the case management solution and incident management solution of the bank.	Each OEM has its own way of integration in our case email notifications can be sent to incident management and case management solution for generating the tickets. Also request you to please provide the details of the Case Management & Incident Management solution used by the bank.	It is clarified, the solution should be integrated with the SIEM so that features of case management and incident management is available through the same for the incidents related to email security.

14	10	Email Security & 16	The Solution should have DR capabilities and functionalities so that the email security can be implemented even if email solution is shifted from one setup to another setup. This should be properly configured during implementation.	Each OEM has its own way of setting the DR capability, This clause is limiting our participation, Hence request you to please amend this clause as : The Solution should have DR capabilities and functionalities so that the email security is not impacted even if email solution is shifted from one setup to another setup. This should be properly configured during implementation.	It is clarified, the solution should have DR capabilities and functionalities so that the email security is not impacted even if the email or the email security solution is shifted from one set up to another set up. This should be properly configured during the implementation.
15	11	Email Security & 22	The solution virus engine should support scanning by inbound, outbound and internal direction and configure the policy per direction.	Internal Mail scanning requires visiability of email via a MTA and in that case Mail Solution has to route the emails to Mail Security solution via MTA. Kindly confirm if Bank mail solution can do the routing of internal domain mails, if not then please remove the Internal direction from the clause & amend as : The solution virus engine should support scanning by inbound, outbound and configure the policy.	It is clarified, please be guided by Microsoft Office 365 email architecture. The solution virus engine should support scanning by inbound, outbound direction and configure the policy per direction. Bidder should provide suitable solution for scanning internal emails in addition to above, if it is not handled at the gateway. Further, Please be guided by Microsoft Office 365 email architecture
16	11	Email Security & 35	The solution should be able to restrict incoming, outgoing and internal mails based on file types, file size and also by file name and also through a combination of them.	Internal Mail scanning requires visiability of email via a MTA and in that case Mail Solution has to route the emails to Mail Security solution via MTA. Kindly confirm if Bank mail solution can do the routing of internal domain mails, if not then please remove the Internal mails from the clause & amend as : The solution should be able to restrict incoming and outgoing mails based on file types, file size and also by file name and also through a combination of them.	It is clarified, the solution should be able to restrict incoming, outgoing and internal mails based on file types, file size and also by file name and also through a combination of them if it is routed through the Gateway.
17	11	Email Security & 36	The solution should provide the local domain identification and should drop any email with source email ID not exist.	Ask is not clear however , local domain is the protected domain for which the mails will be accpeted and if sender address is blank it will be dropped. Hope our understanding is correct, please confirm.	Please be guided by RFP
18	13	Email Security & 75	The Proposed solution should provide capabilities for end users to search on quarantined messages specific to them. The solution should allow end users to release mails from quarantine if approved.	For wider participation, please amend the clause as : The Proposed solution should provide capabilities for end users to search on quarantined messages specific to them. The solution should allow end users to release mails from quarantine	It is clarified, the proposed solution should provide capabilities for defined users (like Helpdesk, Administrators etc.) to search on quarantined messages and release emails as required.
19	13	Email DLP & 5	The solution should support Email DLP deployment on cloud for Office 365. All licenses required for the same should be included and management should be from the same centralized management platform	Request for Clarification that cloud mentioned can be referred as hosted deployment as well like mentioned in Email Security Clause 1, Hence request you to please amend the clause as : The solution should support Email DLP deployment on cloud/ hosted environmnet for Office 365. All licenses required for the same should be included and management should be	The solution should support Email DLP deployment on cloud for Office 365. All licenses required for the same should be included and management should be from the centralized management platform

				from the same centralized management platform	
20	13	Email DLP & 6	The solution should have features for masking of email ids of customers/ third parties mentioned in the email being forwarded to service providers etc. In case situation is not having this feature then it should be customize for our Bank before UAT sign off.	We can rewrite the emails in envolpe to hide the original emails. While this point is specifically inclined towards OEM – Broadcom here. Also masking the email also create a data risk as it can change the meaning of email if not correctly defined Hence request you to please amend this clause as : "The solution should have features for masking in reporting of PII , PCI and other email ids attribute of customers/third parties mentioned in the email being forwarded to service providers etc."	It is clarified, these are regulatory guidelines which need to be handled.
21	13	Email DLP & 11	The solution should be integrate with external data storage for the forensics over path to Big Data Lake/Data ware house as required.	Specify the data warehouse integration reuqired , we currently support the DLP integration with expoert to AWS and Azure for the log management POV for the datalake. Moreover any shared path can be configured in Centralised DLP Manager (Hot Cold Standby for DC/DR) to store the forensics	Please be guided by RFP
22	15	Email DLP & 34	Integration with Security Datalake to be implemented in future will be got done without extra	Need to understand the use case however forensics and arhive locations can be shared path.	It is clarified, integration will be in respect of Data / logs which are generated from the email security solutions.
23	15	Email DLP & 42	The reports should be exported to at least CSV, PDF, HTML formats	Request you to please amend the clause as : The reports should be exported to at least CSV and PDF formats	Please be guided by RFP
24	16	Email DLP & 52	Features for disabling or modifying default rules, scenarios, and configurations should be available	Word Scenarios is making the clasue look ambigious, hence request you to please amend the clause as : Features for disabling, modifying default rules, scenarios with bolean logic , configurations should be available.	It is clarified, Scenario means all possible outcomes of situations.
25	63 &64	Email APT & 8	Solution to support below files for execution: Portable Document: PDF Document: DOC, DOCX, DOT, DOCM, DOTX, DOTM, HWP, ODT, PUB, RTF, WPD, XML, XPS and other file type. Spreadsheet: CSV, ODS, SYLK, XLT, XLS, XLM, XLTX, XLSM, XLTM, XLSB, XLA, XLAM, XLL, XLSX and other file type. PowerPoint: ODP, PPS, PPT, PPTX, PPTM, POTX, POTM, PPAM and other file type. Executable: BAT, COM, DLL, EXE, HTA, JS, MACH- O, MSI, PIF, PL, PS1, PY, SCR, SH, SYS, VB, WSF	Most of the important file formats are already covered in the mentioned clause, but adding any "other file type" makes the clause open ended and no OEM will be able to comply to this clause technically. Hence request you to please drop the phrase : "and other file type" from complete section.	It is clarified, other file type is deleted. Incase bank desires any other file format, then the same is to be customized by the successful bidder without any additional cost to the Bank

			and other file type. Archive File: 7Z, ACE, APK, ARJ, BZIP, CAB, CHM, DMG, GZ, ISO, JAR, LHA, LZMA,, NUPKG, RAR, TAR, TARGZ, TNEF, WAR, XAR, XZ, ZIP, ZIPX and other file type. Media: ODG, SVG, SWF, TIFF and other file type. Misc: CLASS, EML, HTML, IQY, PCAP, URL and other file type.		
26	64	Email APT & 9	The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal.	For wider participation, request you to please amend this clasue as : The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families	It is clarified, the Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families. Please be guided by the RFP
27	64	Email APT & 15	Solution should have Content disarm and reconstruction (CDR) capability, which protects against exploits and weaponized content that have not been seen before	OEM Specific Clause, request you to please delete this clause or make it optional for wider participation	Please be guided by RFP
28	64	Cloud Access Security Broker (CASB) & 16	The bidder should also implement a CASB solution to enable role based access to identify application including email by enforcing amalgamated policies for access through cloud from anywhere.	Need to understand the use case. CASB is a separate solution itself. Please share the complete list of detailed Specification of CASB along with Use cases or Request you to please drop the CASB from the scope of this RFP.	It is clarified, reference to CASB is in respect of the email security solution which will be interacting with the email solution in cloud.
29	37	ANNEXURE-III-ELIGIBILITY CRITERIA OF THE BIDDER & 4	The OEM must have successfully implemented Email Security Solutions including Email gateway and Email DLP/ Email ATP in at least two PSU/ Government Organizations/ BFSI/ Private Sector in India, during last three years as on date of submission of Bid with a size of at least 35,000 email users in each.	For wider participation, request you to please amend the clause as : The OEM must have successfully implemented Email Security Solutions including Email gateway / Email DLP/ Email ATP in at least two PSU/ Government Organizations/ BFSI/ Private Sector in India, During last three years as on date of submission of Bid with a size of at least 35,000 email users in each.	**Please refer Corrigendum 1.1**
30	37 & 38	ANNEXURE-III-ELIGIBILITY CRITERIA OF THE BIDDER & 11	The OEM must have successfully implemented Email Security Solutions including Email gateway and Email DLP/ Email ATP on cloud.	For wider participation, request you to please amend the clause as : The OEM must have successfully implemented Email Security Solutions including Email gateway / Email DLP/ Email ATP on hosted cloud	Please be guided by RFP

Sr. No.	RFPP age No.	RFP Clause Name & No.	RFP Clause	Bidder's Query/Suggestion/Remarks	Bank's Response/clarification
1	8	IMPORTANT INSTRUCTION FOR SUBMISSION OF BID	The technical bid should be submitted in a single hard-bound file with not more than 250 pages.	Restricting bidders to submit a bid with limited pages may result in the shortfall of documents as per the RFP requirement. We request you to kindly amend this clause as:	It is clarified, only documents relevant as per RFP should be provided in the Technical Bid documents.

				The technical bid should be submitted in a hard-bound file. No loose pages must be submitted.	
2	17	Other conditions; Clause No-c	Bank reserves the right to change the Successful bidder with three months' notice to the concerned person of the Company.	This clause is ambiguous, kindly clarify in what scenario this clause will be applicable or the Bank will unilaterally decide or the bidder will be asked for explanation. Kindly clarify. Request you to kindly delete this clause, because Clause-a suffices the Bank's requirement.	Please be guided by RFP
3	18	INSTRUCTION TO BIDDERS; Clause No-10; BID EARNEST MONEY	Bidder has to submit the 'Bid Security Declaration' on their organizations letter-head duly signed and stamped by their 'authorized signatory' accepting that if they withdraw or modify their bids during period of validity of the bid or if they are awarded the contract and they fail to sign the contract or fails to submit a performance security before the deadline defined in the request for proposals (RFP) document, they will be Blacklisted.	Request you to kindly share the format for Bid Security Declaration, so that all the bidders should follow same format for submitting bid security declaration.	It is clarified, bidder has to submit the 'Bid Security Declaration' on their organizations letter-head duly signed and stamped by their 'authorized signatory' accepting that if they withdraw or modify their bids during period of validity of the bid or if they are awarded the contract and they fail to sign the contract or fails to submit a performance security before the deadline defined in the request for proposals (RFP) document, they will be Blacklisted
4	28	ANNEXURE I; Clause No-8	Payment will be made quarterly in arrears for On-Site Support (for line item no. 4 in indicative commercial offer), excluding the payment terms for one-time purchase (for line item no. 1,2 and 3 in indicative commercial offer) which will be against receipt of bank guarantee.	As per our understanding 100% payment on delivery of licenses will be released after the submission of PBG i.e. 03% of Total Purchase Order value. Kindly clarify. We further request you to confirm the duration of warranty and ATS to be considered for the project as per the RFP.	Please be guided by RFP
5	33	ANNEXURE I; Clause No-29	The shortlist bidder/TSP shall be required to execute SLA (Service Level Agreement), IP (Integrity Pact) and NDA (Non-Disclosure Agreement) with the Bank.	The draft for SLA (Service Level Agreement) and NDA (Non-Disclosure Agreement) are not provided in the RFP. Request you to kindly share the format of SLA and NDA	Please be guided by RFP
6	36	ANNEXURE-III; Clause No-3	The Bidder must have successfully implemented Email Security Solutions including Email gateway and Email DLP/ Email ATP in at least one PSU/ Government Organizations / BFSI / Private Sector in India, during last three years as on date of submission of Bid with a size of at least 20,000 email users	As per our understanding bidder can meet the criteria with Single or Multiple credentials. Kindly confirm. We request the bank to kindly amend this clause as: The Bidder must have successfully implemented Email Security gateway/ DLP/ ATP in at least one PSU/ Government Organizations / BFSI / Private Sector in India, during last five years as on date of submission of Bid with a size of at least 20,000 email users	**Please refer Corrigendum 1.4**
7	37	ANNEXURE-III; Clause No-9	The bidder should have a minimum turnover of INR 6 crores (Rupees Six crores) or (INR 3 Crores (Rupees Three Crores) for MSE bidders) per annum for the past three financial years i.e. FY2017-18, FY2018-19 & FY2019-20 from their	Since, Email Security Solutions including Email gateway and Email DLP/ Email ATP are categorized under cyber/IT security. Hence, we request you to kindly amend this clause as: The bidder should have a minimum turnover of	**Please refer Corrigendum 1.6**

			Indian Operations from sale of Email Security Solutions including Email gateway and Email DLP/ Email ATP.	INR 6 crores (Rupees Six crores) or (INR 3 Crores (Rupees Three Crores) for MSE bidders) per annum for the past three financial years i.e. FY2017-18, FY2018-19 & FY2019-20 from their Indian Operations from sale of IT/Cyber Security components.	
8	28	ANNEXURE I, TERMS AND CONDITIONS; Clause No-6; DELIVERY/ACTIVATION	DELIVERY/ACTIVATION Bidder shall be responsible for delivery/activation of the complete solution/Service as per the Bank's requirement within 4 weeks from the date of Purchase order. Implementation Period will be 6 weeks. The date on which the complete system is installed will be taken as the date of activation. In case of part activation of the solution/Service, the date of last service enablement will be taken as the date of activation.	As you are aware that all most all the OEM are supplying their materials form outside India, and because of COVID'19 pandemic deliveries are getting delayed. Hence, we request you to kindly amend this clause as: DELIVERY/ACTIVATION Bidder shall be responsible for delivery/activation of the complete solution/Service as per the Bank's requirement within 10 weeks from the date of Purchase order. Implementation Period will be 12 weeks. The date on which the complete system is installed will be taken as the date of activation. In case of part activation of the solution/Service, the date of last service enablement will be taken as the date of activation.	**Please refer Corrigendum 1.5**
9	29	ANNEXURE I, TERMS AND CONDITIONS; Clause No-8	Deliverables Future Integration Expected Timelines Within 8 weeks from the date of Purchase Order (PO) (includes 1 month for UAT & 1 month for Go-Live.	Considering the delay in delivery due to pandemic situation worldwide, we request you to kindly amend this clause as: Deliverables Future Integration Expected Timelines Within 10 weeks after the delivery of material (includes 1 month for UAT & 2 month for Go-Live)	Please be guided by RFP
10	29	ANNEXURE I, TERMS AND CONDITIONS; Clause No-8	Maximum Penalty 10% of Future Integration Cost	We request to kindly amend this clause as: Maximum Penalty 5% of Future Integration Cost	Please be guided by RFP
11	29	ANNEXURE I, TERMS AND CONDITIONS; Clause No-8; PAYMENT, PENALTY, DELIVERY AND TIMELINES	Penalty due to Absence of Onsite Engineer In the absence of the deployed OTS resource at HO, suitable replacement is to be provided on immediate basis. In case of absolute absence (when no replacement is provided), penalty would be deducted @0.5% of monthly charges for each day, up to a maximum of 10%. Onsite support charges for first year post successful implementation/activation of services of contract will be free of cost to the Bank.	We request you to kindly amend this clause as: Penalty due to Absence of Onsite Engineer In the absence of the deployed OTS resource at HO, suitable replacement is to be provided on immediate basis. In case of absolute absence (when no replacement is provided), penalty would be deducted @0.5% of monthly charges for each day, up to a maximum of 05%. Onsite support charges for first year post successful implementation/activation of services of contract will be free of cost to the Bank.	Please be guided by RFP
12	29	ANNEXURE I, TERMS AND CONDITIONS;	Future Integration: Bank will pay as per the cost arrived at Sr. No. 7 of Indicative Commercial Offer Post Reverse-Auction. The implementation is to be	As per the clause No-6 of Annexure-I, implementation period will be 6 weeks. But, at clause No-8 (page no-29); Future Integration,	It is clarified, treat both the clauses as separate i.e. one is for present implementation and other is for future integration.

		Clause No-8; PAYMENT, PENALTY, DELIVERY AND TIMELINES	completed in a maximum of 8 weeks. Bank will provide all the required infrastructure for the same.	you have mentioned that, the implementation is to be completed in a maximum of 8 weeks. Kindly confirm the implementation period. We further request you to kindly amend this clause as: Bank will pay as per the cost arrived at Sr. No. 7 of Indicative Commercial Offer Post Reverse-Auction. The implementation is to be completed in a maximum of 12 weeks. Bank will provide all the required infrastructure for the same.	
13	9	Page No 10	The bidder should follow the data localization guidelines of the Government and regulators as applicable from time to time. A confirmation should be provided in this regard	The proposed solution will be in-line with ISMS guidelines with ISO 27001 and SOC2 Type II certified solution. Please share us the data localization guidelines received from RBI to validate the requirements.	Please be guided by RFP
14	13	Page No 10	The bidder should provide flow chart depicting the actions of the different email security solutions on the email.	What do we understand by different email security solutions? Are we referring to outbound email flow from O365 to Email DLP to Email Security.cloud?	It is clarified, different email security solutions refer to email gateway, email DLP, email ATP and any other email security solution .
15	22	Page No 56	The solution virus engine should support scanning by inbound, outbound and internal direction and configure the policy per direction.	We are assuming internal emails to be emails send within the bank's tenant and such emails can be scanned through API based approach which altogether a separate solution.	It is clarified, please be guided by Microsoft Office 365 email architecture. The solution virus engine should support scanning by inbound, outbound direction and configure the policy per direction. Bidder should provide suitable solution for scanning internal emails in addition to above, if it is not handled at the gateway. Further, Please be guided by Microsoft Office 365 email architecture
16	36	Page No 57	The solution should provide the local domain identification and should drop any email with source email ID not exist.	We require detailed information on this use case - The email security service data protection modules can analyse the headers of the email and take action on the absence of key information if required	Please be guided by RFP
17	6	Page No 63	It should support execution of OS X files and Android applications.	Sending OSX and Android applications over the email are not recommended. Ideally these types of files and applications should be shared through other mediums and blocked over emails. Can you please share the type of file extensions if this a mandatory requirement?	It should support execution of OS Xfiles and android applications if such functionalities of mobile platform support are included in email security solution provided.
18	16	Page No 64	The bidder should also implement a CASB solution to enable role based access to identify application including email by enforcing amalgamated policies for access through aloud from anywhere.	Please elaborate the requirements and CASB Solution details	It is clarified, reference to CASB is in respect of the email security solution which will be interacting with the email solution in cloud.

1	28	DELIVERY/ACTIVATION	Bidder shall be responsible for delivery/activation of the complete solution/Service as per the Bank's requirement within 4 weeks from the date of Purchase order. Implementation Period will be 6 weeks. The date on which the complete system is installed will be taken as the date of activation. In case of part activation of the solution/Service, the date of last service enablement will be taken as the date of activation	Kindly amend the timelines as follows: Bidder shall be responsible for delivery/activation of the complete solution/Service as per the Bank's requirement within 6 weeks from the date of Purchase order. Implementation Period will be 8 weeks. The date on which the complete system is installed will be taken as the date of activation. In case of part activation of the solution/Service, the date of last service enablement will be taken as the date of activation	**Please refer Corrigendum 1.5**
2	28	Penalty due to Downtime	After activation of the Complete solution, Penalty will be deducted for downtime of the services (A) as below Uptime >=99.99 No Penalty 99.50<=Uptime < 99.95 0.1 % of (A) 99.00<=Uptime< 99.50 0.2 % of (A) 98.50<=Uptime< 99.00 0.3 % of (A) 98.00<=Uptime< 98.50 0.4 % of (A) And so on For every 0.5 % drop in the Uptime, Penalty @ 0.1% of (A), up to a maximum of 10% of (A)	Penalties are very stringent, we request the penalty clause for Down Time to be amended as follows: After activation of the Complete solution, Penalty will be deducted for downtime of the services (A) as below Uptime >=99.99 No Penalty 99.50<=Uptime < 99.95 - 0.05 % of (A) 99.00<=Uptime< 99.50 0.10 % of (A) 98.50<=Uptime< 99.00 0.15 % of (A) 98.00<=Uptime< 98.50 0.20 % of (A) And so on For every 0.5 % drop in the Uptime, Penalty @ 0.05% of (A), up to a maximum of 5% of (A)	Please be guided by RFP
3	29	Penalty due to Absence of Onsite Engineer	In the absence of the deployed OTS resource at HO, suitable replacement is to be provided on immediate basis. In case of absolute absence (when no replacement is provided), penalty would be deducted @0.5% of monthly charges for each day, up to a maximum of 10%.	Kindly amend this clause as follows: In the absence of the deployed OTS resource at HO, suitable replacement is to be provided on immediate basis. In case of absolute absence (when no replacement is provided), penalty would be deducted @0.1% of monthly charges for each day, up to a maximum of 5%.	Please be guided by RFP
4	36	ANNEXURE-III - ELIGIBILITY CRITERIA OF THE BIDDER	All Eligibility Criteria	We request the bank to kindly add the following clause: In case of corporate restructuring, all the above listed eligibility criteria can be met by the bidding entity itself, or by the bidding entity's parent company (if the bidding entity is 100% owned subsidiary of the parent company) or fellow subsidiary company. In such a case, all the above eligibility clauses, the term "bidder" shall mean "Bidder / Bidder's Parent Company / Bidder's Subsidiary Company". Supporting documents of the parent company's / fellow subsidiary company's credentials shall be acceptable for all the above eligibility criteria.	Please be guided by RFP

5	36	ANNEXURE-III - ELIGIBILITY CRITERIA OF THE BIDDER	3. The Bidder must have successfully implemented Email Security Solutions including Email gateway and Email DLP/ Email ATP in at least one PSU/ Government Organizations / BFSI / Private Sector in India, during last three years as on date of submission of Bid with a size of at least 20,000 email users	Kindly amend this clause to include under implementation orders. The Bidder must have experience of implementing Email Security Solutions including Email gateway and Email DLP/ Email ATP in at least one PSU/ Government Organizations / BFSI / Private Sector in India, during last three years as on date of submission of Bid with a size of at least 20,000 email users. Ongoing Orders / Contracts which are under implementation at the time of bidding will also be considered.	**Please refer Corrigendum 1.4**
6	37	ANNEXURE-III - ELIGIBILITY CRITERIA OF THE BIDDER	10. The bidder should have a minimum turnover of INR 6 crores (Rupees Six crores) or (INR 3 Crores (Rupees Three Crores) for MSE bidders) per annum for the past three financial years i.e. FY2017-18, FY2018-19 & FY2019-20 from their Indian Operations from sale of Email Security Solutions including Email gateway and Email DLP/ Email ATP.	Organizations providing variety of IT Solution usually do not track revenues solution-wise. We therefore request the bank to kindly amend the criteria to consider the overall turnover pertaining to IT/ITeS, as follows: The bidder should have a minimum turnover of INR 6 crores (Rupees Six crores) or (INR 3 Crores (Rupees Three Crores) for MSE bidders) per annum for the past three financial years i.e. FY2017-18, FY2018-19 & FY2019-20 from their Indian Operations from Information/Cyber Security Services.	**Please refer Corrigendum 1.6**
7	55	Technical Specifications (Annexure-XV)	Security Solution	We request the bank to share specific additional compliance sheets for each security component, if required	It is clarified, requirements is already provided in the RFP. Further details required for implementation will be shared with the successful bidder.
8	9	SCOPE OF WORK	The Bidder/SI shall be responsible to ensure and deliver all the functional, technical and operational requirements for all the products with proper co-ordination with PNB.	Is the bank open for native Microsoft O365 security solution which will meet the RFP's Security Compliance OR is the bank looking in to have a Hybrid Security Solution / Multi-OEM solution which will also cover On-premise security compliance?	Please be guided by RFP
9	10	Email Security & 6	The solution should have features to build scenarios for actions on emails.	Please clarify the scenario meaning , as it is generic . Our understanding is that this means different types of filters. Is our understanding correct ?	It is clarified, Scenario means all possible outcomes of situations.
10	10	Email Security & 7	The Solution should have IPV4 and IPV6 dual stack Compatibility.	As the solution will be delivered from the IAAS setup , so IPv4 or IPv6 should not be criteria for network conenction. Kindly modify the same to "The Solution should have IPV4 or IPV6 Compatibility"	It is clarified, access to neither IPV4 nor IPV6 traffic should be dropped, due to incompatibility in the infrastructure.
11	10	Email Security & 8	The Solution should have APIs/ Connectors / scripts for integration with various security solutions in the bank like ADDM, SMS, SOAR,	Every OEM will have the integration points. Kindly amend as: "The Solution should have APIs/ Connectors / scripts for integration with	Please be guided by RFP

			SIEM, Firewall etc. as applicable and bidder shall enable the requested integration without any additional cost to Bank.	various security solutions in the bank like SIEM etc. as applicable and bidder shall enable the requested integration. Also for any specific integration need to be discuss and factor in PS cost"	
12	10	Email Security & 11	The solution should be integrated with the case management solution and incident management solution of the bank.	Each OEM has its own way of integration. In our case, email notifications can be sent to incident management and case management solution for generating the tickets. Kindly confirm if this is acceptable. Also request you to please provide the details of the Case Management & Incident Management solution used by the bank.	It is clarified, the solution should be integrated with the SIEM so that features of case management and incident management is available through the same for the incidents related to email security.
13	10	Email Security & 16	The Solution should have DR capabilities and functionalities so that the email security can be implemented even if email solution is shifted from one setup to another setup. This should be properly configured during implementation.	Each OEM has its own way of setting the DR capability, This clause is limiting our participation, Hence request you to please amend this clause as : "The Solution should have DR capabilities and functionalities so that the email security is not impacted even if email solution is shifted from one setup to another setup. This should be properly configured during implementation."	It is clarified, solution should have DR capabilities and functionalities so that the email security is not impacted even if the email or the email security solution is shifted from one set up to another set up. This should be properly configured during the implementation.
14	11	Email Security & 22	The solution virus engine should support scanning by inbound, outbound and internal direction and configure the policy per direction.	Internal Mail scanning requires visiability of email via an MTA and in that case Mail Solution has to route the emails to Mail Security solution via MTA. Kindly confirm if Bank mail solution can do the routing of internal domain mails, if not then please remove the Internal direction from the clause & amend as : The solution virus engine should support scanning by inbound, outbound and configure the policy.	It is clarified, please be guided by Microsoft Office 365 email architecture. The solution virus engine should support scanning by inbound, outbound direction and configure the policy per direction. Bidder should provide suitable solution for scanning internal emails in addition to above, if it is not handled at the gateway. Further, Please be guided by Microsoft Office 365 email architecture
15	11	Email Security & 35	The solution should be able to restrict incoming, outgoing and internal mails based on file types, file size and also by file name and also through a combination of them.	Internal Mail scanning requires visiability of email via a MTA and in that case Mail Solution has to route the emails to Mail Security solution via MTA. Kindly confirm if Bank mail solution can do the routing of internal domain mails, if not then please remove the Internal mails from the clause & amend as : "The solution should be able to restrict incoming and outgoing mails based on file types, file size and also by file name and also through a combination of them."	It is clarified, The solution should be able to restrict incoming, outgoing and internal mails based on file types, file size and also by file name and also through a combination of them if it is routed through the Gateway.

16	11	Email Security & 36	The solution should provide the local domain identification and should drop any email with source email ID not exist.	As we understand, this means that the local domain is the protected domain for which the mails will be accpeted and if sender address is blank it will be dropped. Hope our understanding is correct, please confirm.	Please be guided by RFP
17	13	Email Security & 75	The Proposed solution should provide capabilities for end users to search on quarantined messages specific to them. The solution should allow end users to release mails from quarantine if approved.	For wider participation, please amend the clause as : The Proposed solution should provide capabilities for end users to search on quarantined messages specific to them. The solution should allow end users to release mails from quarantine	It is clarified, the proposed solution should provide capabilities for defined users (like Helpdesk, Administrators etc.) to search on quarantined messages and release emails as required.
18	13	Email DLP & 5	The solution should support Email DLP deployment on cloud for Office 365. All licenses required for the same should be included and management should be from the same centralized management platform	Request for Clarification that cloud mentioned can be referred as hosted deployment as well like mentioned in Email Security Clause 1. Hence request you to please amend the clause as : The solution should support Email DLP deployment on cloud/ hosted environmnet for Office 365. All licenses required for the same should be included and management should be from the same centralized management platform.	The solution should support Email DLP deployment on cloud for Office 365. All licenses required for the same should be included and management should be from the centralized management platform
19	13	Email DLP & 6	The solution should have features for masking of email ids of customers/ third parties mentioned in the email being forwarded to service providers etc. In case situation is not having this feature then it should be customize for our Bank before UAT sign off.	We can rewrite the emails in envelope to hide the original emails. This point is specifically inclined towards OEM – Broadcom here. Also masking the email also creates a data risk as it can change the meaning of the email if not correctly defined. Hence request you to please amend this clause as : "The solution should have features for masking in reporting of PII , PCI and other email ids attribute of customers/third parties mentioned in the email being forwarded to service providers etc."	It is clarified, these are regulatory guidelines which need to be handled.
20	13	Email DLP & 11	The solution should be integrate with external data storage for the forensics over path to Big Data Lake/Data ware house as required.	Kindly specify and provide details of the data warehouse integration required. We currently support the DLP integration with export to AWS and Azure for the log management POV for the datalake. Moreover any shared path can be configured in Centralised DLP Manager (Hot Cold Standby for DC/DR) to store the forensics. Kindly confirm if this is acceptable.	Please be guided by RFP

21	15	Email DLP & 34	Integration with Security Datalake to be implemented in future will be got done without extra	Need to understand the use case. Kindly provide the same for this requirement.	It is clarified, integration will be in respect of Data / logs which are generated from the email security solutions.
22	15	Email DLP & 42	The reports should be exported to at least CSV, PDF, HTML formats	Request you to please amend the clause as : The reports should be exported to at least CSV and PDF formats	Please be guided by RFP
23	16	Email DLP & 52	Features for disabling or modifying default rules, scenarios, and configurations should be available	Word Scenarios is making the clasue look ambigious, hence request you to please amend the clause as : Features for disabling, modifying default rules, scenarios with bolean logic , configurations should be available.	It is clarified, Scenario means all possible outcomes of situations.
24	63 &64	Email APT & 8	Solution to support below files for execution: Portable Document: PDF Document: DOC, DOCX, DOT, DOCM, DOTX, DOTM, HWP, ODT, PUB, RTF, WPD, XML, XPS and other file type. Spreadsheet: CSV, ODS, SYLK, XLT, XLS, XLM, XLTX, XLSM, XLTM, XLSB, XLA, XLAM, XLL, XLSX and other file type. PowerPoint: ODP, PPS, PPT, PPTX, PPTM, POTX, POTM, PPAM and other file type. Executable: BAT, COM, DLL, EXE, HTA, JS, MACH- O, MSI, PIF, PL, PS1, PY, SCR, SH, SYS, VB, WSF and other file type. Archive File: 7Z, ACE, APK, ARJ, BZIP, CAB, CHM, DMG, GZ, ISO, JAR, LHA, LZMA,, NUPKG, RAR, TAR, TARGZ, TNEF, WAR, XAR, XZ, ZIP, ZIPX and other file type. Media: ODG, SVG, SWF, TIFF and other file type. Misc: CLASS, EML, HTML, IQY, PCAP, URL and other file type.	Most of the important file formats are already covered in the mentioned clause, but adding any "other file type" makes the clause open ended and no OEM will be able to comply to this clause technically. Hence request you to please drop the phrase : "and other file type" from complete section.	It is clarified, other file type is deleted. Incase bank desires any other file format, then the same is to be customized by the successful bidder without any additional cost to the Bank
25	64	Email APT & 9	The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal.	For wider participation, request you to please amend this clasue as : The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families	It is clarified, proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families
26	64	Email APT & 15	Solution should have Content disarm and reconstruction (CDR) capability, which protects against exploits and weaponized content that have not been seen before	OEM Specific Clause, request you to please delete this clause or make it optional for wider participation	Please be guided by RFP

27	64	Cloud Access Security Broker (CASB) & 16	The bidder should also implement a CASB solution to enable role based access to identify application including email by enforcing amalgamated policies for access through cloud from anywhere.	Need to understand the use case. CASB is a separate solution itself. Please share the complete list of detailed Specification of CASB along with Use cases or Request you to please drop the CASB from the scope of this RFP.	It is clarified, reference to CASB is in respect of the email security solution which will be interacting with the email solution in cloud.
28	37	ANNEXURE-III-ELIGIBILITY CRITERIA OF THE BIDDER & 4	The OEM must have successfully implemented Email Security Solutions including Email gateway and Email DLP/ Email ATP in at least two PSU/ Government Organizations/ BFSI/ Private Sector in India, during last three years as on date of submission of Bid with a size of at least 35,000 email users in each.	For wider participation, request you to please amend the clause as : The OEM must have successfully implemented Email Security Solutions including Email gateway / Email DLP/ Email ATP in at least two PSU/ Government Organizations/ BFSI/ Private Sector in India, During last three years as on date of submission of Bid with a size of at least 35,000 email users in each.	**Please refer Corrigendum 1.1**
29	37 & 38	ANNEXURE-III-ELIGIBILITY CRITERIA OF THE BIDDER & 11	The OEM must have successfully implemented Email Security Solutions including Email gateway and Email DLP/ Email ATP on cloud.	For wider participation, request you to please amend the clause as : The OEM must have successfully implemented Email Security Solutions including Email gateway / Email DLP/ Email ATP on hosted cloud	Please be guided by RFP

Sr. No.	RFPP age No.	RFP Clause Name & No.	RFP Clause	Bidder's Query/Suggestion/Remarks	Bank's Response/clarification
1	36	3. ELIGIBILITY CRITERIA OF THE BIDDER	The Bidder must have successfully implemented Email Security Solutions including Email gateway and Email DLP/ Email ATP in at least one PSU/ Government Organizations / BFSI / Private Sector in India, during last three years as on date of submission of Bid with a size of at least 20,000 email users	Kindly ammend this clause as" The Bidder must have successfully implemented Email Solutions in at least one PSU/ Government Organizations / BFSI / Private Sector in India, during last five years as on date of submission of Bid .	**Please refer Corrigendum 1.4**
2	36	4. ELIGIBILITY CRITERIA OF THE BIDDER	The OEM must have successfully implemented Email Security Solutions including Email gateway and Email DLP/ Email ATP in at least two PSU/ Government Organizations/ BFSI/ Private Sector in India, during last three years as on date of submission of Bid with a size of at least 35,000 email users in each.	Kindly ammend this clause as "The OEM must have successfully implemented Email Solutions including in at least two PSU/ Government Organizations/ BFSI/Private Sector in India, during last five years as on date of submission of Bid.	**Please refer Corrigendum 1.4**
3		5. ELIGIBILITY	Firm should be prime bidder and no consortium is allowed for the solution/ services to be offered	Kindly allow consortium for the rfp.	Please be guided by RFP

		CRITERIA OF THE BIDDER			
4		9. ELIGIBILITY CRITERIA OF THE BIDDER	The bidder should have a minimum turnover of INR 6 crores (Rupees Six crores) or (INR 3 Crores (Rupees Three Crores) for MSE bidders) per annum for the past three financial years i.e. FY2017-18, FY2018-19 & FY2019-20 from their Indian Operations from sale of Email Security Solutions including Email gateway and Email DLP/ Email ATP. The bidder should have positive net worth during the last three financial years i.e. FY2017-18, FY2018-19 & FY2019-20.	Kindly ammend this clause as " The bidder should have a minimum turnover of INR 6 crores (Rupees Six crores) or (INR 3 Crores (Rupees Three Crores) for MSE bidders) per annum for the past three financial years i.e. FY2017-18, FY2018-19 & FY2019-20 from their IT Operations. The bidder should have positive net worth during the last three financial years i.e. FY2017-18, FY2018-19 & FY2019-20.	**Please refer Corrigendum 1.6**
5		10. ELIGIBILITY CRITERIA OF THE BIDDER	The minimum average annual financial turnover of the OEM of the offered product during the last three years, ending on 31st March of the previous financial year, should be at least Rs.12 Crores during the last three financial years i.e. FY2017-18, FY2018-19 & FY2019-20.	Kindly amend this clause as "The minimum average annual financial turnover of the OEM from IT services during the last three years, ending on 31st March of the previous financial year, should be at least Rs.12 Crores during the last three financial years i.e. FY2017-18, FY2018-19 & FY2019-20.	**Please refer Corrigendum 1.7**
6		11. ELIGIBILITY CRITERIA OF THE BIDDER	The OEM must have successfully implemented Email Security Solutions including Email gateway and Email DLP/ Email ATP on cloud.		**Please refer Corrigendum 1.8**
7		12. ELIGIBILITY CRITERIA OF THE BIDDER	The bidder should have sold cloud email security solutions to multiple clients.		Please be guided by RFP
8			General	Kindly confirm the total number of the Email ID required ?	Please be guided by RFP
9			General	Kindly confirm the total number of the domains ?	Please be guided by RFP
10			General	Kindly specify if the Email gateway is required for bulk emails ? If yes Please mention this Bulk email service is under whose scope & also mention the no of bulk emails need to be sent per month.?	Please be guided by RFP
11				Kindly confirm any specific features required from the ESDS end for propose email security solution	Please be guided by RFP
12			General	Please suggest the bidder has to propose only single integrated solution for Email Security that covers Email gateway, email DLP and Email ATP or individual solution can be proposed	Please be guided by RFP
13	14	Data Identification & Policy	The solution should be integrated with Security Operation Centre	Please inform which SIEM solution PNB is using for integration	It is clarified, same will be shared with the successful bidder

		Management(14)			
14	36	3. ELIGIBILITY CRITERIA OF THE BIDDER	The Bidder must have successfully implemented Email Security Solutions including Email gateway and Email DLP/ Email ATP in at least one PSU/ Government Organizations / BFSI / Private Sector in India, during last three years as on date of submission of Bid with a size of at least 20,000 email users	Kindly ammend this clause as" The Bidder must have successfully implemented Email Solutions in at least one PSU/ Government Organizations / BFSI / Private Sector in India, during last five years as on date of submission of Bid .	**Please refer Corrigendum 1.4**

Sr. No.	RFPPage No.	RFP Clause Name & No.	RFP Clause	Bidder's Query/Suggestion/Remarks	Bank's Response/clarification
1	9	3. Scope of Work	The scope of work includes Email Security Solution having following services for Punjab National Bank either On-Premises or on Cloud or both as applicable	Our understanding is that bank wants to select Email Security Solutions for O365 which is cloud offering from MS. Both cloud and on premise solutions have different offerings. Kindly clarify the bank requirement is it on premise or cloud solution	Please be guided by RFP
2	36	Annexure III, ELIGIBILITY CRITERIA OF THE BIDDER, Point 4	The OEM must have successfully implemented Email Security Solutions including Email gateway and Email DLP/ Email ATP in at least two PSU/ Government Organizations/ BFSI/ Private Sector in India, during last three years as on date of submission of Bid with a size of at least 35,000 email users in each.	We request you to kindly consider the following modifications: 1. Modify reference size to at least 20,000 email in place of 35,000. 2. As OEM we do not get the copy of customer PO/work order kindly consider customer email confirmation as supporting document for the same 3. Kindly consider customer email confirmation stating that solution is currently deployed and running instead of implemented during last 3 years as a criterion	**Please refer Corrigendum 1.1**
3	37	Annexure III, ELIGIBILITY CRITERIA OF THE BIDDER, Point 10	The minimum average annual financial turnover of the OEM of the offered product during the last three years, ending on 31st March of the previous financial year, should be at least Rs.12 Crores during the last three financial years i.e. FY2017-18, FY2018-19 & FY2019-20.	As a global listed company we do not disclose country/product level financials, request you to allow submission of overall global financial statement for this requirement	**Please refer Corrigendum 1.7**
4	46	Annexure Xa, MAF, Point 6	In case of default/unable to comply with above at the time of delivery or during implementation or customization, for the software already billed, we agree to take back the supplied items without demur, if already supplied and replace it with an Original & Latest product/component. We also take full responsibility of the Solution & Service SLA as per the content even if there is any defect by our authorized Service Centre / Reseller / SI etc.	We request you to kindly remove "Customization" as these are standardise SaaS offering. Also remove "even if there is any defect by our authorized Service Centre / Reseller / SI etc."	Please be guided by RFP

5	46	Annexure Xa, MAF, Point 8	We take complete Ownership of the complete solution (Hardware & Software) being offered to Bank by M/s_____(Bidder's Name).	Kindly modify "We take ownership of the product supplied to Bank" rest will still be the bidder responsibility	Please be guided by RFP
6	47	Annexure Xb, OEM Undertaking, Point 5	In case of default/unable to comply with above at the time of delivery or during implementation or customization, for the software already billed, we agree to take back the supplied items without demur, if already supplied and replace it with an Original &Latest product/component. We also take full responsibility of the Solution& Service SLA as per the content even if there is any defect by our authorized Service Centre / Reseller / SI etc.	We request you to kindly remove "Customization" as these are standardise SaaS offering. Also remove "even if there is any defect by our authorized Service Centre / Reseller / SI etc."	Please be guided by RFP
7	47	Annexure Xb, OEM Undertaking, Point 7	We take complete Ownership of the complete solution (Hardware & Software) being offered to Bank by M/s_____(Bidder's Name).	Kindly modify "We take ownership of the product supplied to Bank" rest will still be the bidder responsibility	It is clarified, kindly specify clearly the names of software and/or hardware being offered to which ownership is to be taken by OEM
8	48	Annexure XII, PERFORMA FOR 'INDICATIVE COMMERCIAL OFFER', Point 5	Bank may place Orders for Sr. no. 1, 2 & 3 as and when required during the entire contract period at the unit rates finalized after Reverse Auction. Bank is not bound to place any minimum order. The quantity will also be as per requirement.	Our SaaS model have a single offering which includes all the three components, hence request you to kindly modify the financial format accordingly with an option for quoting a single price or combination for all the three line items	Please be guided by RFP
9	55	Annexure XV, Technical Specification, Email Security, Point 1	The proposed email security solution should software/virtual based and can be hosted over any cloud	The solution offered is SaaS based. Kindy remove "Can be hosted over any cloud"	Please be guided by RFP
10	55	Annexure XV, Technical Specification, Email Security, Point 7	The Solution should have IPV4 and IPV6 dual stack Compatibility.	Kindly remove IPV6 we currently only support IPV4	It is clarified, access to neither IPV4 nor IPV6 traffic should be dropped, due to incompatibility in the infrastructure.
11	55	Annexure XV, Technical Specification, Email Security, Point 8	The Solution should have APIs/ Connectors / scripts for integration with various security solutions in the bank like ADDM, SMS, SOAR, SIEM, Firewall etc. as applicable and bidder shall enable the requested integration without any additional cost to Bank.	Our solution can Integrate with SIEM only, kindly remove ADDM, SMS, SOAR, Firewall etc. from the requirement	Please be guided by RFP
12	55	Annexure XV, Technical Specification, Email Security, Point 9	The bidder should follow the data localization guidelines of the Government and regulators as applicable from time to time. A confirmation should be provided in this regard.	1. Guidelines from time to time is an open and broad statement to comply, Kindly modify the scope to current applicable guidelines 2. We are in process of hosting our solution in India, we request bank to consider that at the time of PO placement this requirement should be meet	Please be guided by RFP

13	55	Annexure XV, Technical Specification, Email Security, Point 11	The solution should be integrated with the case management solution and incident management solution of the bank.	Our solution can integrate with SIEM. Kindly remove this requirement	It is clarified, the solution should be integrated with the SIEM so that features of case management and incident management is available through the same for the incidents related to email security.
14	56	Annexure XV, Technical Specification, Email Security, Point 16	The Solution should have DR capabilities and functionalities so that the email security can be implemented even if email solution is shifted from one setup to another setup. This should be properly configured during implementation.	As this is a SaaS based offering, this requirement is not applicable. Kindly remove	It is clarified, solution should have DR capabilities and functionalities so that the email security is not impacted even if the email or the email security solution is shifted from one set up to another set up. This should be properly configured during the implementation.
15	56	Annexure XV, Technical Specification, Email Security, Point 26	The Solution should provide an attachment scanning capability to detect file-based spam messages	Kindly modify. "The solution should provide an attachment scanning capability to detect spam messages"	Please be guided by RFP
16	56	Annexure XV, Technical Specification, Email Security, Point 31	The solution should have at least 1500+ pre-defined content rules inbuilt with Email Security & embedded in the product	Kindly remove, this is OEM specific. Content rules are defined by customer based on business requirements	It is clarified, Bidder should provide the predefined / default content rules available in the system. The bank should have the facility to retain or delete specific rules. New rules/modified rules as required by the bank should be configured in the system before or during the implementation.
17	57	Annexure XV, Technical Specification, Email Security, Point 37	Data Directory services should be in sync and any non-existing mail id, the gateway should drop the mail at the Gateway level, and should maintain the log and sent the notification to administrator & sender.	Kindly modify the clause. SMTP rejects mail with 'Invalid-Recipient.', no bounce email notification is sent to either sender or administrator	Please be guided by RFP
18	57	Annexure XV, Technical Specification, Email Security, Point 41	The solution must allow setting SMTP greeting message, delay time and the full qualified domain name for SMTP session establishment.	Kindly remove, these settings are not valid for SaaS based deployment	**Please refer Corrigendum 1.9**
19	57	Annexure XV, Technical Specification, Email Security, Point 45	The solution must have directory harvesting and DoS prevention capabilities.	We currently support DoS prevention, Directory harvesting is on roadmap, request you to kindly allow the same to be considered for compliance	**Please refer Corrigendum 1.2**
20	57	Annexure XV, Technical Specification, Email Security, Point 46	The solution must allow the administrator to specify the re-try time for a delivery failure.	Kindly modify, "The solution should have capability to re-try for a delivery failure", we cannot configure the re-try time, these are pre defined	It is clarified, solution should have capability to re-try for a delivery failure
21	58	Annexure XV, Technical Specification, Email Security, Point 59	The Solution must have option for end user notification for email quarantining letter to be customized and click boxes that enable the user to release e-mail, report false positives, add senders to allow or block lists and direct links to personal email management portal.	Kindly remove "report false positives", our End User Quarantine portal supports all, except for reporting false positives	It is clarified, reporting false positive can also be achieved through help desk by raising ticket to OEM
22	58	Annexure XV, Technical Specification,	The solution must allow where Administrator can specify which queues can be accessed by end user.	Kindly modify "The solution must have capability to allow end user to access their own queues"	It is clarified, bidder to provide suitable solution to meet the requirement.

		Email Security, Point 60			
23	58	Annexure XV, Technical Specification, Email Security, Point 61	The Personal management portal should be a web-based UI for end users i.e. the console should be available to multiple users and multiple end points and there should be drill down features in the dashboard. They should be customizable based on needs.	Kindly remove "Customizable" from the requirement	Please be guided by RFP
24	58	Annexure XV, Technical Specification, Email Security, Point 62	The Proposed solution should allow email reply to release the email quarantined by solution.	Kindly clarify, this is more of a process not a feature. Further end used have access to quarantine queue to release the email.	Please be guided by RFP
25	58	Annexure XV, Technical Specification, Email Security, Point 64	The solution should support native system backup and software update functionality.	Kindly remove this is not applicable for SaaS based offering	The solution should support native system backup and software update functionality.
26	58	Annexure XV, Technical Specification, Email Security, Point 69	The Proposed solution should be able to consolidate reports from multiple boxes for centralized logging and reporting.	Kindly remove this is not applicable for SaaS based offering	Please be guided by RFP
27	58	Annexure XV, Technical Specification, Email Security, Point 72	The Proposed solution should have True Source IP Detection and Connection Blocking feature should work even if Email Security is deployed behind Corporate Email Relay Server/Firewall SMTP.	Kindly remove this is not applicable for SaaS based offering	Bidder may propose alternate functionality which meets the requirement
28	59	Annexure XV, Technical Specification, Email Security, Point 78	The Proposed Solution should the configuration of workflow. End user's manager should be able to release the quarantined email via replying to the notification email from his inbox	Kindly remove, OEM specific	This is not OEM specific. Identified Admin Users should be able to release the quarantined email.
29	59	Annexure XV, Technical Specification, Email Security, Point 81	The solution should have a central end user management portal for multiple appliances	Kindly remove this is not applicable for SaaS based offering	Please be guided by RFP
30	60	Annexure XV, Technical Specification, Email DLP, Point 6	The solution should have features for masking of email ids of customers/third parties mentioned in the email being forwarded to service providers etc. In case solution is not having this feature then it should be customized for our Bank before UAT sign-off.	Kindly remove, masking is not possible	This is an email DLP feature and is required.
31	60	Annexure XV, Technical Specification, Email DLP, Point 8	The solution should have a comprehensive list of pre-defined policies and templates with over 2000+ patterns to identify and classify information pertaining to different industry like Banking etc.	kindly modify, we support 240+ DLP templates. 2000+ requirement is OEM specific.	The Bidder should provide the predefined / default content rules available in the system. The bank should have the facility to retain or delete specific rules . New rules/modified rules as required by the bank should be configured in the system before or during the implementation.

32	60	Annexure XV, Technical Specification, Email DLP, Point 11	The solution should be integrated with external data storage for the forensics over path to Big Data Lake/Data ware house as required.	Kindly remove this is not applicable for SaaS based offering	Please be guided by RFP
33	60	Annexure XV, Technical Specification, Email DLP, Point 12	The solution should have separate management and Data Layer.	Kindly remove this is not applicable for SaaS based offering	Please be guided by RFP
34	60	Annexure XV, Technical Specification, Email DLP, Point 13	There should be feasibility of integration with any Data Classification solution/rules where ever applicable, with 3rd party Data Classification tool.	Kindly remove, OEM specific	Please be guided by RFP
35	60	Annexure XV, Technical Specification, Email DLP, Point 18	The solution should be able to do full binary fingerprint of files and also should be able to detect even if partial information gets leaks from fingerprinted files or folders	Kindly remove, this is not applicable as this requirement is more of endpoint DLP/crawler	The feature is required in email DLP
36	60	Annexure XV, Technical Specification, Email DLP, Point 20	The solution should be able to fingerprint only specific fields or columns within a database and should be able to identify information from databases by correlating information residing in different columns in a database	Kindly remove, this is not applicable as this requirement is more of endpoint DLP/crawler	The feature is required in email DLP
37	60	Annexure XV, Technical Specification, Email DLP, Point 21	The Solution should have advanced Machine Learning – Ability to automatically learn sensitive information from copies of information that needs to be protected and also automatically learn false positives.	Kindly remove. Sensitive information need to be defined by bank based on business requirements.	The feature is required in email DLP
38	60	Annexure XV, Technical Specification, Email DLP, Point 22	The solution should enforce policies to detect low and slow data leaks for the transaction going in separate emails.	Kindly remove, this is extension of above fingerprinting clause.	The feature is required in email DLP
39	60	Annexure XV, Technical Specification, Email DLP, Point 23	The solution should be able to enforce policies to detect data leaks even through image files through OCR technology.	Kindly remove, OEM specific	Bidder may propose alternate functionality which meets the requirement
40	61	Annexure XV, Technical Specification, Email DLP, Point 25	The solution should be able to identify and block malicious activity like data thefts through files encrypted using non-standard algorithms.	Kindly modify "The solution should be able to identify and block malicious activity like data thefts through files"	Bidder may propose alternate functionality which meets the requirement
41	61	Annexure XV, Technical Specification, Email DLP, Point 26	The Proposed DLP Solution must be GDPR and CCPA Compliant	Kindly remove "CCPA" from clause	**Please refer Corrigendum 1.10**

42	61	Annexure XV, Technical Specification, Email DLP, Point 27	The solution should be able to alert and notify sender, sender's manager and the policy owner whenever there is a policy violation, Different notification templates for different audience should be possible	Kindly modify, Admin can configure the notifications to be sent to anyone within the organization. Remove sender, sender manager, policy owner from clause	It is clarified, admin should be able to configure the notifications as per requirement.
43	61	Annexure XV, Technical Specification, Email DLP, Point 28	The solution should support quarantine as an action for email policy violations and should allow the sender's manager to review the mail and provide permissions for him to release the mail without logging into the UI	Kindly modify, we supports quarantine as an action for policy violation. Besides the users, only the admin can view/release such emails, from the UI. Remove "sender's manager to review the mail and provide permissions for him to release the mail without logging into the UI"	This is functionality desired. Bidder to provide suitable solution as per RFP.
44	61	Annexure XV, Technical Specification, Email DLP, Point 30	The incident should display the complete identity of the sender (Full name, Business unit, manager name etc.) and destination of transmission for all network and endpoint channels. The solution should also allow assigning of incidents to a specific incident manager	Kindly remove, OEM specific	These are functionalities and is not OEM specific. Bidder/OEM may provide alternate mechanism to meet requirement.
45	61	Annexure XV, Technical Specification, Email DLP, Point 31	The solution should provide automatic notification to incident managers when a new incident is assigned to them and the incident should not allow for deletion even by the product administrator	Kindly remove. OEM Specific	These are functionalities and is not OEM specific. Bidder/OEM may provide alternate mechanism to meet requirement.
46	61	Annexure XV, Technical Specification, Email DLP, Point 32	The solution should allow a specific incident manager to manage incidents of specific policy violation, specific user groups etc.	Kindly remove. OEM Specific	These are functionalities and is not OEM specific. Bidder/OEM may provide alternate mechanism to meet requirement.
47	61	Annexure XV, Technical Specification, Email DLP, Point 33	The solution should have options for managing and remediating incidents through email by providing incident management options within the in the notification email itself.	Kindly remove. OEM Specific	These are functionalities and is not OEM specific. Bidder/OEM may provide alternate mechanism to meet requirement.
48	61	Annexure XV, Technical Specification, Email DLP, Point 34	Integration with Security Datalake to be implemented in future will be got done without extra cost.	Kindly remove this is not applicable for SaaS based offering	It is clarified, integration will be in respect of Data / logs which are generated from the email security solutions.
49	61	Annexure XV, Technical Specification, Email DLP, Point 36	The system should create separate roles for technical administration of servers, user administration, policy creation and editing, incident remediation, and incident viewing for data at rest, in motion, or at the endpoint	Kindly modify, we allows admin to create subaccounts for with different permission and management scope. Kindly "delete data in rest or at the endpoint" from the clause	Please be guided by RFP
50	62	Annexure XV, Technical Specification, Email DLP, Point 45	The proposed solution should provide Incident Workflow capabilities where user/Business Manager can remediate the DLP policy violations actions from handsets/emails without logging into the Management Console	Kindly remove. OEM Specific	These are functionalities and is not OEM specific. Bidder/OEM may provide alternate mechanism to meet requirement

51	62	Annexure XV, Technical Specification, Email DLP, Point 47	The Proposed DLP engine must performs a post-processing incident grouping step to avoid displaying related incidents in different cases. All incidents from the same user that have the same classification are combined into a group and DLP case card.	Kindly remove. OEM Specific	These are functionalities and is not OEM specific. Bidder/OEM may provide alternate mechanism to meet requirement
52	62	Annexure XV, Technical Specification, Email DLP, Point 48	The Proposed Solution dashboard must display the number of cases in the designated period that fall above the risk score threshold that you've selected. Risk score thresholds must be customizable and instantly produce a report to prioritize the cases from high-to-low risk levels by leveraging analytics or machine learning technologies.	Kindly remove. OEM Specific	Bidder may propose alternate functionality which meets the requirement
53	63	Annexure XV, Technical Specification, Email DLP, Point 49	Workflow operations in DLP networking and mobile reports can now be applied to all filtered incidents or to selected incidents only. This includes operations such as: -Assigning incidents -Changing incident status -Changing incident severity -Ignoring incidents -Tagging incidents -Adding comments	Kindly remove. OEM Specific	**Please refer Corrigendum 1.11**
54	63	Annexure XV, Technical Specification, Email APT, Point 6	It should support execution of OS X files and Android applications.	Kindly remove "Android Applications" from clause	It should support execution of OS Xfiles and android applications if such functionalities of mobile platform support are included in email security solution provided.
55	63	Annexure XV, Technical Specification, Email APT, Point 7	It should support the execution of various OS or support hardware emulation	Kindly clarify the OS on which bank expect the support. We support windows and mac OS.	Please be guided by RFP
56	63	Annexure XV, Technical Specification, Email APT, Point 8	Solution to support below files for execution: Portable Document: PDF Document: DOC, DOCX, DOT, DOCM, DOTX, DOTM, HWP, ODT, PUB, RTF, WPD, XML, XPS and other file type. Spreadsheet: CSV, ODS, SYLK, XLT, XLS, XLM, XLTX, XLSM, XLTM, XLSB, XLA, XLAM, XLL, XLSX and other file type. PowerPoint: ODP, PPS, PPT, PPTX, PPTM, POTX, POTM, PPAM and other file type. Executable: BAT, COM, DLL, EXE, HTA, JS, MACH-O, MSI, PIF, PL, PS1, PY, SCR, SH, SYS, VB, WSF and other file type. Archive File: 7Z, ACE, APK, ARJ, BZIP, CAB, CHM, DMG, GZ, ISO, JAR, LHA, LZMA,, NUPKG, RAR, TAR, TARGZ, TNEF, WAR, XAR, XZ, ZIP, ZIPX and other file type. Media: ODG, SVG, SWF, TIFF and other file type Misc: CLASS, EML, HTML, IQY, PCAP, URL and other file type.	Kindly remove the following formats as they are not supported. HWP, ODT, WPD, XPS, ODS, SYLK, XLL, ODP, POTX, PIF, PL, PY, SH, LZMA, NUPKG, WAR, XAR, ZIPX, ODG, TIFF, PCAP	It is clarified, other file type is deleted. Incase bank desires any other file format, then the same is to be customized by the successful bidder without any additional cost to the Bank
57	9	Section 3 : Scope of Work	The Bidder/SI shall be responsible to ensure and deliver all the functional, technical and operational	Please confirm whether the scope of Bidder is limited to implementation(installation ,	Please be guided by RFP

			requirements for all the products with proper co-ordination with PNB	configuration and activation) and whether the management of the solution after implementation is not in the scope of bidder	
58	10	Email Security Point 10	Implementation architecture for DC-DR along with the functions performed as per DR scenario should be provided containing full details.	Please confirm whether DC /DR is valid if the bidder is providing solution on the cloud	It is clarified, solution should have DR capabilities and functionalities so that the email security is not impacted even if the email or the email security solution is shifted from one set up to another set up. This should be properly configured during the implementation.
59	10	Email Security Point 11	The solution should be integrated with the case management solution and incident management solution of the bank.	Please confirm which case management and incident management solution is implemented at PNB's site	Case management – Service Plus Service Desk from CA-Broadcom. Incident Management part of RSA and Arcsight SIEM
60	13	Data Identification & Policy Management Point:8	The solution should have a comprehensive list of pre-defined policies and templates with over 2000+ patterns to identify and classify information pertaining to different industry like Banking etc.	Please confirm whether classification of data has already been done in the organisation	It is clarified, Bidder should provide the predefined / default content rules available in the system. The bank should have the facility to retain or delete specific rules. New rules/modified rules as required by the bank should be configured in the system before or during the implementation.
61	16	Email ATP Point: 16	The bidder should also implement a CASB solution to enable role based access to identify application including email by enforcing amalgamated policies for access through aloud from anywhere	Please confirm whether PNB need a dedicated CASB solution If Yes, what is the overall scope & sizing of CASB solution	The reference to CASB is in respect of the email security solution which will be interacting with the email solution in cloud.
62	37	ELIGIBILITY CRITERIA OF THE BIDDER	The bidder should have a minimum turnover of INR 6 crores (Rupees Six crores) or (INR 3 Crores (Rupees Three Crores) for MSE bidders) per annum for the past three financial years i.e. FY2017-18, FY2018-19 & FY2019-20 from their Indian Operations from sale of Email Security Solutions including Email gateway and Email DLP/ Email ATP. The bidder should have positive net worth during the last three financial years i.e. FY2017-18, FY2018-19 & FY2019-20	Request PNB to relax the clause to The bidder should have a minimum turnover of INR 6 crores (Rupees Six crores) or (INR 3 Crores (Rupees Three Crores) for MSE bidders) per annum for the past three financial years i.e. FY2017-18, FY2018-19 & FY2019-20 from their Indian Operations from sale of Security Solutions The bidder should have positive net worth during the last three financial years i.e. FY2017-18, FY2018-19 & FY2019-20	**Please refer Corrigendum 1.6**
63	59	Email DLP & ATP	NA	Please confirm the log storage and retention period for Email DLP solution & Email ATP	It is clarified, data has to be preserved online for 6 months and thereafter it has to be archived and provided to bank as and when required.
64	36	ELIGIBILITY CRITERIA OF THE BIDDER Point :3	The Bidder must have successfully implemented Email Security Solutions including Email gateway and Email DLP/ Email ATP in at least one PSU/ Government Organizations / BFSI / Private Sector in India, during last three years as on date of submission of Bid with a size of at least 20,000 email users	Request PNB to relax the clause to The Bidder must have successfully implemented Email Security Solutions including Email gateway and Email DLP/ Email ATP in at least one PSU/ Government Organizations / BFSI / Private Sector in India, during last three years as on date of submission of Bid with a size of at least 10,000 email users	**Please refer Corrigendum 1.4**
65	38	ELIGIBILITY CRITERIA OF	The bidder should have sold cloud email security solutions to multiple clients.	Request PNB to relax the clause to	**Please refer Corrigendum 1.12**

		THE BIDDER Point 12		The bidder should have sold email security solutions to multiple clients.	
66	30	Training	The training should cover complete administration & day to day maintenance of the solution and should be classroom based.	Please confirm whether the training can be provided in an online classroom mode	Please be guided by RFP
67	10	Detailed Scope of work	The Bidder shall be responsible to implement the Email Security solution as per the requirement of the RFP to secure the Bank's Email infrastructure deployed (i.e. Microsoft O365)	Kindly provide the details of existing license of 0365 Please confirm whether providing license will be a top-up on existing license or bidder has to provide a fresh license	It is clarified, bidder has to provide fresh license.
68	10	Detailed Scope of work	The Bidder shall be responsible to implement the Email Security solution as per the requirement of the RFP to secure the Bank's Email infrastructure deployed (i.e. Microsoft O365)	Do we need to have a consortium with the licensee provider	Please be guided by RFP
69	10	Email Security & 6	The solution should have features to build scenarios for actions on emails.	Please clarify the scenario meaning, as its generic . Our understanding is different types of filters, Is our understanding correct ?	It is clarified, Scenario means all possible outcomes of situations.
70	10	Email Security & 16	The Solution should have DR capabilities and functionalities so that the email security can be implemented even if email solution is shifted from one setup to another setup. This should be properly configured during implementation.	Each OEM has its own way of setting the DR capability, This clause is limiting our participation, Hence request you to please amend this clause as: The Solution should have DR capabilities and functionalities so that the email security is not impacted even if email solution is shifted from one setup to another setup. This should be properly configured during implementation.	It is clarified, solution should have DR capabilities and functionalities so that the email security is not impacted even if the email or the email security solution is shifted from one set up to another set up. This should be properly configured during the implementation.
71	11	Email Security & 22	The solution virus engine should support scanning by inbound, outbound and internal direction and configure the policy per direction.	Internal Mail scanning requires visiability of email via a MTA and in that case Mail Solution has to route the emails to Mail Security solution via MTA. Kindly confirm if Bank mail solution can do the routing of internal domain mails, if not then please remove the Internal direction from the clause & amend as : The solution virus engine should support scanning by inbound, outbound and configure the policy.	It is clarified, please be guided by Microsoft Office 365 email architecture. The solution virus engine should support scanning by inbound, outbound direction and configure the policy per direction. Bidder should provide suitable solution for scanning internal emails in addition to above, if it is not handled at the gateway. Further, Please be guided by Microsoft Office 365 email architecture
72	11	Email Security & 35	The solution should be able to restrict incoming, outgoing and internal mails based on file types, file size and also by file name and also through a combination of them.	Internal Mail scanning requires visiability of email via a MTA and in that case Mail Solution has to route the emails to Mail Security solution via MTA. Kindly confirm if Bank mail solution can do the routing of internal domain mails, if not then please remove the Internal mails from the clause & amend as : The solution should be able to restrict incoming and outgoing mails based on file types, file size and also by file name and also through a combination of them.	It is clarified, solution should be able to restrict incoming, outgoing and internal mails based on file types, file size and also by file name and also through a combination of them if it is routed through the Gateway.
73	11	Email Security & 36	The solution should provide the local domain identification and should drop any email with source email ID not exist.	Ask is not clear however , local domain is the protected domain for which the mails will be accpeted and if sender address is blank it will	Please be guided by RFP

				be dropped. Hope our understanding is correct, please confirm.	
74	13	Email Security & 75	The Proposed solution should provide capabilities for end users to search on quarantined messages specific to them. The solution should allow end users to release mails from quarantine if approved.	For wider participation, please amend the clause as : The Proposed solution should provide capabilities for end users to search on quarantined messages specific to them. The solution should allow end users to release mails from quarantine	The proposed solution should provide capabilities for defined users (like Helpdesk, Administrators etc) to search on quarantined messages and release emails as required
75	13	Email DLP & 5	The solution should support Email DLP deployment on cloud for Office 365. All licenses required for the same should be included and management should be from the same centralized management platform	Request for Clarification that cloud mentioned can be referred as hosted deployment as well like mentioned in Email Security Clause 1, Hence request you to please amend the clause as : The solution should support Email DLP deployment on cloud/ hosted environmnet for Office 365. All licenses required for the same should be included and management should be from the same centralized management platform	It is clarified, solution should support Email DLP deployment on cloud for Office 365. All licenses required for the same should be included and management should be from the centralized management platform
76	13	Email DLP & 11	The solution should be integrate with external data storage for the forensics over path to Big Data Lake/Data ware house as required.	Specify the data warehouse integration reuqired , we currently support the DLP integration with expoert to AWS and Azure for the log management POV for the datalake. Moreover any shared path can be configured in Centralised DLP Manager (Hot Cold Standby for DC/DR) to store the forensics	Please be guided by RFP
77	15	Email DLP & 42	The reports should be exported to at least CSV, PDF, HTML formats	Request you to please amend the clause as : The reports should be exported to at least CSV and PDF formats	Please be guided by RFP
78	16	Email DLP & 52	Features for disabling or modifying default rules, scenarios, and configurations should be available	Word Scenarios is making the clasue look ambigious, hence request you to please amend the clause as : Features for disabling, modifying default rules, scenarios with bolean logic , configurations should be available.	It is clarified, Scenario means all possible outcomes of situations.
79	64	Email APT & 9	The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal.	For wider participation, request you to please amend this clasue as : The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families	The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families
80	37 & 38	ANNEXURE-III-ELIGIBILITY CRITERIA OF THE BIDDER & 11	The OEM must have successfully implemented Email Security Solutions including Email gateway and Email DLP/ Email ATP on cloud.	For wider participation, request you to please amend the clause as : The OEM must have successfully implemented Email Security Solutions including Email gateway / Email DLP/ Email ATP on hosted cloud	Please be guided by RFP

Sr. No.	RFPPage No.	RFP Clause Name & No.	RFP Clause	Bidder's Query/Suggestion/Remarks	Bank's Response/clarification
1	37	Clause no. 7	The bidder should have support centers in Delhi NCR and Mumbai	What documents are needed in support of this clause. Also what is the minimum number of support engineers required.	Please be guided by RFP
2	38	Clause no. 20	Power of Attorney executed on stamp paper and copy of board resolution	From where we can purchase the stamp paper (Delhi & Mumbai). Also what should be the value of stamp paper.	Please be guided by the extent regulations.
3	38	Clause no. 17	Escalation Matrix and Details of Support Centre (Both OEM & Bidder)	Can OEM and Bidder be the same entity or they have to be different.	There is no restriction of OEM being the bidder. However all clauses as required for OEM and Bidder need to be complied.

Sr. No.	RFPPage No.	RFP Clause Name & No.	RFP Clause	Bidder's Query/Suggestion/Remarks	Bank's Response/clarification
1.	9	3. Scope of Work	The scope of work includes Email Security Solution having following services for Punjab National Bank either On-Premises or on Cloud or both as applicable	Our understanding is that bank want to select Email Security Solutions for O365 which is cloud offering from MS. Both cloud and on premise solutions have different offerings. Kindly clarify the bank requirement is it on premise or cloud solution	Please be guided by RFP
2.	36	Annexure III, ELIGIBILITY CRITERIA OF THE BIDDER, Point 4	The OEM must have successfully implemented Email Security Solutions including Email gateway and Email DLP/ Email ATP in at least two PSU/ Government Organizations/ BFSI/ Private Sector in India, during last three years as on date of submission of Bid with a size of at least 35,000 email users in each.	We request you to kindly consider the following modifications: 1. Modify reference size to at least 20,000 email in place of 35,000. 2. As OEM we do not get the copy of customer PO/work order kindly consider customer email confirmation as supporting document for the same 3. Kindly consider customer email confirmation stating that solution is currently deployed and running instead of implemented during last 3 years as a criterion	**Please refer Corrigendum 1.1**
3.	37	Annexure III, ELIGIBILITY CRITERIA OF THE BIDDER, Point 10	The minimum average annual financial turnover of the OEM of the offered product during the last three years, ending on 31st March of the previous financial year, should be at least Rs.12 Crores during the last three financial years i.e. FY2017-18, FY2018-19 & FY2019-20.	As a global listed company we do not disclose country/product level financials, request you to allow submission of overall global financial statement for this requirement	**Please refer Corrigendum 1.7**
4.	46	Annexure Xa, MAF, Point 6	In case of default/unable to comply with above at the time of delivery or during implementation or customization, for the software already billed, we agree to take back the supplied items without demur, if already supplied and replace it with an Original & Latest product/component. We also take full responsibility of the Solution & Service SLA as per the content even if there is any defect by our authorized Service Centre / Reseller / SI etc.	We request you to kindly remove "Customization" as these are standardise SaaS offering. Also remove "even if there is any defect by our authorized Service Centre / Reseller / SI etc."	Please be guided by RFP
5.	46	Annexure Xa, MAF, Point 8	We take complete Ownership of the complete solution (Hardware & Software) being offered to Bank by M/s_____(Bidder's Name).	Kindly modify "We take ownership of the product supplied to Bank" rest will still be the bidder responsibility	Please be guided by RFP

6.	47	Annexure Xb, OEM Undertaking, Point 5	In case of default/unable to comply with above at the time of delivery or during implementation or customization, for the software already billed, we agree to take back the supplied items without demur, if already supplied and replace it with an Original &Latest product/component. We also take full responsibility of the Solution& Service SLA as per the content even if there is any defect by our authorized Service Centre / Reseller / SI etc.	We request you to kindly remove "Customization" as these are standardise SaaS offering. Also remove "even if there is any defect by our authorized Service Centre / Reseller / SI etc."	Please be guided by RFP
7.	47	Annexure Xb, OEM Undertaking, Point 7	We take complete Ownership of the complete solution (Hardware & Software) being offered to Bank by M/s_____(Bidder's Name).	Kindly modify "We take ownership of the product supplied to Bank" rest will still be the bidder responsibility	Please be guided by RFP
8.	48	Annexure XII, PERFORMA FOR 'INDICATIVE COMMERCIAL OFFER', Point 5	Bank may place Orders for Sr. no. 1, 2 & 3 as and when required during the entire contract period at the unit rates finalized after Reverse Auction. Bank is not bound to place any minimum order. The quantity will also be as per requirement.	Our SaaS model have a single offering which includes all the three components, hence request you to kindly modify the financial format accordingly with an option for quoting a single price or combination for all the three line items	Please be guided by RFP
9.	55	Annexure XV, Technical Specification, Email Security, Point 1	The proposed email security solution should software/virtual based and can be hosted over any cloud	The solution offered is SaaS based. Kindy remove "Can be hosted over any cloud"	Please be guided by RFP
10	55	Annexure XV, Technical Specification, Email Security, Point 7	The Solution should have IPV4 and IPV6 dual stack Compatibility.	Kindly remove IPV6 we currently only support IPV4	It is clarified, access to neither IPV4 nor IPV6 traffic should be dropped, due to incompatibility in the infrastructure.
11	55	Annexure XV, Technical Specification, Email Security, Point 8	The Solution should have APIs/ Connectors / scripts for integration with various security solutions in the bank like ADDM, SMS, SOAR, SIEM, Firewall etc. as applicable and bidder shall enable the requested integration without any additional cost to Bank.	Our solution can Integrate with SIEM only, kindly remove ADDM, SMS, SOAR, Firewall etc. from the requirement	Please be guided by RFP
12	55	Annexure XV, Technical Specification, Email Security, Point 9	The bidder should follow the data localization guidelines of the Government and regulators as applicable from time to time. A confirmation should be provided in this regard.	1. Guidelines from time to time is an open and broad statement to comply, Kindly modify the scope to current applicable guidelines 2. We are in process of hosting our solution in India, we request bank to consider that at the time of PO placement this requirement should be meet	Please be guided by RFP
13	55	Annexure XV, Technical Specification, Email Security, Point 11	The solution should be integrated with the case management solution and incident management solution of the bank.	Our solution can integrate with SIEM. Kindly remove this requirement	The solution should be integrated with the SIEM so that features of case management and incident management is available through the same for the incidents related to email security.
14	56	Annexure XV, Technical Specification, Email Security, Point 16	The Solution should have DR capabilities and functionalities so that the email security can be implemented even if email solution is shifted from one setup to another setup. This should be properly configured during implementation.	As this is a SaaS based offering, this requirement is not applicable. Kindly remove	It is clarified, solution should have DR capabilities and functionalities so that the email security is not impacted even if the email or the email security solution is shifted from one set up to another set up. This should be properly configured during the implementation.

15	56	Annexure XV, Technical Specification, Email Security, Point 26	The Solution should provide an attachment scanning capability to detect file-based spam messages	Kindly modify. "The solution should provide an attachment scanning capability to detect spam messages"	Please be guided by RFP
16	56	Annexure XV, Technical Specification, Email Security, Point 31	The solution should have at least 1500+ pre-defined content rules inbuilt with Email Security & embedded in the product	Kindly remove, this is OEM specific. Content rules are defined by customer based on business requirements	The Bidder should provide the predefined / default content rules available in the system. The bank should have the facility to retain or delete specific rules. New rules/modified rules as required by the bank should be configured in the system before or during the implementation.
17	57	Annexure XV, Technical Specification, Email Security, Point 37	Data Directory services should be in sync and any non-existing mail id, the gateway should drop the mail at the Gateway level, and should maintain the log and sent the notification to administrator & sender.	Kindly modify the clause. SMTP rejects mail with 'Invalid-Recipient.', no bounce email notification is sent to either sender or administrator	Please be guided by RFP
18	57	Annexure XV, Technical Specification, Email Security, Point 41	The solution must allow setting SMTP greeting message, delay time and the full qualified domain name for SMTP session establishment.	Kindly remove, these settings are not valid for SaaS based deployment	**Please refer Corrigendum 1.9**
19	57	Annexure XV, Technical Specification, Email Security, Point 45	The solution must have directory harvesting and DoS prevention capabilities.	We currently support DoS prevention, Directory harvesting is on roadmap, request you to kindly allow the same to be considered for compliance	**Please refer Corrigendum 1.2**
20	57	Annexure XV, Technical Specification, Email Security, Point 46	The solution must allow the administrator to specify the re-try time for a delivery failure.	Kindly modify, "The solution should have capability to re-try for a delivery failure", we cannot configure the re-try time, these are pre-defined	It is clarified, solution should have capability to re-try for a delivery failure.
21	58	Annexure XV, Technical Specification, Email Security, Point 59	The Solution must have option for end user notification for email quarantining letter to be customized and click boxes that enable the user to release e-mail, report false positives, add senders to allow or block lists and direct links to personal email management portal.	Kindly remove "report false positives", our End User Quarantine portal supports all, except for reporting false positives	It is clarified, reporting false positive can also be achieved through help desk by raising ticket to OEM
22	58	Annexure XV, Technical Specification, Email Security, Point 60	The solution must allow where Administrator can specify which queues can be accessed by end user.	Kindly modify "The solution must have capability to allow end user to access their own queues"	It is clarified, bidder to provide suitable solution to meet the requirement.
23	58	Annexure XV, Technical Specification, Email Security, Point 61	The Personal management portal should be a web-based UI for end users i.e. the console should be available to multiple users and multiple end points and there should be drill down features in the dashboard. They should be customizable based on needs.	Kindly remove "Customizable" from the requirement	Please be guided by RFP
24	58	Annexure XV, Technical Specification, Email Security, Point 62	The Proposed solution should allow email reply to release the email quarantined by solution.	Kindly clarify, this is more of a process not a feature. Further end used have access to quarantine queue to release the email.	Please be guided by RFP

25	58	Annexure XV, Technical Specification, Email Security, Point 64	The solution should support native system backup and software update functionality.	Kindly remove this is not applicable for SaaS based offering	The solution should support native system backup and software update functionality.
26	58	Annexure XV, Technical Specification, Email Security, Point 69	The Proposed solution should be able to consolidate reports from multiple boxes for centralized logging and reporting.	Kindly remove this is not applicable for SaaS based offering	Please be guided by RFP
27	58	Annexure XV, Technical Specification, Email Security, Point 72	The Proposed solution should have True Source IP Detection and Connection Blocking feature should work even if Email Security is deployed behind Corporate Email Relay Server/Firewall SMTP.	Kindly remove this is not applicable for SaaS based offering	Bidder may propose alternate functionality which meets the requirement
28	59	Annexure XV, Technical Specification, Email Security, Point 78	The Proposed Solution should the configuration of workflow. End user's manager should be able to release the quarantined email via replying to the notification email from his inbox	Kindly remove, OEM specific	Please be guided by RFP
29	59	Annexure XV, Technical Specification, Email Security, Point 81	The solution should have a central end user management portal for multiple appliances	Kindly remove this is not applicable for SaaS based offering	Please be guided by RFP
30	60	Annexure XV, Technical Specification, Email DLP, Point 6	The solution should have features for masking of email ids of customers/third parties mentioned in the email being forwarded to service providers etc. In case solution is not having this feature then it should be customized for our Bank before UAT sign-off.	Kindly remove, masking is not possible	It is clarified, these are regulatory guidelines which need to be handled.
31	60	Annexure XV, Technical Specification, Email DLP, Point 8	The solution should have a comprehensive list of pre-defined policies and templates with over 2000+ patterns to identify and classify information pertaining to different industry like Banking etc.	kindly modify, we support 240+ DLP templates. 2000+ requirement is OEM specific.	The Bidder should provide the predefined / default content rules available in the system. The bank should have the facility to retain or delete specific rules. New rules/modified rules as required by the bank should be configured in the system before or during the implementation.
32	60	Annexure XV, Technical Specification, Email DLP, Point 11	The solution should be integrated with external data storage for the forensics over path to Big Data Lake/Data ware house as required.	Kindly remove this is not applicable for SaaS based offering	Please be guided by RFP
33	60	Annexure XV, Technical Specification, Email DLP, Point 12	The solution should have separate management and Data Layer.	Kindly remove this is not applicable for SaaS based offering	Please be guided by RFP
34	60	Annexure XV, Technical Specification, Email DLP, Point 13	There should be feasibility of integration with any Data Classification solution/rules where ever applicable, with 3rd party Data Classification tool.	Kindly remove, OEM specific	Please be guided by RFP
35	60	Annexure XV, Technical Specification,	The solution should be able to do full binary fingerprint of files and also should be able to detect	Kindly remove, this is not applicable as this requirement is more of endpoint DLP/crawler	Please be guided by RFP

		Email DLP, Point 18	even if partial information gets leaks from fingerprinted files or folders		
36	60	Annexure XV, Technical Specification, Email DLP, Point 20	The solution should be able to fingerprint only specific fields or columns within a database and should be able to identify information from databases by correlating information residing in different columns in a database	Kindly remove, this is not applicable as this requirement is more of endpoint DLP/crawler	**Solution if applicable to email security, to be provided.**
37	60	Annexure XV, Technical Specification, Email DLP, Point 21	The Solution should have advanced Machine Learning – Ability to automatically learn sensitive information from copies of information that needs to be protected and also automatically learn false positives.	Kindly remove. Sensitive information need to be defined by bank based on business requirements.	Please be guided by RFP
38	60	Annexure XV, Technical Specification, Email DLP, Point 22	The solution should enforce policies to detect low and slow data leaks for the transaction going in separate emails.	Kindly remove, this is extension of above fingerprinting clause.	**Solution if applicable to email security, to be provided.**
39	60	Annexure XV, Technical Specification, Email DLP, Point 23	The solution should be able to enforce policies to detect data leaks even through image files through OCR technology.	Kindly remove, OEM specific	Bidder may propose alternate functionality which meets the requirement
40	61	Annexure XV, Technical Specification, Email DLP, Point 25	The solution should be able to identify and block malicious activity like data thefts through files encrypted using non-standard algorithms.	Kindly modify "The solution should be able to identify and block malicious activity like data thefts through files"	Bidder may propose alternate functionality which meets the requirement
41	61	Annexure XV, Technical Specification, Email DLP, Point 26	The Proposed DLP Solution must be GDPR and CCPA Compliant	Kindly remove "CCPA" from clause	**Please refer Corrigendum 1.10**
42	61	Annexure XV, Technical Specification, Email DLP, Point 27	The solution should be able to alert and notify sender, sender's manager and the policy owner whenever there is a policy violation, Different notification templates for different audience should be possible	Kindly modify, Admin can configure the notifications to be sent to anyone within the organization. Remove sender, sender manager, policy owner from clause	It is clarified, admin should be able to configure the notifications as per requirement.
43	61	Annexure XV, Technical Specification, Email DLP, Point 28	The solution should support quarantine as an action for email policy violations and should allow the sender's manager to review the mail and provide permissions for him to release the mail without logging into the UI	Kindly modify, we support quarantine as an action for policy violation. Besides the users, only the admin can view/release such emails, from the UI. Remove "sender's manager to review the mail and provide permissions for him to release the mail without logging into the UI"	This is functionality desired. Bidder to provide suitable solution as per RFP.
44	61	Annexure XV, Technical Specification, Email DLP, Point 30	The incident should display the complete identity of the sender (Full name, Business unit, manager name etc.) and destination of transmission for all network and endpoint channels. The solution should also allow assigning of incidents to a specific incident manager	Kindly remove, OEM specific	These are functionalities and is not OEM specific. Bidder/OEM may provide alternate mechanism to meet requirement.
45	61	Annexure XV, Technical Specification,	The solution should provide automatic notification to incident managers when a new incident is assigned to them and the incident should not allow for deletion even by the product administrator	Kindly remove. OEM Specific	These are functionalities and is not OEM specific. Bidder/OEM may provide alternate mechanism to meet requirement.

		Email DLP, Point 31			
46	61	Annexure XV, Technical Specification, Email DLP, Point 32	The solution should allow a specific incident manager to manage incidents of specific policy violation, specific user groups etc.	Kindly remove. OEM Specific	These are functionalities and is not OEM specific. Bidder/OEM may provide alternate mechanism to meet requirement.
47	61	Annexure XV, Technical Specification, Email DLP, Point 33	The solution should have options for managing and remediating incidents through email by providing incident management options within the in the notification email itself.	Kindly remove. OEM Specific	Bidder can indicate alternate functionalities provided to address the required feature.
48	61	Annexure XV, Technical Specification, Email DLP, Point 34	Integration with Security Datalake to be implemented in future will be got done without extra cost.	Kindly remove this is not applicable for SaaS based offering	Integration will be in respect of Data / logs which are generated from the email security solutions.
49	61	Annexure XV, Technical Specification, Email DLP, Point 36	The system should create separate roles for technical administration of servers, user administration, policy creation and editing, incident remediation, and incident viewing for data at rest, in motion, or at the endpoint	Kindly modify, we allows admin to create subaccounts for with different permission and management scope. Kindly "delete data in rest or at the endpoint" from the clause	Please be guided by RFP
50	62	Annexure XV, Technical Specification, Email DLP, Point 45	The proposed solution should provide Incident Workflow capabilities where user/Business Manager can remediate the DLP policy violations actions from handsets/emails without logging into the Management Console	Kindly remove. OEM Specific	It is clarified, Bidder can indicate alternate functionalities provided to address the required feature.
51	62	Annexure XV, Technical Specification, Email DLP, Point 47	The Proposed DLP engine must performs a post-processing incident grouping step to avoid displaying related incidents in different cases. All incidents from the same user that have the same classification are combined into a group and DLP case card.	Kindly remove. OEM Specific	It is clarified, bidder can indicate alternate functionalities provided to address the required feature.
52	62	Annexure XV, Technical Specification, Email DLP, Point 48	The Proposed Solution dashboard must display the number of cases in the designated period that fall above the risk score threshold that you've selected. Risk score thresholds must be customizable and instantly produce a report to prioritize the cases from high-to-low risk levels by leveraging analytics or machine learning technologies.	Kindly remove. OEM Specific	Bidder may propose alternate functionality which meets the requirement
53	63	Annexure XV, Technical Specification, Email DLP, Point 49	Workflow operations in DLP networking and mobile reports can now be applied to all filtered incidents or to selected incidents only. This includes operations such as: -Assigning incidents -Changing incident status -Changing incident severity -Ignoring incidents -Tagging incidents -Adding comments	Kindly remove. OEM Specific	**Please refer Corrigendum 1.11**
54	63	Annexure XV, Technical Specification, Email APT, Point 6	It should support execution of OS X files and Android applications.	Kindly remove "Android Applications" from clause	Please be guided by RFP
55	63	Annexure XV, Technical Specification,	It should support the execution of various OS or support hardware emulation	Kindly clarify the OS on which bank expect the support. We support windows and mac OS.	Please be guided by RFP

		Email APT, Point 7			
56	63	Annexure XV, Technical Specification, Email APT, Point 8	Solution to support below files for execution: Portable Document: PDF Document: DOC, DOCX, DOT, DOCM, DOTX, DOTM, HWP, ODT, PUB, RTF, WPD, XML, XPS and other file type. Spreadsheet: CSV, ODS, SYLK, XLT, XLS, XLM, XLTX, XLSM, XLTM, XLSB, XLA, XLAM, XLL, XLSX and other file type. PowerPoint: ODP, PPS, PPT, PPTX, PPTM, POTX, POTM, PPAM and other file type. Executable: BAT, COM, DLL, EXE, HTA, JS, MACH-O, MSI, PIF, PL, PS1, PY, SCR, SH, SYS, VB, WSF and other file type. Archive File: 7Z, ACE, APK, ARJ, BZIP, CAB, CHM, DMG, GZ, ISO, JAR, LHA, LZMA,, NUPKG, RAR, TAR, TARGZ, TNEF, WAR, XAR, XZ, ZIP, ZIPX and other file type. Media: ODG, SVG, SWF, TIFF and other file type Misc: CLASS, EML, HTML, IQY, PCAP, URL and other file type.	Kindly remove the following formats as they are not supported. HWP, ODT, WPD, XPS, ODS, SYLK, XLL, ODP, POTX, PIF, PL, PY, SH, LZMA, NUPKG, WAR, XAR, ZIPX, ODG, TIFF, PCAP	It is clarified, other file type is deleted. Incase bank desires any other file format, then the same is to be customized by the successful bidder without any additional cost to the Bank

Sr. No.	RFPPage No.	RFP Clause Name & No.	RFP Clause	Bidder's Query/Suggestion/Remarks	Bank's Response/clarification
1.	36	ELIGIBILITY CRITERIA OF THE BIDDER/OEM, Point no 5	Firm should be prime bidder and no consortium is allowed for the solution/ services to be offered	Please allow consortium bid, so that Indian (make in India) vendors can Participate	It is clarified, Bidder can opt for multiple OEM to arrive at Solution. However, each OEM should comply with eligibility Criteria defined in RFP. Additionally, there should be synergy among the products of different OEMs and should be compliant as per RFP
2.	36	ELIGIBILITY CRITERIA OF THE BIDDER/OEM, Point no 4	The OEM must have successfully implemented Email Security Solutions including Email gateway and Email DLP/ Email ATP in at least two PSU/ Government Organizations/ BFSI/ Private Sector in India, during last three years as on date of submission of Bid with a size of at least 35,000 email users in each	please remove email size for implementation so that Indian (make in india) vendors can Participate	**Please refer Corrigendum 1.1**

Sr. No.	RFPPage No.	RFP Clause Name & No.	RFP Clause	Bidder's Query/Suggestion/Remarks	Bank's Response/clarification
1.	9	Scope of Work	The scope of work includes Email Security Solution having following services for Punjab National Bank either On-Premises or on Cloud or both as applicable:	Clarification This clause is opposite to the entire technical specifications where the ask is to deliver the solution using a cloud. Is the Bank looking for a on prem solution or cloud or we can provide any option? Please clarify ?	Please be guided by RFP.
2.	10,55	1	The proposed email security solution should software/virtual based and can be hosted over any cloud.	The proposed email security solution should software/virtual based and can be hosted over any cloud OR should be hardware	Please be guided by RFP

				appliance/service built on purpose built email gateway appliance. Ask is for a end to end solution that meets the objective instead of the form factor. Same is mentioned at multiple points in RFP. "The scope of work includes Email Security Solution having following services for Punjab National Bank either On-Premises or on Cloud or both." "The Proposed solution should be able to consolidate reports from multiple boxes for centralized logging and reporting."	
3.	10,55	8	The Solution should have APIs/ Connectors / scripts for integration with various security solutions in the bank like ADDM, SMS, SOAR, SIEM, Firewall etc. as applicable and bidder shall enable the requested integration without any additional cost to Bank.	The Solution should have APIs/ Connectors / scripts / syslog for integration with various security solutions in the bank like ADDM, SMS, SOAR, SIEM, Firewall etc. as applicable and bidder shall enable the requested integration without any additional cost to Bank. Email Security Gateway shall deposit the logs in a syslog server , All other security solutions in the bank like ADDM , SMS , SOAR , SIEM , Firewall shall access data from syslog server to achieve integration	Please be guided by RFP.
4.	10,55	9	The bidder should follow the data localization guidelines of the Government and regulators as applicable from time to time. A confirmation should be provided in this regard.	Clarification The bidder should follow the data localization guidelines of the Government and regulators as applicable from time to time. A confirmation should be provided in this regard. All email security related pointers and IP's should be within Indian Geography , No Pointer or IP's related to MX / A Record / SPF / DKIM / DMARC / RDNS etc should be based outside Indian Geography.	Please be guided by RFP.
5.	10,55	11	The solution should be integrated with the case management solution and incident management solution of the bank.	Clarification Such integration are API based. Proposed solution API is a representational state transfer (REST) based set of operations that provide secure and authenticated access to the reports, report counters, tracking, quarantine, and configuration. You can retrieve the appliance reporting, tracking, and quarantine data using the API. We understand that this will meet the ask however also share the case management solution and incident management solution used by Bank.	It is clarified, solution should be integrated with the SIEM so that features of case management and incident management is available through the same for the incidents related to email security.

6.	10,55	12	The solution should provide analytical reports based on the emails processed by the system between two periods to enable fine tuning of policies.	Clarification From the ask we understand that solution should be able to provide interactive reporting to capture contextual data, analysis of which will help admins to do fine tuning of different parameters if required. Interactive email reporting provides filtering based on several types of criteria, including the following: IP address,Domain,Internal user, Destination domain, Internal sender domain, Internal sender IP address, Incoming TLS domain, Outgoing TLS domain,SHA-256 etc.	Please be guided by RFP
7.	11,56	22	The solution virus engine should support scanning by inbound, outbound and internal direction and configure the policy per direction	Clarification Inbound & Outbound Email will be scanned by the Cloud Email Security Gateway , For Internal Email to be scanned ,Microsoft O365 email platform should support functionality of routing internal email to Cloud Email Security gateway for scanning. Bank to confirm if internal email routing via cloud email security gateway is supported by O365	It is clarified, please be guided by Microsoft Office 365 email architecture. The solution virus engine should support scanning by inbound, outbound direction and configure the policy per direction. Bidder should provide suitable solution for scanning internal emails in addition to above, if it is not handled at the gateway. Further, Please be guided by Microsoft Office 365 email architecture
8.	10,11,56	15,25	Solution should protect against URL-based threats and should have lookalike domain detection capability	Clarification We understand that ask is for protection against highly targeted, socially engineered email attacks coming from lookalike domains. That can be delivered with DMARC verification which is a much powerful feature to fight against “Direct Domain Spoofing” and also includes “Display Name” & “Brand Impersonation” attacks. DMARC ties in information authenticated with SPF or DKIM (sending domain source, or signature) with what is presented to the end-recipient in the “From” header and ascertains that SPF and/or DKIM identifiers are aligned with the FROM header identifier. Also Forged Email Detection (FED) is another important line of defense against email spoofing also Dictionary of cousin domains or look-alike domains, based on your own domain by using DNSTWIST (https://github.com/elceef/dnstwist) to match against look-alike domain spoofing. Please confirm if the understanding is correct.	It is clarified, bidder to provide suitable functionalities as per RFP
9.	11,56	31	The solution should have at least 1500+ pre-defined content rules inbuilt with Email Security & embedded in the product	The solution should have at least 1500+ pre-defined content rules inbuilt with Email Security & embedded in the product OR should provide the capability to define custom content filter based on the BANK requirement All the incoming and outgoing mails pass through a set of policies if all 1500 content rules	It is clarified, the Bidder should provide the predefined / default content rules available in the system. The bank should have the facility to retain or delete specific rules. New rules/modified rules as required by the bank should be configured in the system before or during the implementation.

				will be inspected against each and every message then it will introduce a delivery delay and built up the queue for messaging. So request you to consider option to define the customer filter as per the requirement of bank instead of pre-built list of rules.	
10	11,57	35	The solution should be able to restrict incoming, outgoing and internal mails based on file types, file size and also by file name and also through a combination of them	Clarification Inbound & Outbound Email will be scanned by the Content filters set on Cloud Email Security Gateway , For Internal Email to be scanned ,Microsoft O365 email platform should support functionality of routing internal email to Cloud Email Security gateway for content scanning. Bank to confirm if internal email routing via cloud email security gateway is supported by O365	Please be guided by RFP
11	12,57	48	The solution must support internal sender authentication.	Clarification Does internal sender in this context mean , Application Server / Web Server / Printers etc which have identity in AD/LDAP , which need to be authernticated by Cloud Email Security Gateway to Send Email . If it dosenot mean Application Server / Web Server / Printers etc , Please explain	It is clarified, internal sender means from which email was originated.
12	12,57	45	The solution must have directory harvesting and DoS prevention capabilities.	The solution must have protection against directory harvesting attacks. DOS is more applicable to network traffic that can be protected by gateways firewalls or IPS and should not be the capability of the email gateway solutions.	Please be guided by RFP
13	12,58	57	The Solution must support quarantine administrator role. Thus only the delegated administrator is allowed to access the message in specific queue.	Clarification Administrator assigned with custom role to quarantine will get access to quarantine queue please confirm if the ask is same Proposed solution supports custom roles to allow delegated administrators to access the following All reports (optionally restricted by Reporting Group) Mail Policy reports (optionally restricted by Reporting Group) DLP reports (optionally restricted by Reporting Group) Message Tracking Quarantines Log Subscription	It is clarified, solution should support different roles as required for managing the email security besides specific roles for operational support.
14	12,58	60	The solution should allow where Administrator can specify which queues can be accessed by end user.	Request to remove this clause	**Please refer Corrigendum 1.3**

				The ask is contradicting with clause number 57 where only delegated administered is authorized for quarantine queue access and also giving quarantine queue access to user posses a high risk as if any user released his/her mail without checking the threat context may lead to a threat entry into the PNB network.	
15	12,58	61	The Personal management portal should be a web based UI for end users i.e. the console should be available to multiple users and multiple end points and there should be drill down features in the dashboard. They should be customizable based on needs	Clarification Personal Management portal can be customized to limited extent.	Please be guided by RFP
16	12,58	62	The Proposed solution should allow email reply to release the email quarantined by solution.	Request to remove this clause The ask is contradicting with clause number 57 where only delegated administered is authorized for quarantine queue access and also giving quarantine queue access to user posses a high risk as if any user released his/her mail without checking the threat context may lead to a threat entry into the PNB network.	Please be guided by RFP
17	13,59	78	The Proposed Solution should the configuration of workflow. End user's manager should be able to release the quarantined email via replying to the notification email from his inbox	Request to remove this clause The ask is contradicting with clause number 57 where only delegated administered is authorized for quarantine queue access and also giving quarantine queue access to user posses a high risk as if any user released his/her mail without checking the threat context may lead to a threat entry into the PNB network.	Please be guided by RFP
18	13,59	79	The notification message to end users should be completely customizable.	Clarification Notification message customization capabilities is limited	Please be guided by RFP
19	13,59	80	The Proposed solution should allow end users to create their own personal allow and block lists. The solution should allow administrators to define which queues can be accessed by end user	Clarification Query : Does Queue in this context refer to quarantine queue ? & Is the ask contradicting with clause number 57 where delegated administrator is authorized for quarantine queue access.	This is functionality desired. Bidder to provide suitable solution as per RFP.
20	16,63	2	The Solution should have multiple AV/APT engines for anti-virus and malware scanning. Solution should provide on cloud AV/APT service from day1	The Solution should have multiple AV/APT engines for anti-virus and malware scanning. Solution should provide on cloud AV/APT service from day1 or should be hardware appliance/service built on purpose built appliance. "Ask is for a end to end solution that meets the objective instead of the form factor. Same is mentioned at multiple points in RFP.	Please be guided by RFP

				"The scope of work includes Email Security Solution having following services for Punjab National Bank either On-Premises or on Cloud or both." "The Proposed solution should be able to consolidate reports from multiple boxes for centralized logging and reporting."	
21	16,63	6	It should support execution of OS X files and Android applications.	Request to remove this clause The ask is contradicting with clause number 5 where ask is "Sandbox Service should have Kernel visibility with minimal OS version dependencies" Bank supported this ask in "RFP for procurement of Network Anti- Advanced Persistent Threat (N/w-Anti-APT) and Deception/Decoy Solutions." published in 2019 for maximum participation and the point was read as "Solution should be deployed on premise and along with on premise sandboxing capability where the objectionable content may be executed and inspected, of the Windows Operating Systems (32 and 64 bit) This requirement should be based on virtual execution and should not be Hardware or chip based function" after corrigendum 1.	It should support execution of OS Xfiles and android applications if such functionalities of mobile platform support are included in email security solution provided.
22	16,63	8	Solution to support below files for execution: Portable Document: PDF Document: DOC, DOCX, DOT, DOCM, DOTX, DOTM, HWP, ODT, PUB, RTF, WPD, XML, XPS and other file type. Spreadsheet: CSV, ODS, SYLK, XLT, XLS, XLM, XLTX, XLSM, XLTM, XLSB, XLA, XLAM, XLL, XLSX and other file type. PowerPoint: ODP, PPS, PPT, PPTX, PPTM, POTX, POTM, PPAM and other file type. Executable: BAT, COM, DLL, EXE, HTA, JS, MACH-O, MSI, PIF, PL, PS1, PY, SCR, SH, SYS, VB, WSF and other file type. Archive File: 7Z, ACE, APK, ARJ, BZIP, CAB, CHM, DMG, GZ, ISO, JAR, LHA, LZMA,, NUPKG, RAR, TAR, TARGZ, TNEF, WAR, XAR, XZ, ZIP, ZIPX and other file type. Media: ODG, SVG, SWF, TIFF and other file type. Misc: CLASS, EML, HTML, IQY, PCAP, URL and other file type.	Solution to support below files for execution: Portable Document: PDF Document: DOC, DOCX, DOT, DOCM, DOTX, DOTM, HWP, ODT, PUB, RTF, XML, XPS and other file type. Spreadsheet: CSV, ODS, XLT, XLS, XLM, XLTX, XLSM, XLTM, XLSB, XLA, XLAM, XLL, XLSX and other file type. Executable: BAT, COM, DLL, EXE, HTA, JS, MSI, PIF, PS1, SCR, SYS, VB, WSF and other file type. Archive File: CAB, CHM, ISO, JAR and other file type. Media: SWF and other file type. Misc: EML, HTML, IQY, URL and other file type. PNB needs protection against the dynamic threats which is a never-ending battle against malware. So this should not be only limited to certain extension but should be based on the dynamic context information against which each new sample is analyzed. Malware changes over time; we have records of those changes. You can perform thorough retrospective remediation following a security breach. You can	It is clarified, other file type is deleted. Incase bank desires any other file format, then the same is to be customized by the successful bidder without any additional cost to the Bank

				prepare more effective defences against the next generation of malware attacks. The list of extensions may not be tally with all the OEM's and restrict the participation.	
23	16,64	13	The solution should have option to store email or file in queue in case the similar file with same hash value receive in the given timespan then the action should be followed.	Request to remove this clause This will not improve any threat efficacy objective should be to automate the removal of emails with files that become malicious after the initial point of inspection. Retrospective events	Please be guided by RFP
24	16,64	16	The bidder should also implement a CASB solution to enable role based access to identify application including email by enforcing amalgamated policies for access through aloud from anywhere.	Request to remove this clause Cloud-native cloud access security broker (CASB) that helps customers move to the cloud safely. It protects your cloud users, data, and apps. uses open, and automated approach uses APIs to manage the risks in your cloud app ecosystem. Proposed solution complies to FedRAMP,SSAE16 – SOC 2 Type 2 Certified,SOC 3 Certified – Trust Services Report for Service Organizations,TRUSTe,Cloud Security Alliance Security, Trust & Assurance Registry (STAR) However CASB shares the metadata in cloud which may not be localized in geographical boundaries. This is independent solution for protection of cloud based SAAS applications and not part of Email Security.	Please be guided by RFP
25	36	Eligibility Criteria of the Bidder	Firm should be prime bidder and no consortium is allowed for the solution/ services to be offered	Bidder should provide the solution fully compliant as asked by the Bank. Bidder may choose single OEM or multiple OEM to arrive at the solution. This is restricting the bid to a single OEM and is also not allowing the Bank to get the best of the solution. We request the bank to allow multiple OEMs to provide a solution for Bank's requirement.	It is clarified, Bidder can opt for multiple OEM to arrive at Solution. However, each OEM should comply with eligibility Criteria defined in RFP. Additionally, these should be synergy among the products of different OEMs and should be compliant as per RFP
26	36	Eligibility Criteria of the Bidder	The bidder should have Support centres in India.	The Bidder and OEM should have support centres in India. We feel that the OEM must also have support centres in India and must be asked by the Bank. Otherwise in normal business	**Please refer Corrigendum 1.13**
27	37	Eligibility Criteria of the Bidder	The Bidder should have support centers in Delhi NCR and Mumbai	The Bidder and OEM should have support centres in India. As the requested email security services is to be delviered from the Cloud & also 2 On-site support resources will be present to manage the	Please be guided by RFP

				solution , The 24x 7 backend support centre can be either in Delhi NCR or Mumbai	
28	46	MAF	In case of default/unable to comply with above at the time of delivery or during implementation or customization, for the software already billed, we agree to take back the supplied items without demur, if already supplied and replace it with an Original &Latest product/component. We also take full responsibility of the Solution& Service SLA as per the content even if there is any defect by our authorized Service Centre / Reseller / SI etc.	Kindly remove.	Please be guided by RFP