

Response to Pre-bid Queries
RFP : IFT/DLP/120923

Sr No	Clause No	Page No	Clause	Query	IFTAS Response
1	21	38	The solution should be able to define the workflow based on organization requirement. It can further integrate with AD server and workflow can be configured and release any quarantine email.	Please help us with more clarifications related to workflow requirement	Workflow to approve/reject the quarantine mail by approving authority within respective department.
2	25	38	The solution should be capable to provide templates and workflows for compliance with security and privacy standards such as ISO 27001, PCI DSS V4.0.	Request IFTAS team to amend this clause as: The solution should be capable to provide templates and workflows for compliance with security and privacy standards such as ISO 27001 or PCI DSS V4.0	As per RFP, requirement is for both ISO 27001 and PCI DSS V4.0 compliance.
3	36	39	The solution should integrate with advance SIEM and SOAR technologies.	Request IFTAS team to amend this clause as: The solution should integrate with advance SIEM or SOAR technologies.	As per RFP, requirement is for both SIEM and SOAR
4	40	39	The DLP Solution must have capability to integrate with 3rd party Proxy solution for content inspection using ICAP channel or must have DLP engine on OEM provided Proxy itself. But bidder needs to make sure the seamless and centralized deployment for DLP and URL filtering	DLP integrates with 3rd party proxy solution. Need clarification on DLP engine on OEM provided proxy itself, does IFTAS asking Web proxy solutions along with DLP, please help us to clarify this point.	DLP to be integrated with the existing IFTAS Proxy solution.

5	1	41	The solution should have the capability to revoke access to the documents/files to users at any time even after delivery	This feature is not part of DLP technology; however, these features can be available (DRM) Data rights Management solutions, request IFTAS team to remove this clause from specifications	As per RFP, These all are Good to have feature will be add value to the overall solution and are not a mandatory features.
6	2	41	The solution should be capable to defend against internal or external threats.	This feature is referring to endpoint AV/EDR, DLP can protect sensitive data, defending against internal or external threats can be manage by endpoint security solutions, please guide us whether bidder should provide solutions for endpoint security or not	
7	3	41	Solution should be capable to Restricting applications allowed to use sensitive content — e.g., only allowing encryption with an approved enterprise solution, not tools downloaded online that don't allow enterprise data recovery.	This feature is not available in DLP solution, IFTAS team can have (DRM) solutions along with encryption technology to get this feature, request IFTAS team to remove this clause from specifications.	
8	4	41	The solution should support automatic deletion /Disabling of internal and external users based on changes in identity Sources.	This is not a DLP feature, request IFTAS team to remove this clause from RFP.	
9	5	41	The solution should support highly granular rights: viewing, editing, printing, copying, forwarding, screen capture prevention (even when file opens in native application), timebased expiry, and restrict access based on client type.	Not a DLP feature, request IFTAS team to remove this clause, this feature can be available in DRM solutions.	

10	7	41	The solution should have the capability to allow document creators to assign different rights for each user or group in the same window.	Not a DLP feature, request IFTAS team to remove this clause, this feature can be available in DRM solutions.
11	8	41	The solution should have the capability to provide off-line use of protected documents; can also control the period for which the user can have offline use.	DLP can provide DLP protection for off-line users, but controlling time/period would not be possible, IFTAS team should look DRM solutions to achieve time control features for documents, request IFTAS team to amend this clause as: The solution should have the capability to provide protection for off-line use of documents.
12	9	41	The solution should be such that there is no single point for unprotecting the documents other than document owner.	Not a DLP feature, request IFTAS team to remove this clause, this feature can be available in DRM solutions.
13	10	41	The rights and policies on the document must apply irrespective of how the document is shared. i.e., copied to USB, FTP, shared via G-drive, Dropbox etc. and should be independent of the collaboration platforms.	Documents can be protected while sharing/copying to USB, FTP or G-drive, Dropbox etc. Document rights management can be achieved via (DRM) solutions, request IFTAS team to remove or amend this clause as: Proposed DLP solution should have policies where the sensitive document must protect irrespective of how the document is shared. i.e., copied to USB, FTP, shared via G-drive, Dropbox etc. Protecting data for collaborations platform, you may need separate solutions like (CASB), please help us

				to understand your use cases related to collaboration platform.
14	11	42	The assigned rights should be dynamic; one can grant and withdraw the rights for a specific user or group for the protected document at any time without the need to recall or resend the document.	Not a DLP features, request IFTAS team to remove this clause, this feature can be achieved on DRM solutions.
15	12	42	The system administrator should be able to define and control which users are allowed to define policies and can monitor these policies for compliance as per IFTAS' security policy. The Admin or Owner of the document should also be able to transfer document ownership.	As far as concerns controlling and monitoring of DLP policies can be support by DLP with role based admin feature. Document transfer and ownership feature not part of DLP, this feature relevant to (DRM) solutions, request IFTAS team to amend this clause as: The system administrator should be able to define and control which users are allowed to define policies and can monitor these policies for compliance as per IFTAS' security policy.
16	15	42	The solution should provide search and- browse capabilities for documents, activities, and rights templates for end users and administrators.	Not a DLP feature, request IFTAS team to remove this clause, you can get this feature on (DRM) solutions
17	16	42	The solution should have the capability to keep encryption keys secure and content always separate.	Not a DLP features, request IFTAS team to remove this clause from RFP

18	17	42	The solution should be capable to provide two- factor authentication.	Request IFTAS Team to amend this clause as: The solution should be capable to integrate with authentication server like – AD, LDAP, etc.)
19	18	42	Documents / emails should be encrypted using AES 256- bit encryption or higher algorithm.	Not a DLP feature, IFTAS should have remove this clause or guide us whether bidder should encryption solutions or not.
20	19	42	The bidder shall provide the encryption technics used in the solution.	Not a DLP feature, please guide us, whether bidder should propose encryption solutions or not
21	20	42	The solution should be able to identify Data Lossed in the form unknown and known encrypted format like password protected word document. The solution should be able to identify malicious traffic pattern generated by Malware infected PC in order to prevent future Data Loss age by the malware.	This feature is not part of DLP technology, you need to have encryption technology along with endpoint security (NGAV) solutions, request IFATS team to guide whether bidder should propose encryption and NGAV solutions or not.
22	21	42	The solution should support the multiple Endpoint Profile Creation for the Better Security between the different departments. Encryption Keys are also should be isolated between the different departments. The endpoint installed should have the capability to create the Bypass ID after validation by the administrator by generating the Passcode.	Not a DLP features, IFTAS need to have encryption, request IFATS team to guide whether bidder should propose encryption solution or not
23	22	42	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	Partial data leakage feature is referring to a particular DLP vendor, request IFTAS team to amend this clause as: The solution should be

				able to do full binary fingerprint of files and also should be able to detect even if information gets leaks from fingerprinted files or folders	
24	23	42	The solution should support the templates for detecting the Deep Web Urls- .i2P and .Onion , Encrypted attachments to competitors , Password Dissemination , User Traffic over time , Unknown Encrypted File Formats Detection. The solution should support detection of PKCS #12 files (.p12, .pfx) that are commonly used to bundle a private key with its X.509 certificate	Password / encrypted files or data cannot be read by DLP solutions, request IFATS team to remove this clause from RFP.	
25	24	43	The DLP 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.	Machine learning feature is leading to a particular DLP vendor, request IFTAS team to amend this clause as: The DLP 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.	
26			General	Number of Endpoint Users	100
27				Timeline to complete the project.	As per RFP project timeline.
28				What are the channels to be covered (Anything apart from Endpoints and Network as mentioned in the RFP)	As per RFP .Endpoint, Web and email channels

29			Is Data classification solution in use? (If yes, please mention the tool	Yes, Klassify tool
30			Is IRM/RMS Solution in use? (If yes, please mention the tool	No
31			Do you have Data classification framework already in place	Yes
32			What is the data that needs to be protected using DLP (Student PII data, Specific Ips, Any customized data formats, particular file formats etc;)	All the relevant data.
33			Type of directory server used and version	Windows Active Directory Server.
34			What minimum features are required. (Whether sensitive data is just to be blocked, blocked and reported, allowed and reported etc;)	As per RFP, All these use cases required and to be configured as per IFTAS policy.
35			Any specific reports are required? (Number of DLP incidents, number of false positives etc;)	The compliance and other relevant reports required.
36			Any cloud based applications like O365, Gsuite or any other application for which you are looking for visibility and control.	We are using O365.
37			Any known compliances that need to be considered for DLP protection?	PCI DSS V4.0 and ISO 27001.
38			Will DLP need to also get integrated into the SIEM/SOC	Yes
39			Do you need High Availability and Disaster recovery setup as well?	Yes
40			Do you need to have OCR(Optical character	As per RFP

				recognition) feature as well.	
41				Which proxy , av/edr, encryption solutions on systems currently	Will be shared with successful bidder.
42				Do you use sccm or equivalent tool to deploy agents ?	Yes
43				Do you have any preferred DLP vendor	No
44				If Data classification and DLP both are needed, is it acceptable to have different vendors for each of the solution	Only DLP needed. Data classification is already in place.
45				Do you need only implementation in DC or do you also need DR setup?	DC- DR setup as per RFP
46				Will there be any user count increase forecast for immediate future.	Yes , expected upto 500.
47		5	The Solution should have High Availability implemented between DC and DR Site.	Please confirm IFTAS needs HA in both DC & DR location or HA between DC and DR only	HA between DC and DR
48	Annexure III	44	Clarification	As per RFP one onsite resource will be hired for support. Please confirm the location for the onsite resource.	Hyderabad
49	Project Milestone	11	Software/hardware and license delivery	Request IFTAS to extend delivery timeline for 2-3 weeks to 5 to 6 weeks	As per RFP, further discussed and finalized with successful bidder
50	AMC Support	17	The successful bidder shall provide 24 X 7 support during the warranty period, ensuring the accepted level of performance as specified in "Service Level Agreement".	As per RFP one onsite resource will be hired for support.	As per RFP, It is envisaged that the onsite resource is for limited period of one year and decided there after. however AMC will be for the contract period .