

PROJECT: SECURE DATA MANAGEMENT SOLUTION**QUERIES/CLARIFICATIONS RAISED DURING THE PRE-BID CONFERENCE:**

	Query/Clarifications	TWG/BAC Reply
1.1	With reference to item number 7 of the Technical Specifications, which states that the bidder shall work with the Supplier and/or Representative to integrate the proposed solution with the Network Data Loss Prevention (DLP) system and other related services as required, may we confirm which network DLP solution is currently in place and which of the proposed solutions, DLP or FRP are required to integrate with it?	There is no Network DLP solution currently in place. The proposed DLP Solution should support integration with various systems (e.g. (Drive Encryption, File and Removable Media Protection, AD etc..).
1.2	May we confirm whether the HA setup will be configured at a different site?	It will be configured at the Main Office only.
1.3	Regarding the eligibility components for on-going contracts, do we need to attach supporting documents such as Notices of Award, etc.?	Per BAC, there is no need to attach supporting documents of the on-going contracts
1.4	Regarding the Bid Data Sheet on page 42, we would like to seek clarification on the Bid Security. Are we required to submit both the authorized bid securing declaration and the bid security? We would just like to confirm because the statement uses the word 'and.'	You only need to submit one; please choose between the two. We already raised this concern with the GPPB, and according to them, you may use only one option for your Bid Security. You may submit either cash equivalent to 2% of the ABC, a Bid Security using a Surety Bond equivalent to 5% of the ABC, or a Bid Securing Declaration.
1.5	We would also like to confirm the Project Identification Number for this project. For the Secure Data Management Solution, it is 2026-032.	Yes.

WRITTEN QUERIES:

	Query/Clarifications	TWG/BAC Reply
2.1	<p>Technical Specifications 6.4 Other Requirements Page 81</p> <p>The Bidder shall work with the Supplier and/or the Representative to integrate the proposed solution with the Network Data Loss Prevention (DLP) system and other related services as required.</p> <p>What is the existing Network DLP in-placed? Which of the target solutions (DLP, Drive Encryption, File and Removable Media Protection) are required to be integrated with the Network DLP?</p>	Refer to 1.1
2.2	<p>SECTION VII - TECHNICAL SPECIFICATIONS</p> <p>II. DATA LOSS PREVENTION (DLP) REQUIREMENT</p> <p>2.4 The solution must provide comprehensive protection for all possible leaking channels, including:</p> <ul style="list-style-type: none"> a) Application File Access Protection b) Clipboard Protection c) Protection on cloud storage such as Box, Dropbox, Google Drive, iCloud, OneDrive, Office365, and Syncplicity d) Email Protection e) Mobile Protection f) Network Communication Protection g) Network Share Protection h) Printer Protection i) Removable Storage Protection j) Screen Capture Protection k) Web Protection 	

	<p>Is mobile protection needed?</p> <p>What data can users' access, and which applications are used for sharing information?</p>	<p>Yes. For SSS issued mobile.</p> <p>Users' access to data will depends on the allowed policy and access privilege. Sharing of information will also depends on the data classifications per applications or systems.</p>
2.3	<p>SECTION VII - TECHNICAL SPECIFICATIONS</p> <p>II. DATA LOSS PREVENTION (DLP) REQUIREMENT</p> <p>2.6 The solution must be able to allow organizations to scan files, Offline Storage Table (OST) and Personal Storage Table (PST) stored in endpoints.</p> <p>Is PST sufficient to meet this requirement?</p>	<p>No, we maintain the requirement</p>
2.4	<p>SECTION VII - TECHNICAL SPECIFICATIONS</p> <p>II. DATA LOSS PREVENTION (DLP) REQUIREMENT</p> <p>2.16 The solution must provide protection for USB drives, smartphones, Bluetooth devices, and other removable media.</p> <p>" The solution must provide protection for USB drives, smartphones, Bluetooth devices, and other removable media. "</p> <p>Is a smartphone destination required? What percentage of users are smartphone users?</p>	<p>Yes, we will provide to the winning bidder</p>
2.5	<p>SECTION VII - TECHNICAL SPECIFICATIONS</p> <p>IV NATIVE DRIVE ENCRYPTION REQUIREMENT</p> <p>4.1 Optionally, the solution must provide centralization and simplification of both Microsoft</p>	

<p>BitLocker and Apple FileVault's management, providing a unified platform for managing encryption on devices.</p> <p>4.2 The solution must protect data on devices that are lost or stolen by ensuring that encryption is in place to prevent unauthorized access to sensitive information.</p> <p>4.3 The solution must be able to deploy through a single console available on-premises that suits the organization's needs.</p> <p>4.4 The solution must be able to turn on PIN features to enhance security, adding an additional layer of protection to encrypted devices by requiring a personal identification number (PIN) for access.</p> <p>4.5 The solution must collect, manage, and rotate encryption keys to facilitate activities such as enterprise recovery, ensuring that encryption keys are securely stored and regularly updated to maintain data security.</p> <p>4.6 The solution must generate reports on devices by operating system and provides visibility across the environment, allowing administrators to track the status of encryption deployment and monitor compliance with organizational policies.</p> <p>Items 4.1 to 4.6. The current specification requires a single on-premises console from the security vendor to centralize the management of Microsoft BitLocker and Apple FileVault. Considering that modern government agencies standardizing on Zero Trust architectures typically utilize their existing Unified Endpoint Management (UEM) investments (such as Microsoft Intune or Microsoft Endpoint Configuration</p>	<p>We maintain the requirement. The solution must provide centralized management of Microsoft BitLocker and Apple FileVault without the dependency of integrating to Unified Endpoint Management (UEM)</p>
---	--

	<p>Manager) to manage native OS encryption natively without third-party vendor lock-in, will the agency consider accepting a solution that enforces industry-leading Data Loss Prevention (DLP) while integrating with or leveraging the agency's existing Microsoft management infrastructure for BitLocker key rotation and recovery?</p>	
2.6	<p>SECTION VII - TECHNICAL SPECIFICATIONS</p> <p><u>V.FILE AND REMOVABLE MEDIA REQUIREMENT</u></p> <p>5.1 The solution must enforce policy-based encryption and require authentication for access to files and removable media device contents, both inside and outside the organization's network.</p> <p>5.2 The solution must be compatible with Windows and macOS devices, offering a variety of authentication methods.</p> <p>5.3 The solution must protect against the unauthorized removal of sensitive data from corporate devices.</p> <p>5.4 The solution must ensure that users are authorized to access encrypted files, folders, network shares, and data on removable media devices.</p> <p>5.5 The solution must be able to integrate with Active Directory to manage the assignment of encryption keys.</p> <p>The specification calls for policy-based encryption for files and removable media device contents.</p> <p>Would the agency accept a modern, streamlined approach where an advanced Data Loss Prevention (DLP) agent restricts data movement by ensuring sensitive files can only be transferred to authorized, pre-encrypted</p>	<p>No, we will not consider modern streamlines approach. We maintain the requirement.</p>

	removable media (utilizing native OS tools like BitLocker to Go), as a fully compliant alternative to procuring a proprietary, third-party USB encryption software module?	
2.7	<p>SECTION VII - TECHNICAL SPECIFICATIONS</p> <p><u>V.FILE AND REMOVABLE MEDIA REQUIREMENT</u></p> <p>5.6 The solution must support portable encryption of email attachments using a self-extractor.</p> <p>The specification requires portable encryption of email attachments using a 'self-extractor'. However, based on modern cybersecurity threat intelligence, self-extracting executable archives (SFX / .exe files) are increasingly categorized as a severe security risk and are routinely blocked or quarantined by modern Secure Email Gateways (SEGs) because threat actors exploit them for stealthy malware delivery and DLL sideloading. To ensure the secure, unhindered delivery of SSS communications without exposing the agency or its partners to executable payloads.</p> <p>Will the agency accept modern secure sharing alternatives such as robust DLP email blocking, standard password-protected AES archives, or secure cloud-based data delivery links?</p>	<p>No. We maintain the requirement. The solution must fully address the requirement by providing portable, self-extracting encryption for sensitive email attachments, with no dependency on Secure Email Gateways (SEGs).</p>
2.8	<p>SECTION VII - TECHNICAL SPECIFICATIONS</p> <p>V.FILE AND REMOVABLE MEDIA REQUIREMENT</p> <p>Is this for a Persistent file/folder encryption everywhere?</p> <p>Or for a removable media only is</p>	<p>Yes</p> <p>No, it is not limited to removable media</p>

	acceptable?	only
2.9	May we request to relax the required year range for completed contracts from 5 years to 8 years so that we can be more eligible and have a greater chance of participating in the bidding.	This will be considered. This amends Item 5.4 of Bid Data Sheet From Bidders should have completed, within a period of five (5) years from the date of submission and receipt of bids, To Bidders should have completed, within a period of eight (8) years from the date of submission and receipt of bids,
2.10	For the SLCC, it is stated under Note No. 3 of the SLCC Form that a Certificate of Final Completion or any proof of completion should include a statement of the bidder's satisfactory performance. For this requirement, would it be acceptable for our document reference to be an Official Receipt as proof of completion? We believe that a certificate of satisfactory performance is not required, as the contract involved only the supply and delivery of licenses, with no services or ongoing performance component.	We maintain the requirement. Bidder must submit the Certificate of Completion or any proof of completion including a statement of the bidders' satisfactory performance.
2.11	Under Technical Specifications item 6.4, our proposed solution can be integrated into different Network Data Loss Prevention (DLP). May we know your current network DLP solution in place?	Refer to 1.1