323 State Street
Augusta, ME 04330

Competitive Bid
Request for Proposal
This is NOT an order.

Sensitive Data Discovery / DLP Solution
Addendum #1

Addendum Issue Date:	**June 14, 2021**
Response Due Date:	**June 18, 2021, 1pm EST**
Return Proposal To:	**Scott Fortin** **Chief Information Security Officer** **Maine Community College System** **323 State Street** **Augusta, ME 04330** **207.629.4004** **sfortin@mccs.me.edu**

Endpoint / Server Data

The abridged inventory included with the original RFP to help provide context on the types of systems that will be scanned using a Sensitive Data Discovery / DLP tool has been expanded to include data from 6/8 institutions:

Device Type	OS	Version	Quantity
Endpoint	*Windows*	*10*	*2000*
Endpoint	*Mac OS*	*10.15 & 11*	*100*
Server	*Windows*	*2019*	*500*
Server	*Linux*	*CentOS 8*	*10*

Bidder Questions/Answers

Six question sets were received from potential respondents. Company-specific information has been removed from the questions. Answers compiled from the RFP committee are below:

Question set #1, received 6/7/21 - 5:53pm

Do you need *software companies* to respond directly? We are working with a few partners to respond to the RFP and I can provide a reply but would rather not compete with our partners. Is it ok to simply work with the partners on the RFP response?

MCCS Answer: Your preference. We'll accept proposals (plural) from all qualified companies. In fact, we're obligated to per state and institution procurement policy. Early on in the RFP design process, we engaged a few software companies that align well with the project needs. The purpose of this pre-RFP communication was to alert software companies of the upcoming RFP and ensure if no partner included the solution as part of their proposal, the software company could respond directly, using internal professional service resources to implement.

If your solution provides file fingerprinting, please describe how the solution utilizes this feature. Is this for the purposes of validating the version and integrity of the file? Would you please elaborate on how you will use this functionality?

MCCS Answer: DLP systems typically employ file fingerprinting techniques to classify data and track user interaction, file movement, and other types of changes. If this feature is utilized by the proposed solution, the exact mechanics need to be understood by all IT staff for purposes of integration with other college IT software and systems. For example, a fingerprint on a file could be used by anti-malware software (Sophos InterceptX in most cases) to allow or deny transfer across the network. Colleges that use next-gen firewalls (Fortinet, Sophos) which include DLP features may be configured to interact with file fingerprints or metadata.

Though not typically called file fingerprinting, there is interest for incorporating Windows/MacOS/Linux file tagging so employees or users can recognize sensitive data files and treat them appropriately. If your solution is capable of providing this functionality, please include specifics in the Special Considerations section of the proposal.

Are there enterprise features that align with a federated organizational structure? I.e. does MCCS currently use a Federated AD Architecture or Independent Forests?

MCCS Answer: The MCCS operates separate AD forests, one per college/institution. One college further divides employee/student accounts into two domains within one forest.

Question set #2, received 6/10/21 - 8:59am

Are scheduled or manually triggered scans a requirement? or can scans occur once upon installation and then as needed in real time as data is written to disk?

MCCS Answer: The MCCS strives to discover all sensitive data stored on college-owned equipment. The functionality articulated in this question is acceptable, given it can detect sensitive data at rest on initial scan AND as new files are created, copied, etc. The solution must also incorporate the ability to add custom sensitive data queries / parameters and search MCCS-owned systems soon after the new configuration is applied. The RFP committee is unsure if the functionality articulated in this question would match stale data at rest associated with a new policy, given the nature of scanning once upon installation and real time on data writes.

Is there a requirement to scan external storage media if connected to a particular system?

MCCS Answer: Yes, the solution should support scanning external storage media connected to systems.

What are the intended remediation actions? Deletion? Preventing the transport of sensitive data?

MCCS Answer: Reporting is essential, remediation will depend on the capabilities of the system. Remediation options to delete, move, copy, quarantine, lock for editing, and alert the end user are desirable actions that could be implemented by colleges, depending on their comfort level with the SDD/DLP solution.

Revoking access to particular files or folders?

MCCS Answer: See above, this is another desirable remediation action if the solution supports it.

Is there a requirement to create custom DLP signatures for types of data that our non-standard in the industry (strings, numbers, etc that are specific to MCCS)?

MCCS Answer: Yes, the solution should support custom DLP signatures and policy.

Is there a requirement to have the management of said solution on-prem? Is cloud acceptable?

MCCS Answer: On-prem, hybrid, and cloud deployment methods are all acceptable, provided consideration is given to how the solution scans on-premise systems, off-premise VPN-connected systems, or systems not connected to the campus LAN (work from home, etc).

What is considered a sensitive data incident? Leakage of sensitive data? Finding sensitive data on a particular machine?

MCCS Answer: Both are considered sensitive data incidents. Colleges will utilize EDR & NGFW technologies to prevent data leakage for data in motion. The primary purpose of this RFP is to detect sensitive data rest and alert for remediation.

Is there a preferred term-length for subscription/support contracts?

MCCS Answer: A 3-year term is preferred for license / support contracts.

Question set #3, received 6/10/21 - 9:25am

One item from my legal team is we need an NDA in place before we can provide answers to the Security Addendum. Please find it attached. Will you be able to get that signed in time on your side before the RFP is due?

MCCS Answer: We cannot agree to use the laws of another state. Our recommendation is to submit a solution proposal without confidential and proprietary technical documents. If clarification is needed on one or more security items, we will request additional information and address NDA measures at that time. However, as we are a public entity, and this is a public bid, parts of your proposal could be subject to FOIA/FOAA requests by other vendors or entities. If this happens, we typically ask vendors to revise their proposals and redact any trade secrets, intellectual property, and certain pricing.

Question set #4, received 6/10/21 - 11:30am

Regarding: Are there enterprise features that align with a federated organization structure? - Is this a federated AD structure or independent forest?

MCCS Answer: The MCCS operates separate AD forests, one per college/institution. One college further divides employee/student accounts into two domains within one forest.

Regarding: Is the agent self-healing and updating after initial install? Please provide detail. - Can you provide clarification on what the reference to “self-healing” is and what is expected?

MCCS Answer: If the SDD/DLP agent or component of the agent crashes, the agent should reinitialize on reboot or alert IT staff to further evaluate the problem. The agent should also upgrade its code version or update its configuration through cloud or on-premise servers when

IT staff make a policy change or request clients upgrade their code versions to patch security vulnerabilities and/or take advantage of new features.

Regarding: Does your solution support integration with multiple identity providers? - Are we looking for access control to the console or platform access i.e. O365, ServiceNow, etc.?

MCCS Answer: We are seeking federated identity / single sign-on from college identity providers (AD / Azure AD) to the SDD/DLP solution. See above questions/answers regarding current AD infrastructure.

Question set #5, received 6/10/21 - 11:35am

Please indicate which institutions in the Maine Community College System have created data inventory and data classification documentation (policies, procedures, databases, or similar).

MCCS Answer: The MCCS Board of Trustees adopted policy #903 which describes Information Classification and associated data definitions (restricted, internal, public). The MCCS and a few member institutions have started data management / data governance initiatives. A comprehensive data inventory is a desired output of this project with the help of a sensitive data discovery tool.

Are security consulting services desired as part of this RFP for value added services? (e.g. *software vendor* installation/configuration, rollout to workstations, interpretation of discovered data, guidance regarding PII remediation)

MCCS Answer: Due to varying levels of IT/IS staffing across the MCCS and the inherit complexity of SDD/DLP systems, support / implementation services to assist IT/IS staff with solution deployment and operation is needed. Pool hours that allow colleges to implement the solution on their own timeline and with varying levels of assistance from the software company or partner have worked well in the past.

Are explicit document metadata employed by any MCCS organization, such as Azure Information Protection (AIP) or MIT tags?

MCCS Answer: Currently, Azure Information Protection & MIT tags are not used by any MCCS institution. There is interest among IT/IS staff to incorporate Windows/MacOS/Linux file tagging so employees or users can recognize sensitive data files and treat them appropriately. If your solution is capable of providing this functionality, please include specifics in the Special Considerations section of the proposal.

Question set #6, received 6/10/21 - 11:40am

Are MAC OS endpoint storage volumes accessible via common protocol ? [NFS or SMB]

MCCS Answer: The MCCS prefers a native MacOS agent to sharing an entire MacOS storage volume via NFS or SMB to allow scanning by a SDD/DLP solution.

Are Linux endpoint storage volumes accessible via a common protocol? [NFS or SMB]

MCCS Answer: The MCCS prefers a native Linux agent to sharing an entire Linux storage volume via NFS or SMB to allow scanning by a SDD/DLP solution.

Which ticketing systems are employed?

MCCS Answer: MCCS institutions currently utilize ManageEngine Service Desk, Solarwinds Web HelpDesk, TeamDynamix, SpiceWorks, and LibAnswers for IT service management. Email reporting is an acceptable 'common approach' to alerting but integration with the aforementioned ITSM tools is desirable.

Regarding 5.2 Company Structure – in reference to 'chart of the organization', what is the requirement? Is the request for Corporate Ownership structure (partner companies/affiliates)?

MCCS Answer: In order to ensure the MCCS partners with financially sound companies (given the sensitive nature of this solution and the data being scanned) the MCCS is requesting a copy of the paperwork that shows incorporation- whether that be as an LLC, corporation, partnership, sole proprietorship, etc. Secondarily, an organizational chart that shows the respondent and relationships to parent or child companies should be included to allow the RFP committee to gauge the ability of the company to deliver on the proposal.

Regarding 6.2 Security – first cell of the matrix notes, "Cloud Services Solution" – is this section a requirement if there are no cloud services included in our proposal?

MCCS Answer: If no cloud services are included in a proposal, section 6.2 and associated appendices should be answered with regard to the on-premise solution that will operate on MCCS networks, servers, and endpoints.