RFP 3178 DIGITAL RESOURCE INVENTORY
Addendum #1

Answer to Vendor Questions
April 7, 2025

Q 1.   What is the number and types of endpoints to be managed (e.g., desktops, laptops, mobile devices)?

A 1.   This RFP does not require management of endpoint devices. As RFP Section II A states:

> The Division seeks to purchase the capacity and capability to implement a digital resource inventory. This system shall provide real-time analytics on application usage and engagement to help the Division measure its return on application investments and provide rostering, account provisioning, and security tools. This system shall be able to offer an internal-facing and public-facing inventory of digital resources that can be categorized by approval status. The solution must interface with Google Chromebooks, Windows devices, Apple devices, Microsoft Azure, and Synergy Student Information System. The system must interface with our Internet Filter and Classroom management system and/or have the ability to control access to apps based on what was approved. Third party risk assessments for inventory system also should be a feature.

RFP 3175 Cybersecurity Identity Protection and SIEM
RFP 3177 Patch Management
RFP 3178 Digital Resource Inventory
RFP 3179 IT and Network Security Audit
RFP 3180 Student Identity and Access Management

Answers to Vendor Questions
April 7, 2025

The following questions were submitted by interested bidders. The questions are cybersecurity related; however, the inquiries did not identify a specific RFP. The Division is issuing this Answers to Vendor Questions document across all five RFPs.

Additionally, "Answers to Vendor Questions" for each of the five individual RFPs are being issued concurrently.

Q 1.   How many users (Faculty) does the school have?
A 1.   There are approximately 3,000 faculty.

Q 2.   How many users (students) does the school have?
A 2.   There are approximately 14,000 students.

Q 3.   Do you use VMs? Can you tell us about VMs vs physical computers?
A 3.   Yes, the Division uses VMs as well as physical computers.

Q 4.   Do you use office 365 or Gsuite mainly?
A 4.   The Division uses both Office 365 and Gsuite.

Q 5.   Is the networking segmented between students and faculty?
A 5.   No, the networking is not segmented between students and faculty.

Q 6.   Please confirm your annual Preliminary Pre-Discount funding Commitment ($)?
A 6.   Total prediscount budget for eligible equipment/service is $544,068.00 for all projects. There are five cybersecurity related RFPs. The amount to spend on each will be determined upon review of proposals. Bidders are encouraged to provide a la carte prices for their products so that the Division may opt to make a partial award consistent with their budget.

Q 7.   What is your total Staff device count?
A 7.   See answer to Question 1.
Q 8.   What is your total Student device Count?
A 8.   Approximately 14,000 student devices.

Q 9.   How many File Servers do you have onsite?
A 9.   This information is not relevant to any of the RFPs and will not be provided.

Q 10.   How many File Servers do you have hosted offsite?
A 10.   This information is not relevant to any of the RFPs and will not be provided.

Q 11.   Are you looking for solutions that you will manage with in-house staff, or would you like a Client-Managed or Fully Managed solution? Would you like quotes for both?
A 11.   Please include both options in your proposal.

Q 12.   Given that available funds will likely not provide maximum protection for all devices; are you looking to provide some level of security for all devices or are you looking for a solution that provides maximum security for your key devices that would be likely targets for an attack? (Servers, Cloud, Key employees, etc.) – Would you be interested in a quote for both?
A 12.   Please include both options in your proposal.

Q 13.   In addition to what you have requested, we may wish to propose an additional alternative security solution for your consideration. To help us customize that solution, please provide us answers to the following Questions:

1) Do you have Anti-Virus with Endpoint Detection and Response (EDR) capabilities? If you, what solution are you using?
2) Do you have a Security Information and Event Management (SIEM) solution in place? If you, what solution are you using?
3) Do you have a Secure Access Service Edge (SASE) solution in place? If you, what solution are you using?
4) Do you have a 24/7 Managed SOC solution in place? If you, what solution are you using?
5) Do you have a Data Loss Prevention (DLP) solution in place? If you, what solution are you using?
6) Do you have a Zero Trust Networking (ZTN) solution in place? If you, what solution are you using?
7) Do you have an Application Allowlisting/Whitelisting solution in place? If you, what solution are you using?
8) Do you have an ongoing Vulnerability Assessment solution in place? If you, what solution are you using?
9) Do you have a SASE solution in place? If you, what solution are you using?
10) Do you have a Password Management solution in place? If you, what solution are you using?
11) Do you have a Patch Management solution in place? If you, what solution are you using?
12) Do you have a Disaster Recovery solution in place? If you, what solution are you using?

A 13. This information is not being provided. The Division does not seek alternative security solutions unless they are comparable to one or more of the issued RFPs. The cybersecurity pilot bidding rules do not allow the Division to accept and award contracts for cybersecurity solutions that are not within the scope of one of the issued RFPs.

Q 14. Please clarify the approximate number of assets, endpoints, or users covered under the scope?
A 14. There are approximately 17,000 items covered under the scope of the various RFPs.

Q 15. Please clarify any specific compliance frameworks or security standards that must be adhered to?
A 15. FERPA, State laws and School board policies must be fulfilled.

Q 16. Please clarify expected service levels or performance requirements for each area?
A 16. This question is not capable of being answered because it is too vague and unclear.

Q 17. How many desktop, laptops, servers physical and virtual require EDR(endpoint protection), for teachers and administrators?
A 17. Approximately 3,000 devices require EDR (endpoint protection) for faculty.

Q 18. How many desktop, laptops, servers physical and virtual require EDR (endpoint protection), for students?
A 18. Approximately 14,000 devices used by students are Chromebooks.

Q 19. Do you want the next-generation firewalls in high availability?
A 19. Such a request is outside the scope of any of the five issued RFPs.

Q 20. How much bandwidth does the firewall need to support?

A 20.   Such a request is outside the scope of any of the five issued RFPs.

Q 21.   How many users require MFA?
A 21.   Ideally all 17,000 users (students and staff combined) require MFA.

Q 22.   How many people need the identity protection, for teachers and administrators?
A 22.   Approximately 3,000 staff.

Q 23.   How many people need the identity protection, for students?
A 23.   Approximately 14,000 students.

Q 24.   How many desktop, laptops, servers physical and virtual require Patch management for teachers and administrators?
A 24.   Approximately 3,000 devices.

Q 25.   How many desktop, laptops, servers physical and virtual require Patch management for students?
A 25.   Approximately 14,000 devices.

Q 26.   Who do you use as a SIEM today?
A 26.   There is no SIEM currently in effect.