Purchasing Department
P. O. Box 13145 • Roanoke, VA 24031
(540) 853-1348 FAX (540) 853-2836

RFP 3175 Cybersecurity Identity Protection and SIEM
Addendum #1

Answers to Vendor Questions
April 7, 2025

Q 1: What was the annual spend for the previous year on this Project?
A 1: This is a new procurement.

Q 2: If this is a new Contract, what is the annual Budget for this?
A 2: Total prediscount budget for eligible equipment/service is $544,068.00 for all projects. RFP 3175 is one of five projects. 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 3: Are you open to a hybrid delivery model with a mix of offshore and onshore resources?
A 3: No.

Q 4: Is work going to be onsite or remote?
A 4: This is a matter of discretion for the vendor. Explain the work plan – onsite, remote, or combination in your proposal.

Q 5: Is there currently an incumbent company or previous incumbent: who completed a similar contract performing these services? If so - are they eligible to bid on this project and can you please provide the incumbent contract number: dollar value: and period of performance?
A 5: Yes. All vendors have the same opportunity and access to the same information to submit bids for this RFP.

Q 6: Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project?
A 6: Please see question and answer 2.

Q 7: Could you elaborate on the specific challenges or pain points you're encountering with the current system that this solution is intended to address?
A 7: The funding from the FCC cybersecurity pilot will allow RCPS to maximize our spend and procurement of additional safeguards against emerging threats.

Q 8: What is the projected timeline for the implementation: testing: and deployment of the new systems?

A 8: The timeline for the performance of work is dependent upon when the Division receives its Funding Commitment Decision Letter (FCDL) approving funding for this project. The Division has three years from the date of the FCDL to purchase the services and for the delivery of the services to be completed. The specific project timeline will be coordinated with Division technology staff and the winning bidder's point of contact.

Q 9: Which specific use cases or scenarios should the new Identity Protection platform focus on to enhance the existing EDR system?
A 9: We do not understand the Q. The vendor who submitted this Q may submit a clarification to the Q via email to ethorton@rcps.info, and we will try to A the Q.

Q 10: Are there any preferred technologies or vendors for the Identity Protection platform that we should take into account?
A 10: There is no preferred technology. Vendors are encouraged to submit alternative proposals using different technologies should they wish to do so.

Q 11: What key performance indicators (KPIs) will be used to assess the success of the integration between the Identity Protection platform and Entra ID/Active Directory?
A 11: This information is not available at this time.

Q 12: Do any legacy systems or additional identity providers need to be supported to ensure compatibility?
A 12: No.

Q 13: Is there a requirement for Single Sign-On (SSO) capabilities across all applications and systems?
A 13: Yes.

Q 14: What particular hybrid identity-based threats are currently concerning you and how should the platform tackle them?
A 14: The Division expects bidders to identify a range of identity threats and how their proposed solution will address and mitigate those threats.

Q 15: Are there any predefined risk detection policies that must be incorporated into the solution?
A 15: The Division seeks to receive template options.

Q 16: What levels of access control (e.g.: role-based: attribute-based) should the IDAM solution accommodate?
A 16: The same Role and Attribute base as both are used today will continue.

Q 17: Are there specific regulatory or compliance standards (e.g.: GDPR: HIPAA) that the IDAM solution needs to follow?
A 17: Yes: FERPA, State laws and School board policies must be fulfilled.

Q 18: Can you provide more details about the types of logs and data sources (e.g.: firewall: server events) that should be integrated into the SIEM system?

A 18: The Division requests that Firewall, Server Events, Endpoint evet logs and access point logs be integrated into the SIEM system.

Q 19: What is the estimated number of events per second (EPS) that the SIEM system should handle during regular operations?
A 19: This number is not knows as we do not have a current solution today.

Q 20: Could you provide a detailed list of log sources (e.g.: firewalls: servers: applications: access points) that need to be integrated?
A 20: Firewall, Server Events, Endpoint evet logs and access point logs need to be integrated into the SIEM solution.

Q 21: What level of customization do you expect for policies and automated responses within the SIEM system?
A 21: The Division expects to have the ability to fully customize policies and responses.

Q 22: Are there particular compliance or regulatory standards that the log retention and reporting features need to meet?
A 22: No.

Q 23: During times of peak activity (such as high traffic or a security incident): how many EPS should the system be prepared to manage?
A 23: The system should be able to handle traffic at all times.

Q 24: How many devices or systems are expected to send logs to the SIEM system initially: and how might this number change over time?
A 24: 3000 users and workstations, 100 servers, databases 5, network devices 400, security solutions VPN, EDR and MDM, Application logs N/A.

Q 25: Are there specific metrics or benchmarks that you are using to evaluate the SIEM system's ingestion and compression efficiency?
A 25: No.

Q 26: Are there specific log sources that generate a high volume of data and need special attention?
A 26: We do not have a current solution today.

Q 27: What is the expected daily log volume in gigabytes or terabytes across all sources?
A 27: This cannot be answered at this time. The information is not available.

Q 28: Is there a variation in data volume during peak times compared to off-peak times?
A 28: This cannot be answered at this time. The information is not available.

Q 29: For the 365-day retention requirement, can you estimate the total storage capacity needed: taking into account the daily log volume and compression?
A 29: The estimate is 25 Gb of storage capacity.

Q 30: Are there any anticipated growth rates for log sources, data volume, or EPS over the next 3 to 5 years?
A 30: We do not anticipate any major changes.

Q 31: What level of compression efficiency is expected and are there preferred algorithms or methods for achieving it?
A 31: We do not have a current solution today.

Q 32: Can you clarify whether the ingest size requirements (minimum of 50 GB) are expected to scale over time and if so what is the anticipated growth?
A 32: That number was placed to ensure that there was enough ingest for all logs.

Q 33: What level of ongoing support and training do you expect from the vendor for operating and maintaining the system?
A 33: Please include support and maintenance options in your proposal. RCPS expects medium to high level support.

Q 34: What criteria will be used to assess the proposals? Are there particular areas of focus such as cost, innovation, or scalability?
A 34: RFP Section VIII contains this information.

Q 35: Are there any reference projects or case studies that the Division would like to review before making a final decision on the vendor?
A 35: Bidders may submit information that may include reference projects or case studies that demonstrate their qualifications and competencies in the area of the procurement. Please note that reference projects or case studies are not mandatory, but may be submitted as part of vendor's proposal.

Q 36: Does RCPS have a preferred implementation? We assume by the language it is Cloud, but would like to confirm.
A 36: The Division initially supports Cloud as preferable but is open to other options.

Q 37: RCPS is expecting log retention to be a minimum of 365 days. Is that 365 days cold storage? How many days of hot searchable logs is RCPS expecting?
A 37: Those logs are intended to be accessible if needed.

Q 38: For resource and planning purposes: could RCPS share where the logs are coming from? Are they coming from faculty, staff, contractors, and/or students? How many faculty, staff, contractors, and/or students is RCPS expecting to send data to be ingested into the Next-Gen SIEM?
A 38: 3,000 Staff, 14,000 Students

Q 39: For resource and planning purposes: could RCPS share how many workstations and servers will be sending logs to the Next-Gen SIEM?
A 39: The estimate is 3000 work stations/servers.

Q 40: Is our assumption correct that RCPS is using CrowdStrike for Next-Gen Antivirus as well? If not, would RCPS be willing to share the vendor providing Next-Gen Antivirus – assuming that RCPS wants this information ingested into the SIEM?
A 40: Yes, RCPS is using CrowdStrike for its antivirus protection.

Q 41: Are there any other additional integrations expected by RCPS? Maybe vulnerability management?
A 41: Please provide these options as an "a la carte" option that the Division may or may not purchase depending on its budget and prioritization of cybersecurity needs.

Q 42: Is RCPS also expecting to ingest Office 365 information as well?
A 42: Some Office 365 data would be ingested.

Q 43: What is the number of devices, applications, and systems to monitor?
A 43: 3000 users and workstations, 100 servers, 4 databases, 400 network devices, security solutions, VPN, EDR and MDM, Application logs N/A.

Q 44: Please indicate integration needs with existing security and IT infrastructure (e.g., FortiGate, FortiAnalyzer, third-party firewalls, SIEMs, servers).
A 44: Firewall, Server Events, Endpoint evet logs and access point logs require integration with existing security IT infrastructure.

Q 45: Confirm licensing requirements such as the number of monitored devices or advanced features (e.g.: machine learning).
A 45: 3000 users and workstations, 100 servers, 5 databases, 400 network devices, security solutions, VPN, EDR and MDM, Application logs N/A.

Q 46: The RFP requires an offeror to have a place of business located within a 220-mile radius of the geographic area of the Division's boundaries, and if not, is disqualified: Please clarify what is meant by the Division's boundaries. How is the actual distance calculated?
A 46: We will waive the requirement if the vendor is able to remotely support the solution they provide.

Q 47: In Section II. STATEMENT OF NEED AND TECHNICAL SCOPE OF WORK point (D): Is the listed preferred product CrowdStrike EDR licensing
A 47: Yes.

Q 48: We can quote two licensing programs for government licensing AOSG or CSP Government. Which is appropriate for Roanoke City Public Schools?
A 48: The Division is unfamiliar with the two government licensing programs cited in the question, and therefore, is unable to answer this question. The vendor should research this question and figure out which of the license programs are eligible for the Division to make purchases under. If the Division is eligible for both license programs, the Division suggests that prices under the more favorable contract should be incorporated into the Vendor's proposal.

Q 49: Is RCPS open to exploring non-USA/Canada based hybrid options to provide the requested services and solutions? Our clients typically want to leverage this option to get access to our global pool of cybersecurity professionals in a cost-efficient manner.
A 49: No.

Q 50: Can the RCPS provide any information on the budget required to support these services? (E.g., budget details)
A 50: This question was answered in Question 2 above.

Q 51: Is the RCPS currently using any service providers that are assisting the School in performing the requested services? If so, who are these providers?
A 51: All Vendors will have access to the same information concerning this procurement, and therefore, all proposals will be evaluated according to the bid evaluation matrix in Section VIII of the RFP and the most cost-effective proposal will be selected.

Q 52: Does the Division require 24/7 monitoring and response capabilities, or are there specific hours of operation for SOC services?
A 52: This is not a requirement. The Division encourages vendors to provide pricing with and without 24/7 monitoring and response capabilities, and further, to describe the specific hours of operation for SOC services that are incorporated into the Vendor's base price (if any such services are part of the base price).

Q 53: Is Division expecting the vendor to provide full L1, L2, and L3 analyst support, or will the focus be primarily on L1 and L2 level support, with escalation to your internal team for L3 tasks?
A 53: Yes, the vendor is expected to provide L1 and L2 support and L3 support and tasks will be escalated to the Division staff.

Q 54: In addition to standard SOC roles such as L1 Analyst, L2 Analyst, SOC Lead, and SOC Manager, are you looking for any specific additional roles to support this engagement, such as Detection Engineer, Customer Success Manager, Compliance Consultant, Threat Hunter, or any other specialized roles?
A 54: The Division does not have pre-conceived requirements and the Vendor should specify the staff plan for this procurement that will enable the Vendor to meet the requirements of the RFP. Please note that the Division is not seeking a SOC as part of this procurement.

Q 55: Are there any compliance regulations (HIPAA, PCI, ISO 27001, etc.) the SOC is required to uphold?
A 55: Bidders must comply with FERPA, State laws and School board policies.

Q 56: Are there any data residency or data sovereignty requirements that the Vendor needs to consider?
A 56: The data must reside in the United States.

Q 57: Is the Division looking for dedicated full-time resources from the partner to deliver the in-scope services, or would you be open to utilizing a shared resource model where resources are shared across multiple clients?

A 57: The Division is looking for a SaaS solution but as noted above is open to considering other service delivery models.

Q 58: What is the current estimated volume of alerts generated in the SIEM, and qualified incidents per month broken down by priority?
A 58: Unknown at this time. There is no solution in place currently.

Q 59: What is your daily ingestion volume (in GB or TB) for logs and events?
A 59: Unknown at this time. There is no solution in place currently.

Q 60: Other than security incidents reported from the SIEM, what other sources does the Division expect bidders to support with SOC services ? E.g. Phishing emails reported from end users, etc.
A 60: The Division is not seeking a SOC solution.

Q 61: Is Division currently subscribed to any Threat Intelligence feed(s)? Does Division have a Threat Intelligence platform? Or looking for new Threat Intelligence Platform?
A 61: The Division is currently subscribed to a Threat Intelligence feed. The Division does not have a Threat Intelligence platform and is not seeking a Threat Intelligence Platform.

Q 62: Please provide details of current security controls in place and confirm which of those security solutions are integrated with SIEM today.
A 62: There is no SIEM today and therefore no security solutions are integrated with SIEM.

Q 63: Does Division seek SOAR capability?
A 63: No.

Q 64: Please provide details of ticketing system currently in use for incident and service management.
A 64: Quest KACE

Q 65: Please provide the count of devices for each category within your environment that will be included for integration into SIEM. Please include additional data source types that are available in your environment
Users
Servers: (Windows, Linux, etc) - count by OS
Workstations: (Windows, Linux, macOS, etc) - count by OS
Database - count by product
Network Devices: (e.g., Firewalls, Routers, Switches)
Security Solutions: (e.g., WAF, VPN, Proxy,EDR, DLP,MDM etc.)
Application logs: (ex.
Other: (any other devices within scope not mentioned above)Users
Servers: (Windows, Linux, etc) - count by OS
Workstations: (Windows, Linux, macOS, etc) - count by OS
Database - count by product
Network Devices: (e.g., Firewalls, Routers, Switches)
Security Solutions: (e.g., WAF, VPN, Proxy,EDR, DLP,MDM etc.)
Application logs: (ex.

Other: (any other devices within scope not mentioned above)

A 65: 3000 users and workstations, 100 servers, five databases, 400 network devices, security solutions -- VPN, EDR and MDM. Application logs N/A.

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.