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

RFP 3177 PATCH MANAGEMENT
Addendum #1

Answer to Vendor Questions
April 7, 2025

Q 1: How many Windows based Workstations and Servers require automated Patch Management and reporting?
A 1: Approximately 3,000 workstation and servers combined.

Q 2: How many of the following require VSS/Patch Management: Desktop, Laptops, Tablets, Mobile Devices (Teachers/Students/Administration)
A 2: Approximately 3,000 workstation and servers combined.

Q 3: How many of the following require VSS/Patch Management: physical servers
A 3: Approximately 10 physical servers.

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: How many of the following require VSS/Patch Management: Virtual servers?
A 5: Approximately 100 virtual servers.

Q 6: How many of the following require VSS/Patch Management: Network devices (routers, switches, etc…)?
A 6: Approximately 400 devices.

Q 7: Are you currently working with an MSP/MSSP for Patch Management or are you handling it yourself?
A 7: This will be handed in-house by RCPS technology staff.

Q 8: What is the number of faculty and administrators' devices (not students) requiring Patch Management?
A 8: Approximately 3,000 devices.

Q 9: How many servers require Patch Management?
A 9: Approximately 100 servers.

Q 10: Are there any specific cybersecurity risks or incidents that RCPS has recently faced which prompted this RFP?
A 10: The cybersecurity pilot funds will allow the Division to address emerging threats.

Q 11: What are the primary pain points with the current patch management process that the new solution should address?
A 11: The cybersecurity pilot funds will allow the Division to address emerging threats.

Q 12: Can you provide more details about the existing Endpoint Detection and Response (EDR) systems in use?
A 12: The Division uses CrowdStrike.

Q 13: Are there any specific interoperability tests or certifications required for the proposed solution to be deemed compatible?
A 13: The solution must work with the Division's current hardware.

Q 14: How often are patches expected to be deployed, and is there a preference for manual versus automated approval processes?
A 14: Patching is expected immediately for critical patches and policy driven for other levels.

Q 15: Are there any specific compliance frameworks (like NIST, CISA) that the solution must adhere to?
Q 15: The Division is open to all compliance frameworks.

Q 16: Please share a list of all operating system versions used for computers and mobile devices.
A 16: Windows, Mac, and iOS.

Q 17: Please share the total number of endpoints to be managed including remote and LAN connected.
A 17: Approximately 3,000.

Q 18: Please share an overview of the types of virtual endpoints in use and how they are currently managed.
A 18: Windows and Linux VMs in vSphere.

Q 19: Please share what vulnerability scanners are being utilized.
A 19: CrowdStrike and Nessus provided by State/Federal Partners.

Q 20: Please clarify the following statement: "Automated Patch Management in conjunction with the existing endpoint management solution"? Specifically, what is the existing patch management solution, aside from Intune?
A 20: Intune and Quest KACE.

Q 21: Please share the ITSM tool currently in use.

A 21: CrowdStrike and Nessus provided by State/Federal Partners.

Q 22: Please elaborate on any other expected critical reports, in addition to those related to patch status, compliance, and unresolved vulnerabilities.
A 22: None expected but please provide options if you have them.

Q 23: Are there any additional endpoint management tools besides Microsoft Intune that the patch management solution must integrate with?
A 23: Quest KACE

Q 24: What are the critical device types and operating systems that the solution must support?
A 24: Windows and Mac endpoints. Windows and Linux servers.

Q 25: Can you provide specific reporting requirements, such as data formats or dashboards expected?
A 25: Please provide options in the proposal.

Q 26: Are there any KPIs or metrics that must be tracked as part of compliance reporting?
A 26: We do not have a current solution today.

Q 27: What are the expected response times for vulnerability detection and patch deployment?
A 27: Immediate responses for critical and policy driven for other criticality.

Q 28: Are there specific service level agreements (SLAs) or uptime requirements for the patch management tool?
A 28: We would obviously prefer 100% uptime. Please provide your proposed SLA.

Q 29: Can you confirm the proportion of the project that is expected to be covered by the CPP funding?
A 29: Total prediscount budget for eligible equipment/service is $544,068.00 for all projects. RFP 3177 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 30: How should vendors handle pricing for ineligible items or services under the CPP?
A 30: Itemize the ineligible costs in their price proposal

Q 31: Should the pricing include extended support and maintenance for the entire contract period, including the potential one-year extension?
A 31: Yes, and this cost should be separately itemized as part of the a la carte menu price proposal that the Division requests.

Q 32: When is the expected start date for implementation, considering the contract finalization on June 3, 2025?
A 32: 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 33: Are there phased implementation milestones, or is the expectation for full deployment immediately after contract signing?
A 33: This is dependent upon the start date when FCDL is received, and joint development of project plan between the vendor and the Division.

Q 34: Are there any expectations around training and knowledge transfer to RCPS IT staff after deployment?
A 34: Yes, basic training on the use of the product should be included in the price proposal. We expect to be able to use the product we purchase, and have access to support if needed.

Q 35: What is the preferred model for ongoing support (e.g., remote, on-site, 24/7)?
A 35: Remote support as needed.

Q 36: Can you clarify the weighting between technical approach (39 points) and price (51 points) during evaluation?
A 36: Allocation of 100 points for each bid, of which 39 points is the maximum score for technical approach and 51 points is the maximum score for price which will be allocated to the lowest cost bid for comparable services. The price points for the other bidders will be awarded based on the formula: low bid/bid being scored x 51 points.

Q 37: What would constitute disqualification beyond failure to meet FCC compliance requirements?
A 37: This is covered in RFP Section VII and Section IX. B.

Q 38: If required, what is the expected format for the oral presentation or technical demonstration?
A 38: This would be a virtual meeting, to be scheduled at the discretion of the Division.

Q 39: Are there any specific clauses or terms that RCPS typically negotiates post-award?
A 39: Sections IX and X of the RFP contain this information.

Q 40: Will there be periodic performance reviews during the contract period?
A 40: Both parties are expected to uphold their contractual obligations. The vendor's performance will be monitored on an ongoing basis.

Q 41: How will RCPS ensure data protection during patch management activities, especially with potentially sensitive student data?
A 41: We try to ensure industry best practices are followed and are receptive to the Vendor's suggestions on how the Division should handle this.

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.