Roanoke City PUBLIC SCHOOLS

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

RFP 3179 IT AND NETWORK SECURITY AUDIT
Addendum #1

Answer to Vendor Questions
April 7, 2025

Q 1. 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 1. All vendors, whether an incumbent or not an incumbent, are eligible to submit a proposal in response to this RFP. The past expenditures have no bearing on the future services that the Division may purchase.

Q 2. Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project?

A 2. The total prediscount budget for eligible equipment/service is $544,068.00 for all 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 there particular security issues or recent incidents that led to the request for this RFP regarding an IT and network security audit?

A 3. The cybersecurity pilot funds will allow the Division to address existing and emerging threats.

Q 4. What key deliverables or outcomes do you anticipate from this project beyond what is outlined in the scope of work?

A 4. The Division anticipates that gaps in its cybersecurity protections will be identified and actions to mitigate and resolve those gaps will be recommended in the report.

Q 5. Can you provide a detailed inventory of the IoT devices currently in use, or should the offeror be responsible for identifying these devices?

A 5. We do not have the detailed inventory that this question requests and anticipates that the inventory will be developed as part of the scope of work under the awarded contract.

Q 6. Have any specific types or brands of IoT devices posed notable security or performance challenges?

A 6. We do not have the detailed inventory that this question implicitly requests, and therefore the Division anticipates that the question will be addressed and answered as part of the scope of work under the awarded contract.

Q 7. What is your anticipated strategy for securing IoT devices? Are there any existing network segmentation policies or best practices that are currently in place?

A 7. Please provide options in your proposal, and an approach for developing this strategy during scope of work under the awarded contract.

Q 8. How many VPN connections are in operation, and are they centralized or distributed across various locations?

A 8. There is one VPN connection in a central location.

Q 9. Are there specific VPN vendors or solutions currently in use that should be considered during the assessment?

A 9. Our VPN should be in scope if the vendor submits a proposal related to VPN.

Q 10. Are there any industry-specific compliance standards (e.g., GDPR, HIPAA) that the VPN recommendations need to address?

A 10. Yes - FERPA, State laws and School board policies.

Q 11. Could you share information about the current configurations and vendor solutions (e.g., VMware, Cisco Meraki) used for these systems?

A 11. This information is not going to be shared at this time because of its sensitive nature and because the information is not essential to the preparation of a proposal to conduct the audit requested in this RFP.

Q 12. Are there particular concerns or past incidents related to misconfigurations in these environments that we should be aware of?

A 12. The cybersecurity pilot funds will allow the Division to address existing and emerging threats.

Q 13. What level of detail do you expect in the mapping and recommendations? For instance, should it include diagrams or simulations?

A 13. Please address your suggested detail in the mapping and recommendations in your proposal. If there are multiple options, please provide them based on a la carte menu pricing.

Q 14. Are there specific policies or standard operating procedures (SOPs) that you believe are outdated or inadequate, or should the review comprehensively cover all documentation?

A 14. The proposed review should cover all documentation and include further suggestions for additional documentation that would be appropriate.

Q 15. Are there specific industry or regulatory standards (e.g., ISO 27001, NIST) that the policies need to align with?

A 15. No.

Q 16. What types of security controls (e.g., firewalls, encryption, IDS/IPS) are currently implemented, and are there preferred technologies or methodologies for their evaluation?

A 16. All of the examples mentioned in the question are in place.

Q 17. Are there known deficiencies in the existing technical controls that should be prioritized during the evaluation?

A 17. No. Please include suggestions in your proposal. The purpose of the audit is to identify deficiencies.

Q 18. Is there a risk management framework (e.g., FAIR, COSO) currently in use, or should one be proposed as part of the remediation plan?

A 18. Please provide options in your proposal.

Q 19. Are there specific high-risk areas or assets that necessitate a more detailed analysis?

A 19. Please include suggestions in your proposal.

Q 20. Are there predefined incident response plans or playbooks that should be evaluated, or is this something that needs to be developed from the ground up?

A 20. There are some plans in place that need to be evaluated and other plans that need to be developed from the ground up.

Q 21. What tools or technologies (e.g., SIEM, SOAR) are currently utilized for incident detection and response?

A 21. Neither SIEM nor SOAR are currently in use.

Q 22. Is there an up-to-date inventory of hardware and software assets, or will this need to be created as part of the audit?

A 22. Please include the creation of this inventory as part of your proposal, using a la carte pricing.

Q 23. Are there specific hardware or software systems that are due for upgrades or replacements?

A 23. Yes, there are.

Q 24. Are there particular aspects of the network infrastructure (e.g., firewall rules, VLANs) that require urgent attention or are known to be vulnerable?
A 24. Please make suggestions around components you deem critical in your proposal.

Q 25. Are there preferred tools for analyzing and securing the network, or should the vendor suggest solutions?
A 25. Please include suggestions in your proposal.

Q 26. Are there known discrepancies between software licenses and actual usage that the audit should focus on?
A 26. No.

Q 27. Is there a preference for specific tools or processes to ensure ongoing license compliance and accurate asset reconciliation?
A 27. Please include suggestions in your proposal.

Q 28. Are there examples of effective step-by-step remediation plans from the past, or do you have preferences for how such plans should be structured?
A 28. Please include suggestions in your proposal.

Q 29. What level of detail do you expect in the final written report and work plan? Should it include a prioritized action list, cost estimates, or timelines for each recommendation?
A 29. Vendors should propose options with different prices for a basic, intermediate and detailed audit report. In all cases, the audit report should include recommended actions for the Division to rectify the vulnerabilities identified.

Q 30. What is the expected timeline for completing the audit, including the submission of findings and recommendations?
A 30. 30 – 90 days.

Q 31. How will the proposals be assessed? Are cost, experience, or innovative solutions prioritized more heavily in the selection process?
A 31. See Section VIII of the RFP. There is a maximum of 100 points to be allocated to each bid, of which 39 points will be available for technical approach and 51 points for price. The lowest price bid for comparable scope of services will receive 51 points, and then price points to other bidders will be awarded based on the formula: low bid/bid being scored x 51 points.

Q 32. Could an exception be made to the rule that automatically disqualifies an Offeror who does not have a place of business located within a 220-mile radius of the geographic area of the Division's boundaries?

A 32. Yes, the Division will waive this requirement if the vendor is able to demonstrate that the vendor can remotely support the solution they provide.

Q 33. For hardware identification, would you like us to identify only the hardware that are connected to the network but not yet listed in your inventory? Or would you prefer us to identify all hardware, including devices that may not currently be connected to the network(which would require an on-site visit)?

A 33. Only devices not yet listed but are connected should be identified as part of the scope of the audit.

Q 34. For the hardware condition assessment, are you requesting an evaluation of the physical condition of the hardware?

A 34. The Division does not need an evaluation of the physical condition of its hardware – concerning the technical serviceability of the hardware and its useful life.

Q 35. Please confirm your IT organization is centralized.

A 35. Yes, the IT organization is centralized.

Q 36. How many IT staff are there? Of these, how many are dedicated to cybersecurity?

A 36. 20 total staff, of which one staff person is devoted to cybersecurity.

Q 37. What is Roanoke Public School's (RCPS's) budget for this project?

A 37. Total prediscount budget for eligible equipment/service is $544,068.00 for all projects. RFP 3180 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 38. Has RCPS had this type of audit performed in the past?

A 38. RCPS has had different types of IT audits conducted in the past.

Q 39. As an organization, are you confined to awarding to the lowest bidder?

A 39. See answer to question 31. RFP Section VIII addresses this question.

Q 40. Two titles are listed: IT and Network Security Audit and Cybersecurity Identity Protection and SIEM. Could you please confirm if both titles—'IT and Network Security Audit' and 'Cybersecurity Identity Protection and SIEM'—apply to this RFP?

A 40. The title of this RFP should be IT and Network Security Audit consistent with the Table of Contents and first page of the RFP.

Q 41. Are there any specific areas within the policies and procedures that you believe need more focus or improvement?

A 41. No.

Q 42. What does the task to “Evaluate Risk Management” entail? Is this a review of RCPS’s process for assessing and mitigating IT risks?

A 42. Yes, this is a review of the Division’s process for assessing and mitigating IT risks.

Q 43. When was the last IT risk assessment performed? Will we have access to the report?

A 43. 2022 and access to the report will be shared with the awarded vendor subject to required protections against disclosure of the information.

Q 44. Can you provide an approximate number of current software licenses? How often is compliance with license agreements reviewed?

A 44. The Division cannot answer this question because it is too broad.

Q 45. The scope includes an evaluation of “technical security controls.” What exactly does this include? Is this a full review of IT processes and general controls, such as change and configuration management, data and system backup, disaster recovery, end-user training, logging and monitoring, identity management, etc.? Or, is it limited to select components of IT operations, such as patch management and data backup?

A 45. Please include all of these options in your proposal.

Q 46. What is included in the task to “ensure incident readiness”?

A 46. This task means, by the vendor’s measure, is the Division prepared to respond to security incidents.

Q 47. Is this limited to a review of RCPS’s incident response plan? Is the incident response plan formal and documented? When was it last tested and updated?

A 47. No, this proposal is not limited to review of the Division’s incident response plan which was last updated in 2025.

Q 48. Is a tabletop exercise/incident response simulation desired? If so, how many participants should the exercise include?

A 48. Please include this option in your proposal.

Q 49. What are RCPS’s primary concerns from a compliance standpoint?

A 49. The cybersecurity pilot funds will allow the Division to address existing and emerging threats.

Q 50. Excluding redundant or firewalls running in HA mode, how many firewalls are in scope?

A 50. One firewall.

Q 51. Does RCPS have a current hardware/software inventory?
A 51. Yes.

Q 52. We interpret this to be a detailed configuration review of the security components of various hardware elements (server operating systems, workstations, routers, and switches). Assuming that is correct, how many routers | switches are in scope for a configuration review?
A 52. Approximately 400 devices.

Q 53. How many unique server operating systems or OS builds are in scope for security configuration reviews?
A 53. Approximately five operating systems/OS builds.

Q 54. What operating systems are running on the workstations? Windows 10/11 only? MacOS?
A 54. Windows 10/11 and Mac OS

Q 55. How many enterprise applications are in scope?
A 55. Please include this in your proposal.

Q 56. Are detailed security assessments of technical application controls, user access permissions, segregation of duties, web interfaces, APIs, databases, and host operating systems desired? Or, is the software evaluation focused more on software license compliance?
A 56. Please include this in your proposal.

Q 57. What brands of devices do you have in your network?
A 57. Lenovo, Dell, and Apple primarily.

Q 58. What security assessments or penetration tests have been conducted recently?
A 58. An external vulnerability assessment and penetration test has been conducted recently.

Q 59. Are security patches and firmware updates applied regularly to all devices?
A 59. Yes.

Q 60. What authentication and encryption mechanisms are used for IoT devices?
A 60. Part of the scope of the RFP is for the vendor to identify all IoT devices and to address the authentication and encryption mechanisms for those devices.

Q 61. Are IoT devices segmented into dedicated VLANs or network zones?
A 61. Yes, that is the plan.

Q 62. Is there centralized logging or behavioral monitoring for IoT device traffic?
A 62. There is no centralized logging or behavioral monitoring for IoT device traffic.

Q 63. Are multi-factor authentication (MFA) and least privilege principles enforced for VPN access?
A 63. Yes.

Q 64. How are VLANs structured to segment network traffic?
A 64. This information is not publicly available due to security concerns. The winning bidder will have access to this information with appropriate safeguards to protect against disclosure of the information in the public domain. Further, the Division believes that this information is ***not*** essential for a vendor to be able to prepare a proposal.

Q 65. How is storage area network (SAN) access controlled and monitored?
A 65. This is done according to industry best practices.

Q 66. Is VCenter properly secured with role-based access controls (RBAC) and encrypted communication?
A 66. Yes, it is.

Q 67. Are existing audit logs maintained for VCenter access and changes?
A 67. Yes, they are.

Q 68. Are firewall rules audited regularly, and how are changes tracked?
A 68. Yes, they are.

Q 69. Are change management practices in place for VLANs, SAN, and firewall configurations?
A 69. No, they are not.

Q 70. What security measures (e.g., IDS/IPS, logging) are in place for network traffic monitoring?
A 70. IDS/IPS measures are in place for network traffic monitoring.

Q 71. Are security policies and standard operating procedures (SOPs) documented and enforced?
A 71. Yes, they are.

Q 72. What security frameworks (e.g., NIST, ISO 27001, CIS Controls) are followed?
A 72. The Division does not conform to a single security framework.

Q 73. How often are security controls reviewed and updated?
A 73. The security controls are reviewed and updated annually.

Q 74. How is compliance with industry standards (e.g., HIPAA, GDPR, PCI-DSS) verified?
A 74. Compliance with industry standards is verified through third-party audits.

Q 75. What tools are used to monitor and enforce security policy compliance?
A 75. This information is not publicly available due to security concerns. The winning bidder will have access to this information with appropriate safeguards to protect against disclosure of the information in the public domain. Further, the Division believes that this information is ***not*** essential for a vendor to be able to prepare a proposal.

Q 76. Are staff members trained on security SOPs and compliance requirements?
A 76. Yes, they are.

Q 77. What is the frequency and scope of internal or external security audits?
A 77. This information is not publicly available due to security concerns. The winning bidder will have access to this information with appropriate safeguards to protect against disclosure of the information in the public domain. Further, the Division believes that this information is ***not*** essential for a vendor to be able to prepare a proposal.

Q 78. Is a formal risk assessment or risk register maintained?
A 78. This information is not publicly available due to security concerns. The winning bidder will have access to this information with appropriate safeguards to protect against disclosure of the information in the public domain. Further, the Division believes that this information is ***not*** essential for a vendor to be able to prepare a proposal.

Q 79. Is there a Security Information and Event Management (SIEM) platform in use?
A 79. A SIEM platform is not currently in use.

Q 80. Are incident response plans documented and regularly tested?
A 80. Yes, they are.

Q 81. What is the average response time to detected security incidents?
A 81. Based on the incidents that have occurred to date, the response time has been immediate.

Q 82. Are there established incident escalation procedures?
A 82. Yes, there are.

Q 83. Have tabletop or live simulation exercises been conducted?
A 83. Yes, they have.

Q 84. How is the hardware and software inventory currently maintained and validated?

A 84. The hardware and software inventory is maintained through a third party system and is subject to annual audits.

Q 85. Are automated tools used for asset discovery and tracking?

A 85. No, they are not.

Q 86. How is license compliance verified?

A 86. The Division is unable to answer the question because they do not understand what is being asked.

Q 87. Are there processes in place for reconciling inventory with procurement and warranty records?

A 87. Yes, there are.

Q 88. How frequently is asset data updated and validated?

A 88. Asset data is updated and validated annually at a minimum.

Q 89. Is there an incumbent currently providing these services? If so, who is it?

A 89. Yes, there is an incumbent and its identification is irrelevant. All vendors, whether an incumbent or not an incumbent, are eligible to submit a proposal in response to this RFP.

Q 90. You mentioned this may apply to FCC CPP grants. Do you know how much funding you intend to request? Have you developed an Independent Government Cost Estimate (IGCE)?

A 90. See answer to question 2. Further the development of an IGCE is not required. The purpose of competitively bidding this project is to obtain the most cost-effective proposal.

Q 91. Are you open to a blended model (on-site and remote), or do you prefer all assessments to be conducted on-site?

A 91. The Division is open to all options.

Q 92. What are the Division’s top priorities or pain points that this audit is intended to address?

A 92. The purpose of the audit is stated in the RFP.

Q 93. Are there specific areas of concern within the environment (e.g., cloud security, endpoint protection, IoT)?

A 93. The cybersecurity pilot funds will allow the Division to address existing and emerging threats

Q 94. What internal resources (e.g., staff time, tools, access) will be made available to support the audit?

A 94. The winning bidder will have access to the cybersecurity coordinator to answer questions and provide data.

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.