RFP-3151 Information Technology (IT) Audit Services
Pre Bid Questions

1. Q: Will the execution of this engagement require on-site contractors or can this be done remotely?

A: Remote work is acceptable and often preferred. However, certain engagements may require on-site presence depending on the nature of the audit.

2. Q: Will this engagement require the winning vendor to perform the external penetration tests and vulnerability scans?

A: Yes. It is likely the winning contractor(s) may perform the external penetration tests and vulnerability scans

3. Q: Can non-minority subcontractors be used?

A: Yes. JCPS must be notified prior to subcontractors being used.

4. Q: What is the timeframe expected for completion?

A: This varies by project type and scope. While simple audits may require fewer than 200 hours, more complex engagements may range from 350 to 650 hours or more. The selected vendor(s) will likely complete a variety of projects during the project period.

5. Q: Who would the contractor specifically report to?

A: The contractor will report to the JCPS Internal Audit Department.

6. Q: Will/can any of the JCPS internal auditors participate in the audits performed by the contractor?

A: Yes. JCPS Internal Audit will coordinate and may participate in engagements depending on scope and resource needs.

7. Q: Much of the work will require an auditor to be onsite for a considerable amount of time. Will JCPS prefer a local resource over an out of state resource?

A: The selected vendor(s) will likely complete a variety of projects during the project period. The needs for each project will vary. JCPS does not have preference regarding the use of a local resource.

8. Q: Many frameworks are listed in the RFP, has the school system adopted any of the specific frameworks listed? E.g. ISO27001, COBIT, CIS, NIST CSF

A: JCPS's Internal Audit department does not have a designated IT Governance framework.

9. Q: Is a formalized change control process implemented into operation at JCPS?

A: Generally, yes. However, this may vary on an application-by-application basis.

10. Q: Will the contractor present reports to the School Board?

A: The vendor(s) may be asked to present findings to management and occasionally to the Board or Audit Risk Management Advisory Committee. This will be determined on a case-by-case basis.

11. Q: Does a solid, documented inventory of systems and system owners exist and can be provided to the contractor?

A: This is currently under development.

12. Q: Has data classification been performed and is documented by JCPS?

A: This is currently under development.

13. Q: Is an information security policy documented, adopted, and operationalized at JCPS?

A: Generally, yes. However, this is under further development.

14. Q: Are network and enterprise-level system diagrams documented and be made available to the contractor?

A: Generally, yes. However, this may vary on an application-by-application basis.

15. Q: Is an ISO or CISO on staff?

A: A Chief Information Security Officer is on staff. Although, the official title may differ.

16. Q: Is there a cybersecurity team?

A: Yes. JCPS has a Cybersecurity Team.

17. Q: Can an org chart be provided?

A: Yes. The organization chart is available on the website.

18. Q: Does a vulnerability management program currently exist?

A: Yes, currently using known CVE's and application correlation via agent detection. Different Platforms, not automated.

19. Q: Are any MSP services in use today? If so, for what functions?

A: No

20. Q: When was the last IT audit?

A: A variety of IT Audit projects have been performed.

21. Q: Will past IT audit reports be made available to the contractor?

A: Yes. Past IT audit reports will be made available to the contractor

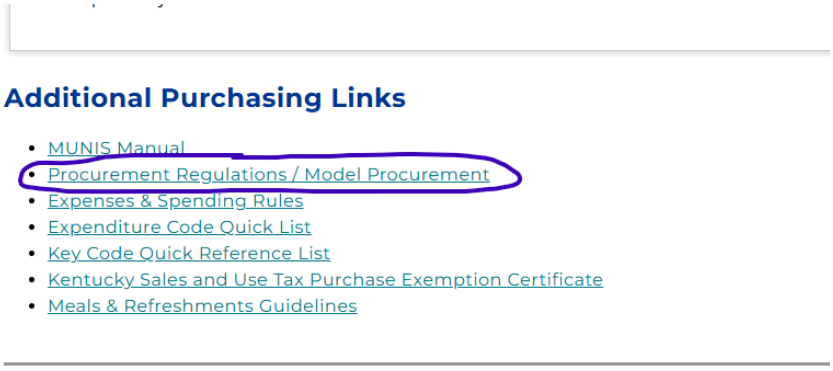
22. Q: Is this project grant funded?

A: No, this project is not grant funded.

23. Q: The link for the Model Procurement Regulations on page 3 of the RFP is not working, can you provide a working link?

A: **chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://core-docs.s3.us-east-1.amazonaws.com/documents/asset/uploaded_file/4298/JCPS/4060346/Model_Procurement.pdf**

This link can be found in the below screenshot on the JCPS Purchasing page



24. Q: Is the IT organization centralized or decentralized?

A: The IT Department is primarily centralized.

25. Q: What is Jefferson County Public School's (JCPS's) budget for this project?

A: JCPS does not disclose its IT audit services budget as part of this RFP.

26. Q: Has JCPS performed this type of audit in the past?

A: The selected vendor(s) will likely complete a variety of projects during the project period, some of which have been performed before.

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

A: No. JCPS is not required to award contracts based on the lowest bidder.

28. Q: Internal Network VAPT. Approximately how many subnets are in scope?

A: 375 Subnets

29. Q: Firewall Configuration Review Excluding redundant or firewalls running in HA mode, how many firewalls are in scope?

A: One

30. Q: Web Applications. Are the web applications Internet-facing or internal only?

A: A combination of both.

31. Q: Enterprise Applications
    Q: In addition to Munis, Time and Attendance, Student Assignment, and Provisioning UI – are there any additional enterprise applications in scope?
    Q: Are the enterprise applications COTS or internally developed?

A: There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Each IT audit will be engaged separately in accordance with the terms of the contract with the selected vendor(s).

32. Q: Database Security
    Q: How many unique databases are in scope for database-specific testing?
    Q: If databases are in different locations, can all locations be reached from one central location?

A: 21. All databases can be reached from a central location.

33. Server Configuration Analysis

a. How many unique server brands are in scope for testing? How many operating systems and which versions are in scope?

A. Server Brands – Dell, Operating Systems – Windows SVR 2012-2022, Linux Ubuntu 16.04-24.02 lTS

b. What devices does the Security Configuration Review cover?

A. Switches, Physical Servers, Virtual Servers, AP's

34. Wireless Network VAPT

a. Can you confirm if the wireless network is controller-based?

A: Yes

35. Social Engineering

a. How many targets are anticipated for each type of testing?

A. 5-10

36. Mobile Device Management

a. Is there an MDM solution; if so, what is the vendor?

A: JAMF

b. Endpoint Security Review: Can you confirm that the approximately 15,000 Windows Systems are on an OS operating system and the approximately 150,000 Chromebooks are on the Chrome operating system? Are there any additional operating systems?

A: We have Ipad OS, and MacOS systems as well

37. Q: How many documented IT policies, procedures, standards, and guidelines are in place?

A: There are currently 26 procedures and one overarching policy. Standards, guidelines, and processes would need to be answered on a per team basis, as they're not currently centrally managed.

38. Q: How many controls are included in the scope of the assessment?

A: There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Each IT audit will be engaged separately in accordance with the terms of the contract with the selected vendor(s).

39. Q: How many data centers are in scope for testing?

A: 21

40. Q: How many fulltime IT staff are there?

A: Approximately 100

41. Q: Does JCPS have formal HIPAA and FERPA policies | procedures | forms?

A: Yes. JCPS has formal HIPAA and FERPA policies | procedures | forms

42. Q: Which departments should be included in the HIPAA and FERPA Privacy Rule Compliance Assessment, and what is the number of locations per department?

A: Most departments will qualify for inclusion. The final sample of departments may be risk based.

43. Q: How many EMR applications are in scope? Which EMR applications are in scope?

A: None.

44. Q: Is JCPS working with any co-location vendors?

A: No

45. Q: Do you know whether the co-location vendor has multiple co-location facilities or is their operation in just one facility?

A: NA

46. Q: Does the co-location vendor have a SOC type 2 report?

A: NA

47. Q: Will you disclose the name of third party who operates the co-location facility?

A: The District does not disclose the names or contractual information regarding vendors as part of the RFP process.

48. Q: Does JCPS have any administrative/management responsibilities over this co-location?

A: NA

49. Q: How many users would you like to be phished?

A: 10 – 25% of staff population.

50. Q: How many firewalls are active in the environment?

A: This is under development.

51. Q: Can you clarify what your expectations are under network security audit for network monitoring?

A: The District's network monitoring process should be assessed as part of a network security audit.

52. Q: Switches are not called out under the network security audit; should the 2200 switches (or a subset) be part of the audit?

A: Yes

53. Q: Can you define what you're looking for in an awareness assessment?

A: An evaluation of the District's level of understanding of the concepts related to social engineering.

54. Q: What specific standards do you want the risk assessment held to? For example: NIST 800-30, ISO 27005?

A: NIST CSF

55. Q: Is the intention that these tests be executed in a single calendar year, or executed over multiple years under the guidance of the Internal Audit Department?

A: : There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Each IT audit will be engaged separately in accordance with the terms of the contract with the selected vendor(s). Projects may be assigned over the duration of the contract, which may extend beyond one year pending renewal.

56. Q: Are there current cybersecurity frameworks or control libraries JCPS prioritizes (e.g., NIST CSF vs. ISO 27001) in practice?

A: NIST CSF

57. Q: Will penetration testing and vulnerability assessments be conducted annually or on a per-project basis?

A: Annually or semiannually.

58. Q: Will penetration testing include internal networks, external assets, or both?

A: Both

59. Q: Are there any other compliance standards JCPS is subject to (e.g., CJIS, PCI-DSS) not listed in the RFP?

A: Yes.

60. Q: Is JCPS currently using any data loss prevention (DLP) or encryption technologies for PII/PHI?

A: Generally, yes. This is under further development.

61. Q: How frequently are follow-up audits expected to be conducted after the issuance of an initial report?

A: This will depend and vary based on the nature of the engagement.

62. Q: Will JCPS provide access to prior audit reports to aid in understanding the current environment and history of findings?

A: Yes.

63. Q: Will the District require staff from the vendor to be on-site for any engagements, or is remote work acceptable?

A: Remote work is acceptable and often preferred. However, certain engagements may require on-site presence depending on the nature of the audit.

64. Q: Is there an existing IT audit plan that the firm will be supplementing, or will the selected firm help develop a new one from scratch?

A: The selected firm(s) may help develop a new one from scratch

65. Q: Are there any specific systems or applications that the School does not want to be tested, or that require special handling?

A: This will be determined.

66. Q: What is the current level of cybersecurity expertise among your staff, and what training have they undergone?

A: Internal Audit does not have substantial cybersecurity expertise. However, the IT department has a Cybersecurity Team.

67. Q: Are there particular areas of concern or specific threats (e.g., ransomware, APTs) that you are particularly worried about?

A: Yes. Ransomware, Malware, DDoS Attacks, Data breaches, etc,

68. Q: Are there any budgetary constraints or resource limitations that we should consider when developing the roadmap?

A: There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Each IT audit will be engaged separately in accordance with the terms of the contract with the selected vendor(s). Additional detail will be provided prior to engagement for a selected project. Budgetary constraints and resource limitations will vary by project.

69. Q: Can you provide a brief summary of the timeline required for the work?

A: There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Each IT audit will be engaged separately in accordance with the terms of the contract with the selected vendor(s). Additional detail will be provided prior to engagement for a selected project. The timeline will vary by project.

70. Q: Is there a budget that has been allocated for these assessments?

A: JCPS does not disclose budgetary information as part of the RFP process.

71. Q: Are there any requirements for the penetration testers to undergo background checks or other pre-vetting? If so, please provide details.

A: Yes. Must be subject to our standard background check.

72. Q: Do you have any outsourced IT functions?

A: There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Each IT audit will be engaged separately in accordance with the terms of the contract with the selected vendor(s). Additional detail will be provided prior to engagement for a selected project.

73. Q: Are devices hosted in cloud environments? Is it multi-tenant?

A: Yes

74. Q: Are there any IPs we should refrain from scanning?

A: This will be determined.

75. Q: How many data centers do you have? Are any hosted by 3rd party?

A: 21

76. Q: Will you approve conducting wireless pentest remotely using a Pentest Box? If yes, would you be willing to assist with any network connectivity issues while moving the box within its different wireless range?

A: There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Each IT audit will be engaged separately in accordance with the terms of the contract with the selected vendor(s). Additional detail will be provided prior to engagement for a selected project.

77. Q: Is social engineering (I.e., phishing assessment) covered as a part of this scope? If yes:
Provide details on the number of email IDs to be targeted for phishing assessments
Q: How many phishing scenarios are in scope?

Provide details on the number of locations in scope for physical impersonation or piggybacking assessments.
Would you assist in whitelisting IP addresses for phishing campaign should the emails get held in Spam?
Are phone calls or pretext assessments in scope?

A: There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Each IT audit will be engaged separately in accordance with the terms of the contract with the selected vendor(s). Additional detail will be provided prior to engagement for a selected project.

78. Q: Has the organization conducted a third-party network vulnerability assessment previously? If yes, provide the assessment date.

A: Yes Fall 2025

79. Q: Has JCPS already implemented AI-based tools, remote learning platforms, or IoT devices, or is this a forward-looking risk area?

A: Generally, yes. This is under further development.

80. Q: Will Internal Audit staff be assigned to support the execution of the IT audits within scope of this RFP? If yes, what is the level of direct assistance we can expect to receive from internal audit? (It would be helpful to have estimated hours by experience level.)

A: The selected vendor(s) should expect to complete IT Audit projects independently.

81. Q: Does management anticipate the audit can be performed fully virtually? Will site visits be required for the audit? If yes, please indicate the locations?

A: There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Remote work is acceptable and often preferred. However, certain engagements may require on-site presence depending on the nature of the audit.

82. Q: Will the deliverable follow the standard Internal Audit report template?

A: The vendor may use the standard Internal Audit report template.

83. Q: Could you describe the IT structure at JCPS? Is there a central department, or is it distributed?

A: The IT department is centralized.

84. Q: Are there outsourced IT Functions or critical service providers? Can you provide a list of your key 3rd party service providers?

A: There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Each IT audit will be engaged separately in accordance with the terms of the contract with the selected vendor(s). Additional detail will be provided prior to engagement for a selected project.

85. Q: What are the systems that will be included in scope for each audit and are they internally managed or outsourced to a service provider?

A: There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Each IT audit will be engaged separately in accordance with the terms of the contract with the selected vendor(s). Additional detail will be provided prior to engagement for a selected project.

86. Q: For the systems/applications are there common processes to manage them? For example, for user administration, is there one group who handles this? Same question for change management and computer operations.

A: Generally, yes. This is under further development.

Q: Any planned material changes to people, process, and technology?

A: JCPS, like many large districts, may experience strategic, financial, or regulatory changes that affect audit priorities. While no specific change is guaranteed, vendors should be prepared to adapt to evolving needs.

87. Q: Is a specific governance framework utilized by the District (ex. NIST CSF 2.0)

A: Generally, yes. This is under further development.

88. Q: What documentation does IA maintain regarding IT General Controls? If an inventory exists, can you provide details on the key controls identified?

A: This is under development.

89. Q: Other than the listed Web Applications, are there any other in scope systems that should be considered?

A: There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Each IT audit will be engaged separately in accordance with the terms of the contract with the selected vendor(s). Additional detail will be provided prior to engagement for a selected project.

90. Q: Will the penetration testing audit include web application penetration testing? If yes, please provide the scope of systems, and whether you would like authenticated testing?

A: There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Each IT audit will be engaged separately in accordance with the terms of the contract with the selected vendor(s). Additional detail will be provided prior to engagement for a selected project.

91. Q: Is authenticated testing desired for the web applications?
    Q: If yes, please advise for each application:
    Q: Would you consider the app complex, moderately complex, or simple?
    Q: High level – what does the app do?
    Q: Is there an API in use? If so, how many endpoints and parameters exist (approximately what percentage of parameters are read only)?
    Q: How many user roles will be provided?
    Q: Does the application allow fi le uploads?
    Q: Does the application store or process credit card information or PII?

A: There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Each IT audit will be engaged separately in accordance with the terms of the contract with the selected vendor(s). Additional detail will be provided prior to engagement for a selected project.

92. Q: How many employees are in scope for phishing?

A: There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Each IT audit will be engaged separately in accordance with the terms of the contract with the selected vendor(s). Additional detail will be provided prior to engagement for a selected project.

93. Q: Do you want to do more than one email phish to these employees?

A: There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Each IT audit will be engaged separately in accordance with the terms of the contract with the selected vendor(s). Additional detail will be provided prior to engagement for a selected project.

94. Q: Do you want to include phone calls (vishing) as a follow up to the email?

A: There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Each IT audit will be engaged separately in accordance with the terms of the contract with the selected vendor(s). Additional detail will be provided prior to engagement for a selected project.

95. Q: Are there regulatory requirements related to resilience including disaster recovery and business continuity planning that the District is subject to?

A: Yes.

96. Q: How is the Disaster Recovery Plan (DRP) structured? Is there a separate DRP for each IT team, Department, location, or system?

A: Generally, yes. This is under further development.

97. Q: Do all departments follow the same Business Impact Analysis (BIA), Business Continuity Plan (BCP) and DRP structure and process? Would management be comfortable with a sampling approach for review of department, process and application specific plans?

A: This is under further development.

98. Q: Is a tool used to manage the plans, and facilitate plan update and approval?

A: This is under further development.

99. Q: What regulatory requirements will be included in scope in addition to FERPA and HIPAA?

A: There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Each IT audit will be engaged separately in accordance with the terms of the contract with the selected vendor(s). Additional detail will be provided prior to engagement for a selected project.

100. Q: What applications will be included in scope? What are the ERP(s), SIS and other applications?

A: There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Each IT audit will be engaged separately in accordance with the terms of the contract with the selected vendor(s). Additional detail will be provided prior to engagement for a selected project.

101. Q: How many Internal IPs/External IPs at the 5-10 sites you want the vendor to test?

A: There are a variety of applications and systems in scope for the contract. However, the applications and systems selected for an IT audit of the specific application or system will depend on risk. Each IT audit will be engaged separately in accordance with the terms of the contract with the selected vendor(s). Additional detail will be provided prior to engagement for a selected project.

102. Q: How many firewalls are active in the environment?

A: [Response under development. This question has been referred to JCPS IT for input.]

103. Q: Can you clarify what your expectations are under network security audit for network monitoring?

A: The District's network monitoring process should be assessed as part of a network security audit.

104. Q: Switches are not called out under the network security audit; should the 2200 switches (or a subset) be part of the audit?

A: [Response under development. This question has been referred to JCPS IT for input.]

105. Q: Can you define what you're looking for in an awareness assessment?

A: An evaluation of the District's level of understanding of the concepts related to social engineering.

106. Q: What specific standards do you want the risk assessment held to? For example: NIST 800-30, ISO 27005?

A: This will be determined and agreed upon prior to the performance of a Risk Assessment project.

107. Q: Is the intention that these tests be executed in a single calendar year, or executed over multiple years under the guidance of the Internal Audit Department?

A: Executed over multiple years under the guidance of the Internal Audit Department