January 16, 2025

ADDENDUM NO.: Two

TO ALL OFFERORS

REFERENCE:	Request for Proposal No:	RFP# FDC-1220
	Dated:	December 17, 2024
	Commodity:	IT Security Auditing Services
	RFP Closing On:	January 30, 2025 @ 2:00 p.m.

Please note the clarifications and/or changes made on this proposal program:

AMS refers to JMU's Office of Audit Management Services

The following questions are answered below:

1. Are the audits listed in a. through j. all intended to be completed in the one-year contract?

   Answer: The audits listed are a population of potential audits. Typically, 3-5 are selected each year.

2. Has the University contracted with outside service providers to conduct IT Security Audits in the past? If so:
   a. When were the most recent IT Security Audits conducted and what was the scope?
   b. Who was the service provider?

   Answer: Yes. We typically have 3-5 done annually by our contracted vendors.

3. Would the University be willing to share the results of prior IT Security Audits with the awarded vendors?

   Answer: Results are FOIA exempt. They could potentially contain sensitive security information and will not be shared.

4. Does the University have a preference for awarding this project to service providers who have conducted work within the Commonwealth of Virginia?

   Answer: The vendor must be registered to work within the Commonwealth of Virginia and with eVA (https://eva.virginia.gov).

5. Does the University's AMS intend to provide resources and staff to support the IT Security Audits, or is the vendor to provide all the resources?

   Answer: The IT Auditor in AMS manages the audits, assists consultants during the audit, arranges the entrance conference for each audit, and ensures consultants have what they need to complete the audit (credentials, etc.).

6. Will the requested IT Security Audits be required to be conducted to meet Institute of Internal Auditors (IIA) standards?

   Answer: Not required

7. Will the requested IT Security Audits be considered performance audits under Yellow Book?

Answer: No

8. What is the requested start and completion date of the one-year contract?

   Answer: The contract will start after the successful completion of the RPF process. The contract will last for one year and have four optional one-year renewals.

9. Does the University use an audit tracking or compliance software that the audit results will be imported into? If so, what?

   Answer: Documents related to each audit are stored in AMS automated workpaper system.

10. Does the University have an allocated budget for this engagement that can be shared with proposers?

    Answer: AMS has a fixed budget for IT Security Auditing projects.

11. The RFP states, "The selected contractor(s) shall supply professionally certified staff, at hourly rates, qualified to perform IT Security Audits at the direction of the Director of Internal Audit." This seems to indicate that all work will be performed in a staff aug capacity to where JMU leadership will supervise all of the winning bidder's team instead of the bidder's Partner/ Principal/Director's leadership. Can you confirm if this is accurate or if some audits will be co-sourced entirely to the bidder such that the bidder's leadership team is responsible for staff supervision and review of the final deliverables.

    Answer: The contractor chosen to conduct an audit will manage their own staff. AMS will provide assistance to ensure that they have what they need to complete the audit. See #5 answer

12. Does JMU have any estimate for what percentage of the audits or work hours will need to be performed onsite vs just done remotely?

    Answer: Onsite or remotely depends on the audit. Most are done remotely.

13. Does JMU have a planned annual budget for these services or some idea of how many audits will need to be staffed with the winning bidder?

    Answer: AMS has a fixed budget for IT Security Auditing projects. AMS meets with IT annually to discuss the year's upcoming IT audits. Cost is one of the factors that determine the number of audits.

14. Can you clarify if SWAM participation is required or optional, and how will the 10 pts for SWAM usage be scored?

    Answer: SWaM participation is not required. However, JMU strives to work with SWaM vendors whenever practicable. A SWaM vendor would get 10 points if they are a certified SWaM vendor (registered with the Virginia Department of Small Business and Supplier Development (VSBSD)). A non-SWaM vendor utilizing SWaM sub-contractor (registered with VSBSD) would receive some portion of the 10 points available.

15. Can you clarify whether the projects require a mix of on-site and off-site work, or are they predominantly one or the other?

    Answer: Audits are typically either on-site or remote and determined during planning.

16. How will the scope of work for each project be defined? Will templates or prior examples be provided?

    Answer: The scope of audits are typically defined during an entrance conference meeting.

17. What are JMU's highest-priority areas for IT security auditing? Are there any recent audit findings that should be addressed in these engagements?

    Answer: AMS conducts a risk assessment annually. In the past, audits have been on a three-year cycle. Systems that support critical functions are considered a higher priority to assess.

18. Will JMU require resumes or bios for assigned staff during each project proposal?

    Answer: Bios for staff are required for the initial review and selection process. We will select 3-5 organizations to have on contract.

19. Are subcontractors allowed, and if so, are there any restrictions or additional requirements?

    Answer: Yes, they are allowed. Organizations may need to provide bios for any subcontractors used prior to any audit.

20. Can you elaborate on the specific deliverables required for each type of audit (e.g., penetration testing, vulnerability scans, etc.)?

    Answer: A final draft report covering the audit scope, approach and any findings should be provided at the end of an engagement. Any supporting documentations should be provided as well. Scan results, etc.

21. Are sample reports or templates available for review?

    Answer: No. Report format is up to the consultant performing the audit as long as it covers the scope, methodology and findings/recommendations.

22. What specific systems, applications, or networks are in scope for the penetration testing? Are there any excluded systems, applications, or segments of the network?

    Answer: All of our systems are potential candidates for audits. What will be included in an audit will be determined during an entrance conference.

23. What are the primary objectives of the penetration testing (e.g., vulnerability identification, exploit validation, compliance verification)? Is the focus on internal, external, or hybrid penetration testing?

    Answer: Pen tests will be conducted from both internal and external perspectives. The objectives are determined during an entrance conference.

24. Does JMU have a preferred penetration testing methodology (e.g., OWASP Testing Guide, PTES, or NIST SP 800-115)?

    Answer: We do not have a preferred methodology as long as the methodology used is well known.

25. Are automated scanning tools allowed, or is manual testing preferred?

    Answer: Yes, automated scanning tools are allowed. Organizations are responsible for the appropriate use of any tool used during an audit.

26. How often does JMU require penetration testing to be performed (e.g., annually, quarterly)?

    Answer: Annually for GLBA requirement. Network is every other year. Systems that support critical functions once every three years (hosted systems).

27. Will ad-hoc testing be required for major system changes or incidents?

    Answer: In the past, IT has used our contract to have a consultant assess a system after an upgrade.

28. Can JMU provide a network diagram, including segmentation and firewall configurations, to help define testing boundaries?

    Answer: Yes, if necessary, these will be provided prior to an audit.

29. Are there any cloud-based services or hybrid infrastructure elements that need to be tested?

    Answer: We do not conduct testing on cloud systems. We rely on third-party reports.

30. Will test accounts with specific privileges (e.g., admin, standard user) be provided for application testing?

    Answer: Yes, the appropriate accounts will be provided to consultants to complete an audit.

31. Is testing expected to include credentialed scans or only external unauthenticated testing?

    Answer: This will depend on the scope of the audit, which will be determined during an entrance conference.

32. Are wireless networks within scope? If so, how many wireless networks exist, and are separate SSIDs used for guest and internal networks?

    Answer: A wireless network audit is a potential engagement. Actual numbers and SSIDs will be discussed during planning.

33. Are there compliance frameworks or regulatory requirements guiding the penetration testing (e.g., NIST 800-53, ISO 27001, FERPA, HIPAA)?

    Answer: This would be discussed in planning for each project. It could depend on the type of data being processed/stored in the target area.

34. Are there specific reporting formats or templates required to align with these standards?

    Answer: No. Report format is up to the consultant performing the audit as long as it covers the scope, methodology and findings/recommendations.

35. Are there restrictions on the tools, scripts, or software that can be used during testing?

    Answer: No, all automated scanning tools, scripts and software are allowed. Organizations are responsible for the appropriate use of any tool used during an audit.

36. Is social engineering (e.g., phishing or pretexting) included in the scope?

    Answer: Social engineering typically is not included in an audit.

37. Will JMU provide a “blue team” to coordinate defensive responses during testing?

Answer: The Information Security Officer is included in all phases of the audit and will handle defensive responses initially and will delegate to the necessary staff to address.

38. Does JMU expect formal red-team engagements or assume passive observation?

    Answer: Engagements are typically more red team.

39. What specific details are required in the final penetration testing report? (e.g., executive summary, findings by severity, recommendations, risk matrix)

    Answer: A final draft report covering the audit scope, approach and any findings should be provided at the end of an engagement. Any supporting documentations should be provided as well. Scan results, etc.

40. Should reports include mitigation strategies or just identified vulnerabilities?

    Answer: Recommendations on how to remediate the findings are typically included.

41. Does JMU have a preferred risk rating framework for findings (e.g., CVSS scores, custom classifications)?

    Answer: Consultants are free to use any framework.

42. Are proof-of-concept exploits required to demonstrate identified vulnerabilities?

    Answer: They should be included as supporting evidence for identified issues.

43. Is there a process for safe exploitation to minimize downtime or disruptions?

    Answer: Testing times are identified during the entrance conference. Typically, times that would have a low impact are chosen for engagements. Consultants should use caution when testing.

44. Will follow-up testing be required after remediation efforts?

    Answer: Some audits may require follow-up testing.

45. Should the proposal account for retesting as part of the deliverable or provide optional pricing for retesting?

    Answer: Yes, if it is determined during the entrance conference that follow-up testing will be part of the engagement. Otherwise, follow-up testing will be a separate engagement.

46. Is there a dedicated staging or test environment, or will testing occur in the production environment?

    Answer: This will be determined during an entrance conference. Some core systems do have a test environment.

47. What safeguards need to be followed when testing in production?

    Answer: Testing times are identified during the entrance conference. Typically, times that would have a low impact are chosen for engagements. Consultants should use caution when testing. Safeguards are typically discussed during planning.

48. Are there restricted testing windows to avoid disruptions to university operations?

Answer: Testing times are identified during the entrance conference. Typically, times that would have a low impact are chosen for engagements. Consultants should use caution when testing. Safeguards are typically discussed during planning.

49. What are JMU's preferred schedules for conducting tests (e.g., weekends, nights)?

    Answer: Testing times are identified during the entrance conference. Typically, times that would have a low impact are chosen for engagements. Consultants should use caution when testing. Safeguards are typically discussed during planning.

50. What is the process for notifying stakeholders and getting approvals prior to testing?

    Answer: Stakeholders are identified during planning. Most of the time consultants do not need a separate approval prior to testing. They are required to send an email to stakeholders notifying them that they are starting and another email at the end of testing. Consultant's IP address should be shared as well.

51. Are there specific points of contact required during the testing period?

    Answer: Stakeholders are identified during planning. Most of the time consultants do not need a separate approval prior to testing. They are required to send an email to stakeholders notifying them that they are starting and another email at the end of testing. Consultant's IP address should be shared as well.

52. Are there data privacy or legal restrictions that must be observed during testing (e.g.,FERPA, HIPAA)?

    Answer: The university must comply with many regulations, including, but not limited to, HIPAA, FERPA, and GLBA. Consultants are required to proceed cautiously with testing to ensure the security of university systems and data.

53. Will there be specific contract terms to limit liability for findings related to downtime or data exposure?

    Answer: AMS is not sure how a finding could create liability.

54. Are NDAs required for testers, and if so, will templates be provided?

    Answer: Yes, NDA's may be required. A template will be provided.

55. What is JMU's process for responding to vulnerabilities or breaches identified during testing?

    Answer: In most cases, university staff will contact the vendor of the system to determine a resolution.

56. Will testers be involved in drafting incident response plans or conducting tabletop exercises?

    Answer: This has not been done in the past.

57. Does JMU expect named resources (e.g., resumes, certifications) to be identified in the proposal?

    Answer: It would be helpful to identify all potential staff and their experience. This will help us to select the most qualified consultants to have on contract.

58. Is there a minimum certification level required (e.g., OSCP, CEH, GPEN)?

Answer: Consultants who have staff that possess more certifications will be looked at more favorably.

59. Should pricing account for fixed-price engagements, or does JMU prefer time and materials pricing for penetration testing?

    Answer: Consultants should provide an hourly rate for on-site (inclusive of travel) and an hourly rate for remote/off-site work.

60. Are there restrictions on billing categories, such as separate charges for travel and software licenses?

    Answer: Allowable expenses will be discussed during planning.

61. Does JMU require post-engagement workshops or training sessions for internal IT staff?

    Answer: If there are findings, all that is needed are recommendations and appropriate resolutions.

62. Should documentation include step-by-step remediation guidance for IT teams?

    Answer: Any information that will help resolve a finding should be included in a recommendation.

63. Is ongoing vulnerability scanning or maintenance required as part of the contract?

    Answer: The engagements will be a point-in-time assessment of systems.

64. Should pricing for managed services or recurring assessments be included?

    Answer: The engagements will be a point-in-time assessment of systems.

65. Will JMU provide access to any tools, software, or scanning platforms?

    Answer: This has not been done in the past. Consultants have been required to use their own tools.

66. Are there restrictions on third-party tools we can use?

    Answer: The university expects that consultants will use reputable tools during engagements. Any questions about tools can be discussed during planning.

67. How frequently are status reports or updates required?

    Answer: Not all engagements are the same and this will be discussed during planning.

68. Are there any formal review or sign-off processes for deliverables?

    Answer: AMS has an internal review and sign-off process for deliverables received during the engagement.

69. Does JMU prefer fixed-price or time-and-material pricing structures for specific projects?

Answer: Consultants should provide an hourly rate for on-site (including travel) and an hourly rate for remote/off-site work.

70. Should travel costs be itemized separately or included in flat rates?

    Answer: Included in flat rates.

71. What invoicing formats and documentation are required for payment processing?

    Answer: There is no requirement for a specific format. An invoice with the costs associated with completing the engagement should be submitted for payment.

72. Are there specific payment terms for milestone-based deliverables?

    Answer: Payment for engagements is handled when the final report is provided to AMS. There are no exceptions to this.

73. What are the requirements for on-site visits, including badging and access controls?

    Answer: This will be discussed during planning. Typically, consultants are provided with credentials for testing. They will be escorted through sensitive areas if required.

74. Are there specific blackout dates or periods where testing cannot occur due to academic schedules?

    Answer: Yes. Typically, testing will be conducted during times to minimize any impacts.

75. Would the University consider accepting certifications other than those listed in the definition of "Certified Professional" on p. 2 (for example, ITIL Foundation v3, Certified Associate Chief Information Security Officer (C | CISO)? Also, could you please clarify whether all team members must fit the definition of Certified Professional, or if it's sufficient that each engagement be led by consultants with the required certifications?

    Answer: Yes, alternate certifications could be acceptable. Not all team members would need certifications, as long as they are under supervision of a certified consultant.

76. Are there any GLBA or PCIS audit needs that should be included?

    Answer: GLBA required audit is a potential engagement.

77. Is there a preference for NIST 800 or ISO 27001 compliance frameworks?

    Answer: Currently, JMU IT is using ISO.

78. Does this count as a VASCUPP award or is this just for JMU?

    Answer: This contract will be made available to the VASCUPP schools for their use, should they choose to do so. This will be a cooperative contract that can be utilized by any public body, (to include government/state agencies, political subdivisions, etc.), cooperative purchasing organizations, public or private health or educational institutions or any University related foundation and affiliated corporations

79. When is the next anticipated need for audit work to start at JMU?

    Answer: The goal is to have the selected consultants on contract before the end of the current fiscal year. Most likely, the need will not be until next fiscal year (7/1/2025-6/30/2026).

80. The RFP states "Definition of Term – Certified Professional is defined as holding current Certified Information Systems Auditor (CISA), Certified Information Systems Security professional (CISSP), Certified Information Systems Manager (CISM), Microsoft Certified Professional (MCP), Cisco Certified Network Associate (CCNA), Information Systems Security Management Professional (ISSMP)." This Reads as if all of the listed certifications are required for each consultant. Is that correct or is it just that a consultant must have one of the listed certifications for their appropriate area to be deemed a certified professional?

    Answer: At least one of the certifications.

81. Can you explain the last two columns of the table in Attachment B, specifically:
    "Total Subcontractor Contract Amount"
    "Total Dollars Paid Subcontractor to date"

    Answer:

    Total Subcontractor Contract Amount – Dollar amount allocated to SWaM subcontractor in the direct performance of the contract/task.

    Total Dollars Paid Subcontractor to date – The total dollar amount paid by the contract to the subcontractor.

82. Do the columns refer to work previously performed where the Offeror has used the sub-contractor to perform work? Does either value represent an estimate of what work might be performed by a given contractor?

    Answer: No. They should represent an estimate of the what work might be specific to the contract.

83. Under section 5 Part B #6, the ask is to identify sales in the past 12 months to VASCUPP members. Many of these institutions have moved to the VHEPC contract. Can VHEPC data be used in the response?

    Answer: Yes

84. Could you kindly provide information regarding the current budget allocated for these services or details about the prices paid under previous contracts for similar services?

    Answer: Our current budget has been sufficient to do GLBA testing and two to five other projects each year. Each project is carefully planned and scoped with input from JMU's IT and the consultant.

85. Will the University be permitting penetration testing to be performed by existing or previous IT or Managed Service Providers? Or will the University be requiring third-party independence to reduce the risks of conflicts of interest or the optics of "grading one's work"?

    Answer: We are looking to have contracts with some consultants who will perform pen tests.

86. Is the University currently using any service providers that are assisting the University in performing the requested services? If so, who are these providers?

Answer: The current providers can be found here.

87. Is there an incumbent providing similar services to the University? If yes, is the incumbent performing to the satisfaction of the University, and the Chief Information Security Officer?

    Answer: See the answer to question 86 above.

88. Is the incumbent eligible to bid on this contract?

    Answer: Yes.

89. Can the University provide any information on the budget required to support these services? (E.g., budget details)

    Answer: AMS has a fixed budget for these services and cost will be a factor. No more details about the budget will be provided.

90. Does the University have onsite audit preference or vendor can perform remotely?

    Answer: Potential engagements include on-site. There is no preference.

91. Can the University provide a brief high-level description and accounting of their computing infrastructure? (e.g., hard-wired versus wireless, Windows and or Linux and or Mac, number of domains, number networks, number of IP addresses, etc.)

    Answer: If necessary, infrastructure will be discussed during planning for each engagement.

92. How many of the external IP addresses are live or currently in use?

    Answer: Will be discussed during planning for each engagement if necessary.

93. For wireless access points, how many SSIDs and how many locations are in scope?

    Answer: Will be discussed during planning for each engagement if necessary.

94. Are all campus/network locations accessible from the central location of the network?

    Answer: Will be discussed during planning for each engagement if necessary.

95. Is there a EDR solution is in place? If so, what vendor is it? Is it centrally managed?

    Answer: The university refrains from answering this question.

96. Is there a cybersecurity department? Is there an ISO or CISO on staff?

    Answer: The university has an ISO. University IT manages cybersecurity.

97. When was the last time an overarching IT security risk assessment was performed?

    Answer: JMU conducts various risk assessments to meet the needs of the University.

98. Does the University have documentation of the designated system owners and data owners?

    Answer: Yes

99. Is there a conclusive/documented inventory of all assets in scope that can be provided to selected Vendor?

Answer: Will be discussed during planning for each engagement.

100. Does the University currently utilize any internal network vulnerability assessment tools? If so, what is the scan frequency?

Answer: Yes. The university refrains from answering this question.

101. Does the University use baseline images for systems?

Answer: Yes

102. Is formalized change management in place?

Answer: Yes

103. How many voice VLANS and IP phones are in-scope?

Answer: Will be discussed during planning if necessary.

104. How many wireless locations are in-scope?

Answer: Will be discussed during planning if necessary.

105. Does the University want any cloud environments tested? If so, which vendor?

Answer: We do not conduct testing on cloud systems. We rely on third-party reports.

106. Does the University have any remote access services in use (on-demand VPN, GoTo my PC, LogMeIn, etc.) in-scope?

Answer: Will be discussed during planning if necessary.

107. Does the University have any in-bound modems (or remote access) in use?

Answer: Will be discussed during planning if necessary.

108. Is there any allowability to redline terms and conditions to negotiate later?

Answer: Will be discussed during planning if necessary.

109. The RFP is titled “Information Technology Security Auditing Services”, will all projects awarded be strictly security focused? For instance, the statement of needs mentions wireless network assessment/server configuration which can include many considerations aside from security.

Answer: Engagements will be focused on security to assess the controls protecting university systems and data.

110. How is the security team currently staffed/structured and how would you describe your current approach to security?

Answer: Information about the Information Technology Department can be found at https://www.jmu.edu/computing/about/index.shtml

111. Is there a routine and scheduled IT and Security audit services?

Answer: AMS works with IT annually to create the annual audit plan.

112. How often does JMU conduct IT and Security Audit assessments?

Answer: Up to five consultant engagements may be conducted during a fiscal year.

113. Who manages the IT and Security Audit service schedules for JMU?

Answer: Most are managed by the IT Audit Specialist in AMS.

114. Is each academic division responsible for managing its own IT asset?

Answer: Some academic units manage their own systems.

115. Is each academic division responsible for conducting routine and scheduled IT and Security Audit?

Answer: They are included in audits managed by AMS

116. Who is Audit and Management Services (AMS)? Is this an external entity, like a contractor hired by JMU to perform routine IT And Security Audit services? Or, is AMS a division within JMU?

Answer: AMS is JMU's internal audit department.

117. Who is responsible for managing JMU's IT Assets?

Answer: Central IT manages most IT assets.

118. Does JMU keep an inventory list of its IT Assets?

Answer: Yes

119. Who tracks JMU's IT Assets?

Answer: Central IT manages most IT assets.

120. Does each academic division track its own IT Assets?

Answer: Yes

121. Who performs routine and scheduled maintenance?

Answer: Central IT for most systems

122. Is this RFP to replace the existing/current staff of contractors performing under formal Statement of Work agreement?

Answer: The current contracts expire in April of 2025.

123. Is this RFP to provide supplemental support to JMU Personnel performing IT Audit functions listed in Section IV, Paragraph C (a-j)?

Answer: Yes, we outsource highly technical audits, such as pen tests and vulnerability assessments. JMU's IT Auditor oversees the outsourced projects.

124. Is this RFP to also provide supplemental support to current Staff of Contractors that are performing IT Audit functions under formal Statement of Work agreement?

Answer: This RFP is to support JMU's AMS department.

125. How many Staff of Contractors currently provide IT Audit Services to JMU-AMS under formal Statement of Work agreement?

Answer: We have four vendors on contract.

126. How many of these IT Audit functions are being performed by JMU Personnel?

Answer: The listed examples are performed by consultants.

127. How many of these IT Audit functions are being performed by the Staff of Contractors that are performing under formal Statement of Work agreement?

Answer: The listed examples are performed by consultants.

128. How many web applications are being assessed?

Answer: This will be determined during planning.

129. What framework and platform are being used for the web application(s)?

Answer: This will be discussed during planning.

130. How many static pages are being assessed? (approximate)

Answer: This will be discussed during planning.

131. How many dynamic pages are being assessed? (approximate)

Answer: This will be discussed during planning.

132. Will the source code be made readily available?

Answer: No

133. Do you want role-based testing performed against this application?

Answer: This will be discussed during planning.

134. Do you want credentialed scans/assessments of the web applications performed?

Answer: This will be discussed during planning.

135. How many total IP addresses are being tested?

Answer: This will be discussed during planning.

136. How many internal IP addresses, if applicable?

Answer: This will be discussed during planning.

137. How many external IP addresses, if applicable?

Answer: This will be discussed during planning.

138. Are there any security devices in place that may impact the results of a penetration test such as a firewall, intrusion detection/prevention system, web application firewall, or load balancer?

Answer: This will be discussed during planning.

139. Would the University prefer SWaM agencies?

Answer: JMU strives to work with SWaM vendor whenever practicable.

140. Is subcontracting mandatory for SWaM-certified agencies?

Answer: No

141. Would the university award 10 points as per the evaluation criteria to a Prime -SWaM certified agency if the Prime vendor does not subcontract for this opportunity?

Answer: Yes, as long as they are SWaM certified with the VSBSD.

142. How many individual projects or separate Statement of Works were issued under this award in the previous five-year contract period?

Answer: We typically have 3-5 engagements per fiscal year.

143. Can you please provide the total dollar value of work awarded under this award during the previous five-year contract period?

Answer: This information is not readily available.

144. Who is the individual the proposal will be addressed to?

Answer: Instructions are on page 17 of the RFP.

145. The RFP states that a certified professional is defined as someone holding a current CISA, CISSP, CISM, MCP, CCNA, or ISSMP certification. Would JMU consider adding the CompTIA Advanced Security Practitioner (CASP+) to the list? This certification requires 10 years' of hands-on IT experience and at least 5 years of hands-on IT security experience. The certification demonstrates advanced competency in areas such as risk management, enterprise security, and governance.

Answer: This list is not comprehensive. All reputable certifications should be mentioned.

146. Who is responsible for determining the on-site versus off-site requirements?

Answer: This will be discussed during planning.

147. What is the anticipated level of on-site engagement, if any? And how many locations will require an on-site visit?

Answer: This will be discussed during planning.

148. Are there specific workshare requirements under the Small Business Subcontracting Plan?

Answer: There are no requirements to utilize SWaM vendors. However, JMU strives to work with SWaM vendors whenever practicable.

149. Is strict adherence to ISO 27002 security framework requirements mandatory, or are alternative frameworks, such as NIST, acceptable?

Answer: ISO 27002 is preferred. However, any reputable framework could be used.

150. Is it required to provide resumes for all proposed personnel at the time of submission?

Answer: It will help us adequately assess potential consultants if they provide information for all potential staff.

151. Can you confirm the number of wireless networks to be assessed and their respective locations?

Answer: This will be discussed during planning.

152. Could you provide the total number of web applications that require testing?

Answer: This will be discussed during planning.

153. Are there any specific requirements or needs for cloud security assessments in this engagement?

Answer: No. We do not conduct testing on cloud systems.

154. Is the request for a point in time scan of the Universities attack surface or an ongoing service to monitor for external vulnerabilities in real-time?

Answer: The engagements will be a point-in-time assessment of systems.

155. Is there an expectation that active or passive wireless survey would be conducted? If so the locations and floor plans of locations to be surveyed would be needed for an accurate SOW.

Answer: This will be discussed during planning.

156. What are the vendors, models, operating system versions and quantities of firewall and routers in the environment?

Answer: This will be discussed during planning.

157. What server operating system version and number of servers in the environment? Are these servers physical or virtual?

Answer: This will be discussed during planning.

158. What hypervisors are being used in the environment?

Answer: This will be discussed during planning.

159. What IaaS and SaaS platforms are being used in the environment?

Answer: This will be discussed during planning.

160. How many databases are in the environment?

Answer: This will be discussed during planning.

161. What platforms are these databases hosted on?

Answer: This will be discussed during planning.

162. What applications use these databases?

Answer: This will be discussed during planning.

163. Is the intent of this assessment to review the network vulnerability management process?

Answer: This will be discussed during planning.

164. How many web applications are in scope?

Answer: This will be discussed during planning.

165. Where are these web applications hosted?

Answer: This will be discussed during planning.

166. What platforms do these applications run on?

Answer: This will be discussed during planning.

167. What version of Windows are the domain controller running?

Answer: This will be discussed during planning.

168. Is there integration with Entra ID or other identity providers?

Answer: This will be discussed during planning.

169. If the state has already arrived at best market value rates for these services and an contract is in place to reference, why is an RFP being issued?)

Answer: JMU's current contracts for these services will expire in April 2025, and this RFP is being issued to replace them.

170. Is the support requested in the proposal hands-on, or purely advisor in performing an audit of functions conducted by JMU?

Answer: Our goal is to have multiple contractors on contract to provide audit services to assess technical controls. The engagements could be considered hands-on.

171. In order to perform work in this RFP, are contractors required to possess all or some of the certifications listed in Paragraph C? May some of these certifications be alternated pending we have more technical certifications that meet the same requirement?

Answer: It is not required for the staff to possess all the certifications.

172. (C.1.a) Pertaining to conducting External Vulnerability Scanning, are there any third-party assets or assets explicitly excluded from this scope?

Answer: This will be discussed during planning.

173. (C.1.b) Pertaining to conducting Wireless Network Assessments: A) How many networks are in scope? B) How many wi-fi access points are in scope? C) Do we have an up-to-date inventory of all wireless access points (APs) and their locations? D) What is the architecture of the wireless network (e.g., standalone, controller-based, cloud-managed)? E) Are there any mesh networks, IoT devices, or specialized APs in use? F) Are there any known issues with signal interference or channel congestion?

Answer: This will be discussed during planning.

174. (C.1.c) Pertaining to conducting Firewall and Router Security Assessments: A) Does JMU use one specific vendor (ie., Cisco, Juniper, Palo Alto) or a combination of vendors for its solution? If so, which vendors are leveraged within its Firewall and Router solution? B) Are any virtual firewalls or cloud-managed routers part of the assessment? C) Are logs enabled for both firewalls and routers? D) Do you allow telemetry to be exported to external entities (such as our SOC)? E) Are logs integrated with a SIEM (Security Information and Event Management) system for analysis?

Answer: This will be discussed during planning.

175. (C.1.d) Pertaining to conducting Server Configuration Assessments: A) Is there an updated inventory of all servers, including their roles and locations? B) Are server configurations documented and maintained in a central repository? C) Is access to remote management interfaces restricted to specific IPs or networks?

Answer: This will be discussed during planning.

176. (C.1.e) Pertaining to conducting Database Architecture Security Assessments: A) Are both production and non-production environments included in the assessment? B) Is there an updated inventory of all databases, including versions and roles? C) Are database architecture diagrams and data flow diagrams documented and up to date? D) Are logs entralized/monitored (e.g., through a SIEM system)? E) Is there a process for evaluating/applying updates without disrupting operations?

Answer: This will be discussed during planning.

177. (C.1.f) Pertaining to conducting Network Scanning Process Assessments: A) Are the tools configured for active, passive, or hybrid scanning? B) How does the organization discover and inventory all connected devices? C) Are unauthorized or rogue devices detected and flagged during scans? D) What size subnet/subnet range does JMU administer/lease? E) What is an estimate of the number of endpoints to be expected on the network? 500 – 1000, 1000 – 2,500, 2-500 – 5,000, or 5,000+? F) Do you allow telemetry to be exported to external entities (such as our SOC)?

Answer: This will be discussed during planning.

178. (C.1.h) Pertaining to conducting Active Directory Security Assessments: A) How many domains and domain controllers (DCs) are in the environment? B) Are all domain controllers running supported OS versions and fully patched? C) Are logs centralized (e.g., SIEM) and monitored for suspicious activities?

Answer: This will be discussed during planning.

179. (C.1.i) Pertaining to conducting Penetration Testing: A) Are there specific exclusions (e.g., certain servers, critical infrastructure)? B) Is the testing internal, external, or both (e.g., testing from within the network or from an external perspective)? C) Are cloud environments, third-party services, or IoT devices included? D) Is testing white-box (full access), black-box (no prior knowledge), or gray-box (partial knowledge)?

Answer: This will be discussed during planning.

180. (C.1.j) Pertaining to assessing Telecommunications: A) Which telecommunication services are included (e.g., voice, VoIP, wireless, data)? B) Are third-party managed services or service providers within scope? C) Are specific geographical locations or facilities included? D) Are third-party carriers and vendors assessed for security and compliance risks? E) Are contracts regularly reviewed for adherence to terms and emerging security needs? F) Are logs collected, centralized, and analyzed for security events?

Answer: This will be discussed during planning.

181. Please briefly describe what you mean by "Network Scanning Process Assessment" and “Telecommunications”.

Answer: Telecom would focus on the security of the VOIP implementation. The network scanning process assessment has never been included in our audit plan because we feel that we are covered by the internal and external pen tests.

182. Please describe what "other products and services" you typically see in your audits, or what you mean by this phrase.

Answer: We have not had any billing for services other than travel and lodging.

183. What is the typical lead time that you provide to your vendors for your audits?

Answer: During our meeting with IT at the beginning of the fiscal year, we identify the audits to be included for the year as well as identifying the potential consultants. AMS will reach out to those consultants to determine availability and request proposals.

184. Will the universities in each of the listed zones be utilizing services from selected vendors, or just JMU?

Answer: This RFP is being issued for JMU’s needs and will be made available to other VASCUPP schools, should they choose to utilize it. Pricing should be provided so that any VASCUPP school could potentially use it.++

185. How much did JMU spend across all task orders on the previous contract vehicle?

Answer: This information is not readily available.

186. How many task orders were issued on the previous contract vehicle?

Answer: This information is not readily available.

187. What was the work breakdown structure between the 4 incumbents on the previous contract vehicle? Can we see the number of task orders awarded to each contractor?

Answer: This information is not readily available.

188. What is the spending ceiling on the contract vehicle?

Answer: Our current budget is sufficient to support GLBA pen testing, plus 2-5 additional projects per year.

189. Are we required to provide auditing services for all 10 categories, or is it OK to support only a subset?

Answer: No. AMS will contact contractors to submit a proposal for one of the audits when it is on the schedule. It is fine to support a subset of the services.

190. Is certification required for all bidder participants? Can education, training and experience replace certifications?

Answer: Consultants who have staff that possess more certifications will be looked at more favorably.

191. What brand of firewall equipment are you using?

Answer: This will be discussed during planning.

192. What brand of router equipment are you using?

Answer: This will be discussed during planning.

193. Does your Active Directory (AD) consist of on-premise, Azure AD, or some combination?

Answer: This will be discussed during planning.

194. What types of services does Telecommunications entail?

Answer: This will be discussed during planning.

195. With regards to Telecommunications, what sort of audit or IT activity should be expected? Would this be geared as an audit of process and controls, or a technical assessment for vulnerabilities and penetration testing (i.e. war dialing).

Answer: Telecom would focus on the security of the VOIP implementation.

196. C.1.a - C.1.i- What tools and technologies are currently in place for external vulnerability scanning, network assessments, and penetration testing? Are consultants expected to use university-provided tools or supply their own?

Answer: We expect consultants to use their own tools.

197. Page 3, Paragraph #6: Does JMU provide access to system architecture diagrams, configurations, or previous audit reports to inform the current project scope?

Answer: These will be shared during the planning of an engagement.

198. Page 3, Paragraph A: Since JMU follows ISO 27002, how mature is the current implementation of these controls across IT systems? Are there specific areas of non-compliance that require attention?

Answer: The university refrains from answering this question.

199. C.1.a - C.1.i What level of access will consultants be granted during audits (e.g., administrative privileges, network access)?

Answer: Consultants will be given necessary access to system to complete testing.

200. For on-site engagements, what are the physical security requirements and protocols for accessing sensitive areas of the network or facilities?

Answer: This will be determined during planning of an engagement. Consultants, at a minimum, will be escorted to sensitive areas.

201. What level of collaboration is expected between the consultant and JMU's internal IT teams during the project?

Answer: The IT Auditor in AMS manages the audits and will assist consultants during the audit. Arranging the entrance conference for each audit and ensuring consultants have what they need to complete the audit (credentials, etc.).

202. In the event that significant risks or vulnerabilities are identified, how quickly can the IT team allocate resources to address them, and what role will the consultants play in the remediation process?

Answer: IT has the resources to address issues identified during an audit. Consultants should notify IT and AMS as soon as possible of significant risks or vulnerabilities as well as providing a recommendation to address the issue(s).

203. How does JMU's IT team currently track and manage vulnerabilities or remediation tasks? Should the consultants integrate with existing ticketing or reporting systems? No

Answer: Will be discussed during planning for each engagement.

204. Is there a preferred ratio of remote to on-site work for projects, or is this determined on a case-by-case basis?

Answer: This is determined during planning.

205. How frequently will status updates or check-in meetings be required during active audit engagements?

Answer: This is determined during planning.

206. For larger projects, is there a preferred team size, or is it acceptable for a single highly qualified professional to perform the audit?

Answer: These audits can be completed by one person.

207. What is the expected format for audit reports and findings? Does JMU have a preferred reporting template?

Answer: The consultant can utilize their own format. We would like to see the scope, audit approach (methodology), findings and recommendations.

208. Is there an established process for presenting audit findings to executive leadership or stakeholders at JMU?

Answer: Audit reports are presented to the Board of Visitors (Audit, Risk and Compliance Committee)

209. Beyond final reports, are interim reports or preliminary findings required during the audit process?

Answer: No, unless determined otherwise during planning.

210. What is the typical turnaround time for report reviews and feedback after submission?

Answer: Could take up to two weeks for AMS to review reports. Typically, one week.

211. How does JMU prioritize remediation actions following audit findings, and is the consultant involved in verifying that corrective measures are implemented?

Answer: Critical issues are directed to IT immediately after discovery. For these issues, the consultant should work with IT to help address the issue.

212. Specify the VLAN detail; how many are included in the scope?

Answer: This will be determined during planning.

213. Can you please provide the current number of infrastructure details (Physical Server, Virtual Server, Network Devices, etc.)?

Answer: The university refrains from answering this question.

214. How much (%) of the infrastructure is in the cloud?

Answer: In-scope infrastructure location will be discussed during planning.

215. In the IT department/environment, how many employees work?

Answer: Information about the Information Technology Department can be found at https://www.jmu.edu/computing/about/index.shtml

216. Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?

Answer: JMU has multiple server rooms and utilizes some cloud solutions.

Signify receipt of this addendum by initialing *"Addendum #2"* on the signature page of your proposal.

Sincerely,

Doug Chester
Buyer Senior
Phone: 540-568-4272