Addendum No. 1
AHCT Security and Compliance RFP Questions and Answers
November 4, 2019

1. I am hoping you can email me a copy of any specifications and/or documents associated with this project. If they can't be emailed, please let me know. Please do not send them if a fee is required.

   Answer: At this time, due to the sensitivity of the data requested, we will not be able to send detailed documentation to vendors. More detailed discussions will occur during the oral presentation phase of this RFP process.

2. Is it necessary to be on an existing Connecticut state contract to respond to and compete for the business?

   Answer: No, it is no necessary for a vendor to be on Connecticut contract to participate in this RFP.

3. What is the size of the System Security Plan (pages)?

   Answer: Approximately 500 pages

4. What families are included in this first required subset of the three-year cycle?

   Answer: All NIST 800-53 Control families are included in the scope of this 3-year contract

5. Page 6, Project #2, Phase 1: Is this Phase 1 audit for the same application for which the attestation in Project 1 must be conducted?

   Answer: Yes, Project #2, Phase #1 and Project#1 Attestation are for the same application.

6. Page 6, Project #2, Phase 1: What is the size of the CTHIX app?

   Answer: In the last twelve-month AHCT's CTHIX application was used by approximately 732,887 consumers (including Medicaid enrollees) across the state of Connecticut.

7. Page 6, Project #2, Phase 2: What do you see as the differences between Phase 1 and Phase 2?

   Answer: Phase 1 is the application itself while Phase two are those applications that are sources and repositories of data for CTHIX. As an example, our SFTP server is used extensively to support the exchange and sharing to data to and from CTHIX.

8. Page 6, Project #2, Phase 3: What services are provided to you by the Oracle Government Cloud? Is this the hosting site?

   Answer: Our CRM platform is hosted in the Oracle Government Cloud.

Addendum No. 1
AHCT Security and Compliance RFP Questions and Answers
November 4, 2019

9. Page 6, Audit of Third-Party Partners: Are these compliance assessments against processes or is technical testing also needed?

   Answer: These assessments would be a combination of process and technical testing.

10. Page 7, Project #3, Phase 1: What is the size of the Faneuil call center (number of servers, apps, etc.)?

    Answer: Since this is contracted service, we do not have this information. There will be a discovery phase of the workplan that will allow for this information to be disclosed and documented.

11. Page 7, Project #3, Phase 1 and 2: Does Faneuil run both the Virginia and the Connecticut call center?

    Answer: Yes

12. Page 7, Project #3: Do you expect an on-site audit in Virginia?

    Answer: Physical Controls would require actual onsite verification.

13. Page 7, Project #3, Phase 3: What is the size of the custom CRM application to be audited?

    Answer: Since this is contracted service, we do not have this information. There will be a discovery phase of the workplan that will allow for this information to be disclosed and documented.

14. Page 7, Project #4, Phase 1: Where is the Softheon call center located?

    Answer: Stonybrook, NY

15. Page 7, Project #4, Do you expect an on-site audit?

    Answer: Physical Controls would require actual onsite verification.

16. Page 7, Project #4, Phase 1: What is the size of the Softheon call center (number of servers, apps, etc.)?

    Answer: Since this is contracted service, we do not have this information. There will be a discovery phase of the workplan that will allow for this information to be disclosed and documented.

Addendum No. 1
AHCT Security and Compliance RFP Questions and Answers
November 4, 2019

17. Page 7, Project #4, Phase 3: What type of deliverable do you expect from the CRM workflow documentation? Is this the deliverable from Phases 1 and 2?

    Answer: The deliverables should include: (i) a detailed NIST 800-53 Assessment document listing all controls that demonstrate AHCT compliance as well as those controls where we are not compliant; (ii) recommendations on remediation paths and proposed solutions; (iii) a workflow diagram with descriptions of each step; and (iv) a data flow diagram that demonstrates "where" and "how" sensitive and mission critical data is processed.

18. Page 7, Project #4, Phase 3: What is the size of the CRM application to be audited?

    Answer: Since this is contracted service, we do not have this information. There will be a discovery phase of the workplan that will allow for this information to be disclosed and documented.

19. Page 7, Project #5: Where is Scan-Optics located?

    Answer: Manchester, CT

20. Page 7, Project #5: Do you expect an on-site audit?

    Answer: Physical Controls would require actual onsite verification.

21. Page 7, Project #5, Phase 2: How many Scan-Optics applications are used in processing Exchange files?

    Answer: Since this is contracted service, we do not have this information. There will be a discovery phase of the workplan that will allow for this information to be documented.

22. Page 7, Project #5, Phase 2. What is the size of the Scan-Optics applications used in processing Exchange files?

    Answer: Since this is contracted service, we do not have this information. There will be a discovery phase of the workplan that will allow for this information to be disclosed and documented.

23. Page 8, Project #6, Phase 2: What Sir Speedy applications are included in this audit?

    Answer: Since this is contracted service, we do not have this information. There will be a discovery phase of the workplan that will allow for this information to be disclosed and documented

24. Page 8, Project #6, Phase 2: What Sir Speedy location is targeted for the audit?

Answer: Bloomfield, CT

25. Page 8, Project #7, Project Framework Creation, Item 1, Risk Management Framework: Are we comparing the three listed publications to each other, or each to a standard?

    Answer: For clarity purposes and level setting, we are looking for a Program Framework and not a Project Framework. We are comparing the 3 documents for, as an example, but not limited to, overlaps, gaps, unique requirements, etc.

26. Page 8, Project #7, Project Framework Creation, Item 2: What is the work product you are expecting for the Compliance Framework?

    Answer: For clarity purposes and level setting, we are looking for a Program Framework and not a Project Framework. We are expecting the building blocks for building an organization Security and Compliance Program. This would include, but not be limited to, charters, objectives, goals, policies, procedures, workflows, methodology descriptions as well as documented AHCT departmental requirements, etc.

27. Page 8, Project #7, Project Framework Creation, Item 2: What is the work product you are expecting for the Security Framework?

    Answer: For clarity purposes and level setting, we are looking for a Program Framework and not a Project Framework. We are expecting the building blocks for building an organization Security and Compliance Program. This would include, but not be limited to, charters, objectives, goals, policies, procedures, workflows, methodology descriptions as well as documented AHCT departmental requirements, etc.

28. Page 8, Project #7, Project Framework Creation, Item 2: What is the work product you are expecting for the Audit Management Framework?

    Answer: For clarity purposes and level setting, we are looking for a Program Framework and not a Project Framework. We are expecting the building blocks for building an organization Security and Compliance Program. This would include, but not be limited to, charters, objectives, goals, policies, procedures, workflows, methodology descriptions as well as documented AHCT departmental requirements, etc.

29. Page 9, Exchange IT Assets and Security Oversight: Do you want separate deliverables for each of the 4 focus areas?

    Answer: Yes, but also deliverables identifying how each of these depend on each other.

30. Page 9, 2. Identity and Access Management, Item 4, Host and Network Security, Item a: What do you have already documented regarding the current access management process?

Answer: There are architectural diagrams, work flow charts and Access Control policies in place.

31. Page 9, 3. Applications and Database Security, Item a.: What do you mean by "review current capabilities to assess Exchange's application and database security levels"? Are we to assess the security levels or assess your capabilities?

    Answer: We are asking for an assessment of the current security levels in place and our capabilities to support, maintain and enhance, where needed.

32. Page 9, 3. Applications and Database Security, Item b.: Do you have a current network diagram?

    Answer: Yes

33. Page 9, 3. Applications and Database Security, Item b.: Do you want the existing code assessed for its security? If so, how much code is included?

    Answer: Yes, we want the existing code assess for its security. With respect to the second question, more clarification is needed on "How much code is included?"

34. Page 9, 4. Host and Network Security, Item a.: Do we have permission to evaluate the cloud host security "current state"?

    Answer: If awarded your firm is awarded a contract under this RFP, then yes.

35. Page 10, 4. Host and Network Security, Item c.: Is this a penetration test of the entire CTHIX system? If this is the entire system, we need an estimate of the size of the environment for pricing?

    Answer: Production is approximately 100 servers. Including all lower environments, approximately 400 servers

36. Page 10, #5, Item a.: Do you know the size of each of the annual audits?

    Answer: Our audits are based on the NIST 800-53 Control Standards. There are 850+ controls that also need to be reviewed from the CMS MARSE v2.0 as well as the IRS Publication 1075, also subsets of the NIST 800-53 Control standards.

37. Page 10, #5, Item b.: Are there other third-parties besides Faneuil, Softheon, Scan-Optics, and Sir Speedy to be included in the third-party audits?

    Answer: No

Addendum No. 1
AHCT Security and Compliance RFP Questions and Answers
November 4, 2019

38. Page 11, Pricing Proposal: Are you seeking fixed prices or a combination of fixed and hourly? Some of these would be very difficult to establish a fixed price for.

    Answer: We are looking for both approaches. The hourly rates also allow us to look at future ad-hoc requirements as well.

39. Page 13, Submission of Sealed Proposals, 2nd paragraph: Do you require a total of 7 copies plus one original, or a total of 7 copies of the proposal?

    Answer: We require seven (7) copies total. Please be sure to validate (i.e. execute) the Proposal.

40. Page 14, Item III. 2. and Appendix A, page 5, Item 9.c. It is stated on page 14 that we are to include a certificate of insurance within our response, but on page 5 of Appendix A it is stated that the certificates of insurance are to be provided upon execution of the Agreement. Which is correct? Will insurance requirements need to flow-down to subcontractor?

    Answer: We require proof of coverage or the ability to have such coverage by contract execution. This requirement is usually satisfied by including with your Proposal: (i) a certificate of insurance demonstrating the requested coverage amounts; (ii) or providing a letter from your insurance underwriter attesting to such coverage being in place by contract execution. We do not require insurance coverage to flow down to subcontractor as AHCT will not be in privity of contract with any subcontractor, however, that might be prudent from a vendor/subcontractor risk management standpoint.

41. Page 15, Item III. 7: Are we to provide to separate flash drives, one with our technical proposal and one with our cost proposal or may we put both proposals on one flash drive?

    Answer: You can put both Proposal and Pricing Proposal on one flash drive and include it with the Pricing Proposal submission.

42. Page 17, Item IV: Will you accept a separate redacted proposal?

    Answer: We will accept a separate, redacted Proposal along with the unredacted Proposal. Please be sure to provide enough explanation and rationale to justify each claimed exemption consistent with General Statutes § 1-210(b) with your redacted version.

43. Appendix A, page 17, Schedule II, Pricing Proposal: This page is blank – is this intentional?

    Answer: Yes. Appendix A is a preliminary draft of the contract that will be used to engage the selected vendor(s) for the services requested under this RFP. In the final contract, Schedule II – Pricing Proposal will include the selected vendor's Pricing Proposal that was submitted in response to this RFP.

Addendum No. 1
AHCT Security and Compliance RFP Questions and Answers
November 4, 2019

44. What LMS is currently being used for Security and IT training?

    Answer: AHCT's Security and Compliance Department does not currently utilize an LMS. AHCT does license the Noverant LMS for various training activities to meet various State and Federal requirements.

45. What staff are currently in place to support the LMS? What are their respective roles and responsibilities?

    Answer: There are 6 Training Department team members who utilize and support the LMS. The team is comprised of: 1 Manager, 2 Specialists, 2 QA Specialists, and 1 Admin Support.

46. What role does Human Resources have in coordinating and documenting successful completion of required Security and IT training?

    Answer: HR tracks compliance to current Privacy, FTI, PII, HIPAA requirements offered through our LMS or directly from IRS.

47. What training curriculum currently exists for Security and IT training?

    Answer: There is currently no training curriculum available for Security and Compliance, however, AHCT does provide HIPAA and FTI training to all its employees in compliance with State and Federal requirements.

48. What topics are covered for the existing curriculum?

    Answer: See previous question and answer.

49. What areas in the current curriculum need to be expanded and/or upgraded? What are these topic areas?

    Answer: New curriculum needs to be developed as detailed in the RFP.

50. How much time are employees expected spend taking each training module?

    Answer: No more than an hour

51. What level of detail is expected for each training module?

    Answer: The requirements would be defined by the compliance needs that are outlined in NIST 80053, CMS MARSE and IRS Pub1075.

52. What qualifications and level of knowledge do staff have of the subject matter prior to taking the Security and IT training?

Answer: There will be no prerequisites for any of the curriculum offered.

53. What types of users will be taking the training (e.g., end users, administrative users, IT users, etc.)?

    Answer: AHCT currently has 96 FTE's. All FTE's will be required to complete all curriculum.

54. What testing and/or quizzes are conducted to assess staff knowledge and mastery of the proposed subject matter?

    Answer: This is yet to be determined and is part of the scope related to this RFP.

55. What functional groups within Access Health CT will be taking the training?

    Answer: All FTE's within AHCT will be completing Security and Compliance curriculum.

56. How many people in each group will be taking the training, by training module (a-j)?

    Answer: There are a total of 96 FTE's that will be required to complete the curriculum developed as a result of this RFP.

57. What forensic investigation has been conducted to-date at Access Health CT?

    Answer: None to date.

58. Is Access Health CT working with forensic investigators?

    Answer: Not currently.

59. If so, what types of forensic investigations have been conducted or are being planned?

    Answer: See above question and answer.

60. Are their specific techniques that should be covered in the forensic investigation curriculum?

    Answer: This has yet to be determined and is part of the scope of this RFP.

61. What penetration testing has been conducted to-date at Access Health CT?

    Answer: None currently.

62. Is Access Health CT working with an IT team to perform penetration testing?

    Answer: Not currently.

Addendum No. 1
AHCT Security and Compliance RFP Questions and Answers
November 4, 2019

63. Can our team obtain information once an NDA is executed to determine tools, methods, and techniques currently used for penetration testing?

    Answer: Yes.

64. What information will our training development team have access to with respect to specific uses of IT within Access Health that need to be safeguarded and for which training is needed?

    Answer: Access by contracted vendors is limited and on a least privileged policy. Having said this, if access to specific environments are required then applicable roles and access will be granted.

65. What languages, in addition to English, need to be supported by the LMS and used in training modules?

    Answer: Spanish, as needed. This will need to be discussed and agreed upon on a course by course basis.

66. What handicapped/accessibility options are required for training?

    Answer: Classes will be offered through the existing LMS or a contracted service where use of the internet is preferred. The need to access another physical location, other than AHCT, is not preferred as a solution

67. Page 5, Scope of work, Regulatory compliance, Project 1: Are all services required or can a partial list of services be offered?

    Answer: Partial lists of offered services are acceptable.

68. Page 5, Scope of work, Regulatory compliance, Project 1: How much is expected to be conducted on site?

    Answer: Working remotely, where applicable, can be discussed with clear and concise criteria for what is required onsite versus remotely.

69. Page 5, Scope of work, Regulatory compliance, Project 1: Assist with updating and maintaining the following CMS document artifacts, which are required, on a predetermined schedule from CMS. When does current ATC expire for CTHIX?

    Answer: There are several internal activities in the works that impact the delivery of a new ATC. Further discussion is necessary.

70. Page 5, Scope of work, Regulatory compliance, Project 1: Assist with creating and organizing a repository of Security and Compliance related documentation to allow for a more structured

and centralized archive of all related cross-departmental documents. Create or make use of existing retrieval tools used in managing and accessing documentation required by the IRS and HHS/CMS. Now that Medicaid has retired CALT, where does the CTHIX currently store evidence and documents related to maintaining their ATC for CTHIX?

Answer: Our evidence is stored on SharePoint as well as a network shared drive space for redundancy purposes.

71. Page 5, Scope of work, Regulatory compliance, Project 1: Assist with creating and organizing a repository of Security and Compliance related documentation to allow for a more structured and centralized archive of all related cross-departmental documents. Create or make use of existing retrieval tools used in managing and accessing documentation required by the IRS and HHS/CMS. How many individuals (internal and external) have access to the current body of evidence/repository?

    Answer: 5 Individuals

72. Page 5, Scope of work, Regulatory compliance, Project 1. Assist in the analysis and remediation recommendations of Nessus Scan results for the following Department of Social Services (DSS)-hosted and Exchange on-premise platforms. What is the general number of hosts in the (DSS)-hosted and Exchange on-premise platform environment?

    Answer: 100 production servers

73. Page 6, Scope of work, Regulatory compliance, Project 1: Assist with the resolution of open items and preparation of applicable documentation for IRS and CMS:

    Will the awarded vendor be responsible for identifying risks, recommending risk mitigation strategies AND implementing recommendations?

    Answer: The awarded vendors will have the opportunity to offer a proposal to participate in identifying, recommending mitigation strategies as well as implementation solutions.

    What is meant by "assist" in this section? What type of open items are referred to here? (e.g., write policies, respond to findings from IRS, etc.).

    Answer: The reference to “Assist” refers to the awarded vendor working with the AHCT Security and Compliance team to complete needed submissions to CMS and IRS.
    In other words, does the CTHIX require an onsite team (staff augmentation) that is available on an ongoing basis to monitor compliance and mitigate non-compliance over a three-year period? Or would the CTHIX be open to this assistance occurring remotely?

Answer: AHCT is not looking for staff on an ongoing basis. Process, standards, tools, and procedure need to be created and used to perform a onetime audit of the CTHIX application. Ongoing support will be evaluated later, but is not requested as part of this RFP

74. Page 6, Scope of work, Regulatory compliance, Project 2, Audit of Exchange CTHIX Application: How many databases are part of the Audit of Exchange CTHIX Application suite/environment?

    Answer: There is one primary database included in this audit.

75. Page 6, Scope of work, Regulatory compliance, Project 2, Audit of Exchange CTHIX Application: How many web applications (with unique URLs) are part of the Audit of Exchange CTHIX Application suite/environment?

    Answer: There are 3 unique URLs associated with our production CTHIX application.

76. Page 6, Scope of work, Regulatory compliance, Project 2, Audit of Exchange CTHIX Application: Does the CTHIX have a team that is currently conducting network vulnerability scans?

    Answer: Yes

77. Page 6, Scope of work, Regulatory compliance, Project 2, Audit of Exchange CTHIX Application: Does the CTHIX have a team that is currently conducting web application vulnerability scans?

    Answer: Yes

78. Page 6, Scope of work, Regulatory compliance, Project 2, Audit of Exchange CTHIX Application: Does the CTHIX have a team that is currently conducting penetration testing on vulnerabilities identified in scans?

    Answer: No, but the CT Department Administrative Services /Bureau of Enterprise Systems and Technology supports this initiative.

79. Page7, Scope of work, Regulatory compliance, Project 3, Call Center Vendor, Faneuil: Does the current contract language in legal agreements with Faneuil, permit an outside auditor to access/evaluate their network?

    Answer: Yes

80. Page7, Scope of work, Regulatory compliance, Project 4: Does the current contract language in legal agreements with Softheon, permit an outside auditor to access/evaluate their network?

    Answer: Yes

Addendum No. 1
AHCT Security and Compliance RFP Questions and Answers
November 4, 2019

81. Page7, Scope of work, Regulatory compliance, Project 5: Does the current contract language in legal agreements with Scan-Optics, permit an outside auditor to access/evaluate their network?

    Answer: Yes

82. Page7, Scope of work, Regulatory compliance, Project 6: Does the current contract language in legal agreements with Sir-Speedy, permit an outside auditor to access/evaluate their network?

    Answer: Yes

83. Page7, Scope of work, Regulatory compliance, projects 3-6: Are the third-party partners (Faneuil, Softheon, Scan-Optics, Sir Speedy, etc.) considered Business Associates?

    Answer: No

84. Page7, Scope of work, Regulatory compliance, projects 3-6: Are the third-party partners (Faneuil, Softheon, Scan-Optics, Sir Speedy, etc.) required to comply with IRS 1075, HIPAA, or all MARS-e requirements?

    Answer: Yes

85. Page 10, Project 7, Security Operations Center (SOC): Does the CTHIX currently have its own internal SOC or does it utilize a shared (CTHIX wide) SOC?

    Answer: No

86. Page 10, Project 7, Security Operations Center (SOC): Does the CTHIX currently have a documented Incident Response (IR) plan, IR policies, IR procedures?

    Answer: No

87. Page 10, Project 7, Security Operations Center (SOC): What is the CTHIX currently using for a ticketing system (helpdesk system)?

    Answer: Jira

88. Page 10, Project 7, Security Operations Center (SOC): Does the CTHIX currently implement a SIEM and/or collect logs from multiple alert systems (use SPLUNK, SOLARWINDS, CHECKPOINT, etc.)?

    Answer: No

Addendum No. 1
AHCT Security and Compliance RFP Questions and Answers
November 4, 2019

89. Page 10, Project 7, Security Operations Center (SOC): If you answered yes to the previous three questions, are the IR plans, logs and helpdesk ticketing system currently integrated with each other? Or will the awarded vendor be expected to create that integration?

    Answer: The expectation would be to document the plan and requirements for integration once a SOC and SEIM are created.

90. Page 10, SOC: What is the existing SOC capability in CTHIX? Is there a centralized SIEM and a SOC team monitoring it for security events? Please name the existing SIEM solution and the mode of SOC monitoring happening currently.

    Answer: A SOC and SEIM do not currently exist for CTHIX.

91. Page 10, SOC: Is CTHIX open to a Managed Security Service Provider (MSSP) SIEM with Managed SOC services?

    Answer: Yes

92. Page 10, SOC: What is the expected environment coverage - On-premise, Cloud or hybrid?

    Answer: Application Hosted in the CT Data Center

93. Page 10, SOC: What are the cloud environments that are expected to be covered by SOC?

    Answer: Oracle Government Cloud for our CRM

94. Page 10, SOC: What are the number of Data Centers (DCs) and their location?

    Answer: Two (2). The exact locations will be provided once contracts are awarded.

95. Page 10, SOC: What is the total number of log sources in the DCs and in cloud?

    Answer: Approximately 400

96. Page 10, SOC: What is the SOC maturity (low, medium, high) in terms of policies, processes, use-cases etc.?

    Answer: Non-existent

97. Page 10, SOC: What is the level of SOC services required - L1, L2 and/or L3? Does CTHIX have a CSIRT team to handle incidents escalated by SOC team?

    Answer: The SOC does not exist. AHCT expects the selected vendor{s} to participate in its design, which will include recommendations on service levels.

Addendum No. 1
AHCT Security and Compliance RFP Questions and Answers
November 4, 2019

98. Page 9, Identity and Access Management: Do you want the RFP response for IDAM to be restricted to Assessment and Remediation planning exercise which will be followed by proposal for implementation at a later stage?

    Answer: Yes, proposal for implantation should be separate.

99. Page 9, Identity and Access Management: What IDAM services will be in scope for improvement/ transformation? e.g. –
    i. Identity Governance and Administration
    ii. Access Management and SSO
    iii. Privileged Access Management

    Answer: All of the above

100. Page 9, Identity and Access Management: How are you presently managing Access Provisioning and User Lifecycle? Please name the tools being used.

    Answer: IBM SIM/SAM, MS Active Directory and LDAP Services

101. Page 9, Identity and Access Management: Please name if you are using any Access Management tool (WAM, Federation etc.) presently

    Answer: Not presently using any platform other than those mentioned above

102. Page 9, Identity and Access Management: Please name if you are using any Single-Sign-On tool presently.

    Answer: See response in question #100.

103. Page 9, Identity and Access Management: Please name if you are using any Privilege Access Management tool presently.

    Answer: See response in question #100.

104. Page 9, Identity and Access Management: Could you state the business objective this RFP regarding IDAM?

    Answer: Access Control needs to be included in our auditing with recommendations on mitigation and implementation of solutions

105. Page 9, Identity and Access Management: Could you summarize your present pain points/ challenges regarding IDAM?

Answer: Our core application needs an audit, including these controls that will identify exposures. Our pain points are not knowing what we do not know as well as account management not being up to date nor reviewed on a regular basis

Could you summarize your landscape details with respect to the below?

i. How many users?
Answer: Over 200K
ii. Types of users involved?
Answer: Residents f CT, Employees of AHCT as well as Multiple other CT Agencies
iii. How many applications? "
Answer: One core Application, 20+ supporting applications

106. 9-10, Infra sec: Could you please share the inventory of devices in scope with information like make/model, location, active licenses?

Answer: This level of detail will be shared once contracts are awarded.

107. 9-10, Infra sec: Could you please share the ticket data (incidents/change requests/service requests) of last 1 year for devices/services in scope?

Answer: This level of detail will be shared once contracts are awarded.

108. 9-10, Infra sec: Are there any EOL devices? What is the current cycle to refresh EOL devices?

Answer: Yes, but we are currently underway to replace them all by February 2020. There is no approved cycle to refresh/replace EOL devices.

109. 9-10, Infra sec: What is the existing SIEM solution?

Answer: Non-existent

110. Are security tools (firewall, PS/IDS, WAF, AV, EDR etc.) are integrated with SIEM solution?

Answer: See response to question# 109

111. Can Supplier leverage the same?

Answer: See response to question #109

112. 9-10, Infra sec: What is the existing monitoring tool for device health checkup for Network security appliances?

Answer: Device and application health is monitored through New Relics as well as CiscoWorks for Networking.

113. 9-10, Infra sec What is the expected support?

Answer: This section of the RFP is to create a Security and Compliance Program, complete with frameworks to use with Security, IDAM, APP and DBs so that Assets can participate in an oversight solution. AHCT is looking for the creation of these frameworks.

114. Page 8, GRC: Is there any GRC tool being used today for Governance, Risk and Compliance activities? If yes, please share more details about the GRC platform in terms of Information about applications implemented (like Vendor management, Risk management, Audit management, Compliance management etc.).

Answer: AHCT does not presently have a GRC tool.

115. Page 5, GRC: Does AHCT have a consolidated framework already in place with baseline of NIST 800- 53, CMS MARS-E 2.0 and IRS Publication 1075? If yes, when was it last reviewed & updated?

Answer: No

116. Page 5, GRC: What are existing retrieval tools used in managing and accessing documentation required by the IRS and HHS/CMS?

Answer: SharePoint, Jira and FootPrints as well as MS Excel

117. Page 6, GRC: Does AHCT expect service providers to assist with Policies & Procedure Updates? If yes, in what frequency and what is the total number of such policies & procedures in scope?

Answer: Yes, minimally on an annual basis.

118. Page 6, GRC: What is the frequency at which the audit of CTHIX Application and all Supporting Technologies is to be conducted?

Answer: Yearly

119. Page 6, GRC: What is the number of CTHIX Applications and Supporting Technologies to be audited?

Answer: Approximately 25 applications

Addendum No. 1
AHCT Security and Compliance RFP Questions and Answers
November 4, 2019

120. Page 7, GRC**:** What is the mode of audit to be conducted for the call centers and cloud service providers? Is it questionnaire-based vendor self-evaluation, desktop based, on-site assessments?

Answer: All audits will be baselined utilizing NIST 800-53, CMS MARSE and IRS Pub1075.

121. Page 7, GRC: Does AHCT have an audit framework, controls & questionnaire in place adhering to NIST 800- 53, CMS MARS-E 2.0 and IRS Publication 1075 standards? If yes, when was it last reviewed & updated?

Answer: No, this needs to be created as part of the AHCT Security and Compliance Program as detailed in this RFP.

122. Page 8, GRC: Is there an existing framework for Risk Management, Compliance, Security? If yes, when was it last reviewed & updated?

Answer: No, this needs to be created as part of the AHCT Security and Compliance Program

123. Page 9, GRC: Which tool does AHCT use for providing information security awareness training to its Exchange?

Answer: Currently, no formal training curriculum is provided to staff, however, we do provide in person presentations on security awareness, as well as company-wide email communications on the subject, as needed.

124. Page 9, GRC: Does the Exchange have an asset inventory with owners identified?

Answer: This is partially implemented in the AHCT on-premise devices maintained through PDG Inventory. All off-premise systems do not have inventory control systems associated with them. Excel is used as the current solution

125. Page 10, GRC: How many on-going audits are expected to be taken up the service provider at the start of engagement?

Answer: This question requires additional clarity from vendor.

126. Page 10, GRC/VM: How many third-party vendor assessments are expected to be conducted in a year?

Answer: They are listed in Projects 1-6 in the RFP

We presume static and dynamic application security testing are to be included as part of the NIST 800-53 Audit of Exchange CTHIX Application.

Answer: Yes

Please confirm. If yes, please provide he below details about the application.

Answer: The below detail will be provided once awards are given and NDA's are signed

i. Architecture Type (web/mobile/web services/APIs others)
ii. Average size
iii. Type of security testing required viz, Static Application Security Testing (SAST) / Dynamic or Runtime Application Security Testing (DAST) / Application penetration Testing (APT)
iv. Any existing tools that are expected to be leveraged by vendor

127. Page 10, VM: We presume that definition of infra vulnerability management (VM) controls of vulnerability assessments and penetration testing are to be considered as part of the scope for defining the SOC. Please confirm if this understanding is correct. Also, please provide the below details

Answer: The below detail will be provided once contracts are awarded:

i. Number of internal/external devices to be covered by the VM solution
ii. Existing/Preferred/Expected frequency of the vulnerability assessments and penetration tests
iii. Type of VA and PT required, external/internal/authenticated/unauthenticated
iv. Any existing tools that are expected to be leveraged.

128. With regards to the support required for analysis and remediation recommendations of Nessus Scan results, what is the number of servers and other assets that are in the environment?

Answer: Approximately 100 production servers.

129. What is the frequency of generation of:

i. Remediation Reports?
Answer: Monthly

ii. Audit/Assessment Reports?
Answer: None currently.

iii. Policies & Procedures?
Answer: Once policies and procedures are created then yearly review is required.

iv. Contingency Plan?
Answer: Once policies and procedures are created then yearly review is required.

v. Incident Response Plan?
Answer: Once policies and procedures are created then yearly review is required.

vi. Disaster Recovery Plan?

Answer: Once policies and procedures are created then yearly review is required.

vii. Business Continuity Plan?
Answer: Once policies and procedures are created then yearly review is required.

130. What are the GRC tools that currently exist in the environment?

Answer: Non-existent currently

131. With regards to implementing a SOC for the Exchange is there any preference for setting up a shared service or dedicated. Does it need to be in US or offshore is also acceptable?

Answer: Shared Services solutions can be entertained/reviewed. No, offshore is not acceptable.

132. Can you share the volumetric associated with the estate that the SOC needs to monitor?

Answer: A SOC is non-existent currently.

133. Is Access Health looking for the respondent to Price running of the SOC on an ongoing basis, or just design of it?

Answer: AHCT is requesting pricing on both.

134. General: Regarding use of NIST SP 800-53, is the whole set of controls to be used or is it only the ones defined by MARS-E 2.0 and IRS Pub 1075?

Answer: Primarily its CMS MARSE and IRS Pub1075 subsets, but the remaining controls, where applicable, are being requested to be included.

135. Please provide quantifies of each equipment component platform/type for CTHIX, Exchange internal assets, and the vendors' systems for each of the projects to allow us to determine level-of-effort.

Answer: The below detail will be provided once contracts are awarded.

136. Can the work mostly be done at the contractor’s facility?

Answer: The majority of the work is expected to be performed onsite at AHCT.

137. RFP Section 3: For the table's Cost/Rate column pricing, is the amount that we are to add to the table equal to one audit/assessment or total for the three-year contract?

Answer: Please provide separate proposals as well as applicable discounts should the vendor be awarded multiple projects