Addendum No. 2
AHCT Security and Compliance RFP Questions and Answers
November 6, 2019

NIST 800- 53, CMS MARS-E 2.0 and IRS Publication 1075

1. For the POA&M documentation, is the requirement for the vendor to consolidate the actions taken and remediation plans and updates from the various departments and other third-parties?

   Answer: Yes, this is correct.

2. Will the vendor be responsible for annual self-attestation?

   Answer: No, just assistance in completion of the self-attestation. AHCT retains ownership and responsibility for the completed document and submission to CMS.

3. Also, confirm if the State is responsible for the third-party assessment which is the SAR report?

   Answer: Yes, the State of Connecticut is responsible for the SAR.

4. Is the scope restricted to perform the analysis on the Nessus findings or also include assistance with remediation of these findings and taking actions on those remediation items?

   Answer: The scope may include analysis, remediation as well as taking action at AHCT's discretion.

5. What is the frequency at which the Nessus scan are conducted?

   Answer: Monthly and ad-hoc.

6. Please provide an estimate of the number of servers that are included in the scope for Nessus scan results analysis and how many remediation items are expected to be analyzed?

   Answer: Approximately 100 production servers

7. Can you define what is meant by assistance with the resolution of open items? Is this providing advice and recommendations to address the issues only?

   Answer: That is correct. Provide advice, recommendations and documentation updates to capture these outcomes.

Audit CTHIX Application and all Supporting Technologies Project #2: NIST 800-53 Audit of Exchange CTHIX Application

Addendum No. 2
AHCT Security and Compliance RFP Questions and Answers
November 6, 2019

1. Will this be considered an "audit" governed by AICPA standards or an assessment of the CTHIX application governed by CMS MARS E standards?

   Answer: AHCT is expecting a full audit baselined against the NIST 800-53 Controls.

2. Please elaborate if you are looking for 100% testing of all controls (over 350 controls) or is sampling of controls allowed to be used for each control?

   Answer: AHCT is expecting all CMS MARSE controls to be included in this audit.

3. Is the expectation that the vendor will review / audit each and every single server, system, database in scope for the CTHIX application?

   Answer: No, a sampling of the servers is acceptable and will be confirmed through final scope definitions once contracts are awarded.

Audit of Third-Party Partners Project #3 - #6: NIST 800-53 Audit of Exchange's Call Center Vendor, Faneuil, Inc. ("Faneuil")

1. Will AHCT allow a SOC 2 report to be used for the audit? If not, will the vendor have the right to audit the third-party vendor and visit onsite for the "audit"?

   Answer: SOC2 reports are not accepted for the audits specified in this RFP. Yes, access will be arranged with our third party vendors.

Security and Compliance Program Project #7: Assistance with creation of Exchange's Security and Compliance Program.

1. Program Framework Creation baselined to current version of NIST 800-53:

   i. Do you want a gap analysis to be done and know what controls have changed since the last version, or also include the impact analysis with those changed controls conducted for the system and application in scope?

      Answer: AHCT does not have an existing Security and Compliance Program. This framework is in need of being created so that a baseline can be performed.

ii. Please elaborate the objectives of the three frameworks listed in the scope - compliance framework, security framework and audit management framework as part of the risk management framework?

> **Answer:** AHCT is viewing the separate frameworks as building blocks for a successful Security and Compliance Program. The four frameworks listed: Risk, Compliance, Security and Audit Management, have overlap and dependencies. The frameworks should be created separately but clearly show the dependencies and relationships.

2. Documentation Requirements:

i. Please elaborate on the documentation being referred to in this requirement? Please provide details on all the three tasks within this section.

> **Answer:** Documentation refers to policy, procedures, standards and processes required by CMS and IRS to maintain compliance.

3. IT Security Training:

i. Is the source material required for developing the training content available with AHCT? How does AHCT envision the training content format to be prepared - PowerPoint based training or Computer Based Training with certification and tracking, and involves interactive scenario-based training?

> **Answer:** Security Awareness training does not exist and would need to be developed or made available via services offered by a third party vendor.

4. Exchange IT Assets and Security Oversight.

i. Does the scope for this requirement involve providing security oversight (some other third party is performing the tasks) or actually performing these tasks?

> **Answer:** Since AHCT does not have a Security and Compliance Program we are expecting analysis, recommendations and documentation that will be used to take action. These actions will be defined after a Security and Compliance framework is created and approved by AHCT senior leadership.

ii. How are the tasks mentioned in this section different than the previous three frameworks mentioned in section "Program Framework Creation baselined to current version of NIST 800-53?”

> **Answer:** This section will be more detailed and specific to areas such as tools, staffing, reporting, etc.

iii. Is the vendor expected to run the security scans such as penetration testing? If yes, then what is the scope of penetration testing - web application scan or network scan? Please indicate number of IPs and address ranges etc.

Answer: Web application penetration testing is the only in scope requirement.

iv. Does the scope involve implementing the enhancements identified in the assessment or only restricted to provide recommendations?

Answer: The scope may include implementation but initially only requires recommendations. AHCT will assess and take action upon AHCT senior leadership direction and approval.