

Information Security Risk Assessment RFO # SD15-00035

Questions and Answers

1. In Exhibit A – Statement of Work, Section A – Scope of Services, CCHCS lists twelve information systems to be assessed as part of this project. Assuming that all listed systems will be included as part of the enterprise security assessment, are results of the assessment expected to be reported from the overall enterprise perspective or from the perspective of each of the individual systems? We assume the former (they are to be included as part of the enterprise security assessment), but we would like to verify that assumption.

Answer: We would expect the recommendations to be individual for each information system. We would welcome a “top 5” or other means of overall enterprise prioritization based on vendor’s expertise.

2. We have one additional question about this RFO. Under Documents Required Upon Submission of Offer (RFO page 3), item E requests a “copy of valid business license.” Can CCHCS please clarify what documents they are expecting for this submittal?

Answer: A valid business license that demonstrates eligibility to do business in California.

3. Please clarify that you are only looking for a risk assessment related to the HIPAA Security Rule and that you are not looking for an assessment of compliance to the HIPAA Privacy Rule as part of this assessment.

Answer: Risk Assessment will need to be based on the requirements set forth in the Security Rule and will focus on the Security Rule, not the Privacy Rule.

4. NIST SP 800-66 An Introductory Resource for Implementing the HIPAA Security Rule provides guidance for federal facilities in performing HIPAA Risk Assessments and cross references to the requisite controls from NIST SP 800-53 R4 Security and Privacy Controls for Federal Information Systems and Organizations; is it acceptable to follow the guidance provided by NIST SP 800-66 in performing this Risk assessment?

Answer: Yes, it is acceptable and welcomed. Of course, this only addresses the Security Rule of HIPAA. We have also asked to align with 800-53 r4 Moderate controls, so they will need to be cross walked.

5. Does the California Department of Correction and Rehabilitations have ePHI Data Flow diagrams for all in scope systems that can be provided to the successful bidder?

Answer: No, not all systems have a DFD.

6. Are there any trusted network connections in scope for this assessment that belong to third parties?

Answer: The EMR is hosted and has a specific dedicated circuit.

7. Is the technical control testing mandatory or can the effort exclude the technical control testing?

Answer: Yes, the controls should be tested to assure CCHCS of their effectiveness.

8. How many employees are in your organization?

Answer: About 16,000.



Information Security Risk Assessment RFO # SD15-00035

Questions and Answers

9. Is Information Security a centralized function?

Answer: The Information Security Office is centralized, but some IT areas have some security management functions which are decentralized.

10. Are there multiple business units that have their own IT Governance and/or Information Security groups? If yes, please list them here.

Answer: No, IT governance resides in IT.

11. Is there a written security policy available? (If yes, please complete the next two questions)

Answer: Yes, some policies exist and some procedures exist.

12. Please describe the current Information Security Policies. Is there one set of policies, and what is the approximate size? (total number of documents and approximate page count)

Answer: CDCR has the Department Operating Manual and CCHCS has its own set of policies. We currently have about five InfoSec CCHCS specific policies.

13. Are the policies mapped to any particular control requirements such as ISO 27001/27002, HIPAA, PCI or others?

Answer: HIPAA, SAM and NIST.

14. Is the desired assessment focused on a centralized set of controls (i.e. an "Information Security Program"), or disparate controls across multiple systems and infrastructure?

Answer: Some functions are centralized, such as directory authentication, while others are decentralized. Many controls will need to be system specific.

15. How many business processes would be in scope for the desired assessment?

Answer: No specific number exists, but they will be inclusive to the information system itself.

16. Please list the business units, business processes, and any relevant sub-processes:

Answer: There are 12 systems being assessed, we do not have specific processes and business units identified. There is a various amount of business units that traverse the systems

17. What is the current maturity level of the centralized Information Security Program?

Answer: The maturity level is not a metric we currently have available based on any industry standards.



Information Security Risk Assessment RFO # SD15-00035

Questions and Answers

18. Please describe the job functions of the individuals who would need to be interviewed for the purpose of this assessment to understand the current controls within the Information Security Program and infrastructure. (ie. IT, Compliance, Legal, HR, Business Data Owners).

Answer: Roles include infrastructure manages and staff (network, server directory services, security operations), business owners (HIM, radiology, dental, quality management, utilization management). Application Dev teams (managers and staff)

19. What control areas should be in scope for this assessment?

Answer: Please refer to the RFO. Moderate controls 800-53

20. How many physical sites are in scope? Please list at a minimum, data centers and locations for interviews:

Answer: Interviews will be in headquarters and data center (two sites in the Sacramento area)

21. Does your company have a risk management department?

Answer: There is a risk management department under the legal team.

22. Has your company conducted a Business Impact Analysis (BIA) or some other activity to determine the value of IT assets?

Answer: There is a BIA completed, but not a fully robust process

23. Are there any specific areas of the framework controls that deserve more focus than others? If so, please describe:

Answer: We are looking for the supplier to address this based on risk assessment.

24. What is the System Categorization (SC) level as determined through the FIPS-199 process?

Answer: We have not done an SC based on FIPS, so we have selected Moderate controls based on NIST guidelines (800-60)

25. Has the SC been accepted by the project sponsor?

Answer: N/A

26. Has a System Security Plan (SSP) been developed and base lined for each system that falls within the defined scope of the FISMA certification effort?

Answer: No

27. Please provide a copy of the system scoping section from the SSP here:

Answer: N/A



Information Security Risk Assessment RFO # SD15-00035

Questions and Answers

28. What is the current state of the system?

Answer: N/A

29. Is Access Control Management for in-scope systems managed centrally?

Answer: Since most systems use centralized authentication, only information system specific authentication will be included

30. If not, how many different individuals would need to be involved in the review in order to understand controls around assigning access control for network, system, and security administration?

Answer: N/A based on supplier experience. Most systems are centralized auth

31. Approximately how many individuals would need to be interviewed to review the NIST SP800-53 controls for in-scope systems? Please consider individuals from the business as well as from IT / Information Security.

Answer: 20 – 30 CCHCS individuals could be interviewed based on the scope of the systems

32. Will the assessment be performed with or without assurance controls?

Answer: No assurance/attestation will be required. This is an independent assessment. If you need clarity, please give specific examples of what you are defining as controls assurance.

33. Is there any incumbent currently providing the concerned Information Security Risk Assessment to CCHCS? If yes, what is the name of the incumbent firm is it allowed to participate in this bid process?

Answer: There is not incumbent nor do we have a standing contract.

34. Does CCHCS has any preference for certified Minority-Owned Business Enterprise /Women-Owned Business Enterprise?

Answer: The RFO process does not identify any available preferences.

35. Can the City-State provide editable copies of the attachments deemed to be produced in the proposal?

Answer: No editable documents will be provided for this RFO.

36. We understand that the “Estimated Number of Hours” for the consultant against each of the deliverables and associated sub-deliverables has to be provided based on the experience with similar projects and considering standard assumptions for the engagement. Please confirm.

Answer: Yes this is correct.



Information Security Risk Assessment RFO # SD15-00035

Questions and Answers

37. Will you be accepting H1 candidates?

Answer: Please refer to the RFO and CMAS contract for any applicable requirements.

38. How many candidates/resumes we can submit for this opportunity?

Answer: The number is the decision the Offeror deems best for the proposal/engagement.

39. Work samples are required from the Candidate or the Offeror?

Answer: Offeror

40. We understand that at least two (2) customer references are required for each of the proposed Contractor personnel, do we also need to provide Offeror references too? If yes, how many?

Answer: The RFO requires two (2) references for each proposed personnel (candidate), not the Contractor/Offeror (your company).

41. Can we have staff references serve as the Offeror references?

Answer: The RFO only requires references from the candidates not the Offeror.

42. We request CCHCS to extend the RFO Offer Submission due date to allow vendors to submit a comprehensive proposal along with best of the candidates' post receiving the clarifications.

Answer: Please see Addendum 1

43. How many consultants CCHCS desires to on-board for the concerned risk assessment engagement?

Answer: Offeror's decision to propose the best number of consultants based on their experience for a similarly sized engagement.

44. Will CCHCS assign a project manager for managing the Offeror resources?

Answer: No, the vendor will be responsible for the overall engagement. CCHCS has the right to assign a PM to keep the internal interviews and tasks in line with expectations.

45. Is it necessary for the Offeror to have prior experience providing Risk Assessment services to participate in this RFO?

Answer: Yes, please see the requirements within the RFO.

