RETIREMENT SYSTEMS OF ALABAMA
SOC 2 REPORT PROPOSAL
RFP 020 20*00008
Proposer Questions Log

1. To confirm: the only data center in-scope for this project is the ASA data center in Huntsville, Alabama?
   Yes

2. Regarding Section I.A of the RFP: Please clarify why the first year contract will be with the RSA and subsequent years' contracting will be with the ASA.
   Yes, there will be one contract with RSA for the SOC 2 Type 1 engagement. There will be another contract with ASA for the SOC 2 Type 2 engagements for 2022-2024.

3. Has ASA and RSA management identified and mapped current controls in place to satisfy the SOC 2 trust services criteria relevant to security, availability, and confidentiality? No Additionally, will the ASA and RSA be responsible for preparing the description of the system and identifying any user and sub-service organizational control considerations? ASA will prepare description.

4. Does the ASA have a due date for the delivery of the final SOC 2 reports? For the December 31, 2020 for SOC 2 Type 1, the delivery date is no later than February 28, 2021.

5. Does ASA management anticipate documenting their own Section 3 - Description of the System, or would ASA management prefer the audit partner to write the section for ASA management's review? ASA will document the description of the system.

6. Would ASA management prefer work to be completed remotely or on-site? Is management open to a hybrid approach? ASA is open to a hybrid approach.

7. Does ASA management currently have a system in place for the sharing of secured documents that it prefers be utilized for the sharing of information? Yes

8. Has ASA management identified the key contact that would function as the project manager for the SOC services? Yes, Debra Wallace of ASA.

9. Does ASA management anticipate that other current or potential clients will request the SOC 2 report? Yes, but RSA only the first year.

10. Does the RSA require the ASA to be SOC 2 Certified? Yes

11. Will the ASA provide any type of hands-on services to the RSA, or is all RSA system monitoring done by the RSA? Provide colocation services only.

12. To confirm, is the ASA hosted at the RSA strictly a back-up system? Yes

13. Is the ASA considered a hot-site (real-time replication)? Yes

14. Is the ASA taking back-ups of the RSA system as well? Or is that the responsibility of the RSA? The responsibility of RSA.

15. Is the scope of the SOC 2 just related to services completed for the RSA, or for the entire ASA data center and operations? First year for RSA, subsequent years will be worked out with ASA.

16. Are any other types of audits completed (such as ISO)? ASA procures a third party network security assessment every two years.

17. Are policies/procedures in place? Yes Has a readiness assessment been completed? No

18. How does the ASA feel they would do in the SOC 2 examination without first completing a readiness assessment? ASA is confident in their facility and operations.

19. For those on the June 4th call that may have worked with auditors in the past, what did you feel worked best, and what didn't work well, during the process to complete the project engagement?

    RSA: ensuring data that is turned over to the auditors is thoroughly reviewed which may contain key information and reduce further questioning.

20. To help adhere to widespread social distancing/stay-at-home orders and ensure the safety of both our firm's staff and the RSA's staff in regards to COVID-19, will

the RSA accept proposals that are submitted electronically by email, and thus waive the hardcopy and CD proposal response requirements?

Please provide responses as stated in the RFP.

21. In regards to Section IV of the RFP (Additional Documents), where in our proposal would the RSA like us to include these additional documents? In an appendix?

    In an appendix.

22. Do you have an established budget or a not to exceed threshold for this project? If yes, please provide detail.
    Give us your best proposal.

23. There are two similar RFPs listed in STAARS:
    a. Your RFP (RFP 020 20000000008) for SOC 2 Type 1 Services at Huntsville Data Center, due on 7/20/20 2:00 PM CDT.
    b. RFP 091 20000000001 for a SOC 2 Audit (related to the ASA), due on 7/20/20 3:00 AM CDT.

    Are these two unique bidding opportunities, or is RFP 091 20000000001 redundant with RFP 020 20000000008? These are redundant.

24. Does the cost & price analysis section have to be in a separate envelope or as part of the proposals, or both?
    Separate Envelope.

25. Will the SOC 2 Type 1 and subsequent Type 2 reports be intended to meet the needs of a broad range of user entities or will it be used exclusively for RSA?
    First year for RSA, subsequent years will be worked out with ASA.

26. Are you interested in a readiness review / health check to identify SOC 2 control gaps prior to commencing the SOC 2 Type 1 examination? No

27. Will there be one primary point of contact to facilitate meeting and documentation requests? Yes, Debra Wallace of ASA.

28. Approximately, how many IT and Operations personnel support controls of the Huntsville Data Center? 50 – 55 staff members

29. Has a draft of the system description (Section III of the SOC 2 report) and related control activities that meet the SOC 2 trust services criteria been documented? No

a. If yes, how many total control activities were identified?

b. If not, does management plan to document the system description and related controls, or will assistance be required by the chosen provider? ASA will document.

How well defined and documented are the current policies, procedures, and processes? ASA will document before audit begins.

30. Are there any key processes/services outsourced to a third-party (subservice organization) that would be relevant to the scope? No, ASA has a professional services contractor that is housed in the facility and handles all operations. If so, list the third-party service provider, function performed and whether they will be scoped in or carved out of the SOC report (example: security information and event monitoring is outsourced to a third-party security operations center as a service vendor):

Third Party Provider/Vendor	Function outsourced	Carve-out or In-scope

31. Are there any “internal” sub-service organizations used by the company that has a SOC report which can be referred to for this report? (internal departments/subsidiaries performing services relevant to the scope such as a centralized IT SOC report)? No

32. Are the IT controls & related policies & procedures for the systems listed above managed centrally (i.e. applicable to all systems) or decentralized (i.e. application specific)? Managed centrally.

33. Are there any known problems with the in-scope services or controls? No

34. How similar are the policies/procedures/controls between RSA and ASA since they are both government entities within the State of Alabama? Essentially, Do RSA and ASA share any controls, or are they fully independent organizations?

    Both RSA and ASA operate independently.

35. Will the scope include just colocation services or other managed services (backups for example)? If services beyond colocation services are to be included within the scope of the SOC 2 examination, please detail those services.

    First year is for RSA to cover confidentiality, security, and availability of colocation services. Subsequent years may cover processing integrity and privacy should be priced separately.

36. Please confirm there is only one (1) physical data center location in Huntsville, Alabama within the scope of the SOC 2 examination. If there is more than one, please provide details.

    There is one datacenter and it is in Huntsville, AL.

37. The ASA website indicates the organization has undertaken a NIST 800-171 gap assessment. Has ASA completed the implementation of the controls for the NITS 800-171 framework and completed a self-attestation questionnaire?

    ASA is working to becoming NIST 800-171 compliant.

38. Page 7: Will RSA and ASA require all auditors to sign an NDA directly, or will they be covered by the NDA within the contract, and between the vendor and employee?

    As part of the awarded contract, an inclusive NDA will be signed.

39. IT Risk is listed as a Selection Criteria. Please describe the criteria by which RFP submissions and potential vendors will be evaluated for IT Risk.

    Overall IT risk of the potential vendor's response to the RFP.

40. What is the total number of employees in the company? 50-55

41. What is the total number of IT employees? 50-55

42. Which SOC 2 Trust Service Principles do you wish to assert in addition to the required Security Principle? (Processing Integrity, Availability, Confidentiality, and/or Privacy)

First year is for RSA to cover confidentiality, security, and availability of colocation services. Subsequent years may cover processing integrity and privacy should be priced separately.

43. Are you seeking a Type 1 (point-in-time report on control design) or a Type 2 (period of time, typically 6 to 12 months, test of control operating effectiveness) report? T
Type 1 for the period ending December 31, 2020, subsequent years ending December 31st would be a Type 2.

44. Please describe the applications in-scope for the SOC2. Year one, RSA's colocation. Years two through five, ASA may possibly add other applications, but less than ten.

45. Describe how each of the applications listed in the previous question are architected. The intent of the question is to gauge the size and complexity of the applications in question. See answer above

46. Is a directory services application in use (e.g. Active Directory, Novell, etc.)? If so, what is the total number of users on the Domain? Active Directory

47. How many total internal IPs are used? 60-65

48. How many total external IPs are used? Can be provided at a later time.

49. Please briefly describe the future direction of IT within the organization. List any plans to upgrade or replace existing hardware or software. List major system upgrades or data conversions in the last 12 months.

ASA works with educational entities in the state along with other State agencies. No plans to change this direction in the future

50. Do you have an information security policy? How often is it reviewed and updated? ASA is working on documentation.

51. Do you process or store personally identifiable information or electronic personal health information? No

52. Are there any significant problems or deficiencies in the functionality provided by the systems? No If so, please list what work-around procedures are in place.

53. Are there significant IT activities outside the IT function? No Is use made of outsourced service providers? If so, identify what key components have been outsourced.

54. In the last 12 months, have there been any significant operational failures, security incidents, data breaches, or data corruption problems? If so, please describe the management's response to the issues and how the management got comfort over the solution. No

55. Please briefly describe how PCs and servers are backed up, the backup solution, and backup frequency (incl. daily, weekly, monthly, and offsite storage)

    This will be covered during the engagement.

56. Please list any tools that are used for monitoring logical security, including any intrusion prevention or detection systems (IPS/IDS).

    This will be covered during the engagement.

57. What other regulatory and/or compliance frameworks are you subject to? E.g. Sarbanes-Oxley, ISO 27001, etc.

    Sarbanes-Oxley and ISO 27001 do not apply.

58. Because the SOC 2 Type 1 report is as of a point in time, is it important that the actual point in time be 12/31/20, or is 12/31/20 the last date for the point in time and the actual as of date could be prior to 12/31/20?

    Field work may start once the contract has been awarded and agreed upon with ASA. If fieldwork is complete prior to 12/31/2020, then you can issue the Type 1 report. Subsequent reports should cover the entire 12 month period from the date of the Type 1 report for the next 12 months, and so on.

    .

59. Is ASA open to a segmented examination, some work performed prior to 12/31 and some work performed at/subsequent to 12/31?

Field work may start once the contract has been awarded and agreed upon with ASA.

60. Has the ASA documented its controls to meet the applicable trust services criteria for the principles of security, availability and confidentiality? No If not, is the ASA looking to have the CPA firm assist in documenting those controls? ASA will document.

61. Since this is the first SOC examination at ASA, is it preferred to have a preliminary review of existing controls designed to meet the trust services criteria and then allow ASA time to remediate any issues before the SOC 2 Type 1 examination is performed. A preliminary review would be preferred.

62. What is the reason RSA is contracting for the Type 1 and ASA is contracting for the Type 2 examinations.

RSA has agreed as a joint partnership to pay for the first year SOC 2 Type 1, subsequent years will be paid for by ASA.

63. Are there any subservice organizations used by ASA. No If so, please describe. If there are subservice organizations, is it the intent to have the subservice organizations reported under the inclusive or carve-out method?

64. In Section 1.L, Minimum Qualifications, can the Audit Manager/Partner have a CPA certification in lieu of a CISA with requisite experience since a CPA is required in order to sign the opinion? ASA will allow. There would be CISAs on the team but would like the Partner to be a CPA.

65. The above RFP requirement indicates that either the Audit Manager or Audit Partner must have a CISA designation. Will RSA be the sole user entity of the report, or will ASA provide the report to other clients.

The SOC 2 Type 1 will be issued to RSA the first year. Additional users may be added after year one but would be less than ten.

66. Will all work be performed at the Huntsville location? What are the services that are performed out of the Montgomery location?

No services related to this RFP will be performed in Montgomery.

67. How many employees at ASA? 50-55 Can we receive an organizational chart?

68. Just to get a sense of the organization's plans over the next 5 years (term of contract), are there any planned changes in management, platforms, locations, etc. No significant changes are anticipated.

69. How will travel cost be handled?

    Travel is to be included in the fixed price contract and is not a separate amount payable under this contract.

70. We would like to know more on the scope of the SOC 2 Audit as to the specific environment, the exact period of report, 6 months or 12 months, which of the Trust Service Criteria are in scope?

    The SOC 2 Type I Report must be completed with an opinion issued by February 28, 2021. The SOC 2 Type 2 Reports must be completed and opinion issued by February 28 of each subsequent year.

    The results of this RFP will be two contracts: one with RSA for the December 31, 2020 SOC 2 Type 1 report and one with ASA for the SOC 2 Type 2 reports for the twelve month periods ending December 31, 2021, 2022, 2023 and 2024.

    This Request For Proposals (RFP) solicits vendor proposals for Service Organization Controls 2 (SOC 2) reporting services on the Alabama Supercomputer Authority's (ASA) description and the suitability of the design and operating effectiveness of the controls in place at the Huntsville, Alabama data center of the Alabama Supercomputer Authority as of December 31, 2020, in accordance with attestation standards applicable to SOC 2 reporting established by the American Institute of Certified Public Accountants for the trust principles security, availability, and confidentiality.

71. How is the IT department structured? ASA has 50-55 staff in the Huntsville Center. Can you please provide an organization chart with roles and responsibilities? Yes, will be provided during the audit.

72. Can an inventory or count of the applications, software, databases, and hardware be shared? Year one, RSA's colocation requirements. Years two through five, ASA may possibly add other applications, but would be less than ten.

73. What are the most valuable data and mission-critical systems at the organization? ASA works with educational entities in the state along with other State agencies.

74. Are there any significant outsourced IT service providers? No If so, can you please provide a list of service providers?

75. Are you utilizing any cloud services, and will they be part of the SOC 2 report? No

76. What information technology control framework (NIST 800-53, NIST CSF, ISO 27001, COBIT, CIS CSC, etc.) has been adopted or internally developed? ASA is working to becoming NIST 800-171 compliant.

77. Have you had any other IT assessments or audits conducted (internally or by external service providers)? ASA procures a third party network security assessment every two years. If so, can you please share the reports? Yes, will be provided during the audit.

78. Have you performed a SOC 2 Type 1 or Type 2 report(s) for the ASA? No If yes, was it aligned with the 2017 Trust Service Criteria (TSC)?

79. Have you performed a SOC 2 Readiness Assessment for the RSA, and is it aligned with the 2017 Trust Service Criteria (TSC)? No

80. Are controls for the RSA or ASA aligned, or are they different? Both RSA and ASA operate independently. Are the control owners or those responsible for the execution of the same between RSA and ASA? No

81. What IT & Security policies and procedures have you established? ASA has policies and procedures in place and updated documentation will be provided. How often do you perform the review of the policies and procedures? In Progress.

82. Do you have documented service commitments and system requirements of the system and the risk related to achieving those commitments? Yes Are updates or modifications to service commitments and system requirements incorporated into the risk assessment and review process? Yes

83. Regarding Item 7 (Indemnification) in the Sample Agreement to Provide Professional Services (on page 20 of the RFP): AICPA guidelines prohibit accounting firms from indemnifying attest clients from damages, losses or costs that relate, directly or indirectly, to an attest client's acts. Given this prohibition, would the RSA/ASA consider modifying the pro forma indemnification language contained in the sample professional services agreement?

RSA will take any proposed edits to the standard contract language under consideration as part of the RFP process. Any edits to be requested must be included as part of your proposal.

84. Regarding Item 15 (Termination for Default) in the Sample Agreement to Provide Professional Services (on page 21 of the RFP): This clause does not include a notice before termination for default. Will the RSA/ASA add language to this section stating that it shall provide the Contractor with written notice of the reason for such termination and give the Contractor a time period (e.g. 15 business days) to cure or rectify the issue from receipt of such notice before the agreement is terminated?

    RSA will take any proposed edits to the standard contract language under consideration as part of the RFP process. Any edits to be requested must be included as part of your proposal.

85. How will travel cost be handled?

    Travel is to be included in the fixed price contract and is not a separate amount payable under this contract.