NASWA
NATIONAL ASSOCIATION OF STATE WORKFORCE AGENCIES

LIMITED COMPETITION RFP

Request for Proposal:

State Information Data Exchange System (SIDES) Security Audit

Responses to Questions from Bidders

August 28, 2018

Questions and Answers, answer beneath each question in **bold.**

1. The RFP includes the phrase Risk Assessment Report (RAR) which in the FedRAMP and FISMA space RAR is an acronym for Readiness Assessment Report (RAR). The RFP includes the phrase SCA (Security Control Assessment) Report which in the FedRAMP and FISMA space is referred to as the Security Assessment Report (SAR). As they pertain to your NIST 800-53 assessment, are these titles and acronyms we need to work around or will the RFP be amended?

   We would like to keep the RAR and SCA definitions as in the RFP. FedRAMP terms are not applicable as this is not a cloud environment.

   However, where the acronym CSA is used in the RFP, this should be 'Security Control Assessment (SCA) Report'.

2. Section C. Pricing – It's indicted this is a Firm Fixed Price engagement, but then directs the vendor to break down details regarding staff, roles, hourly rates, direct costs, etc. for each deliverable. I've counted at least 10 total deliverables as part of the RFP; providing this level of detail on a response is greater than we've seen on similar RFPs. Will you accept a single table for the entire engagement which outlines the staff roles utilized, staff rates, staff hours by role?

   Yes.

3. Reference page 14 “Proposal Section Number 5 “Cost Estimate” that states, “Pricing shall include a detailed buildup of Labor costs, Other Direct Costs, and Fees”. Also reference page 17 that states, “The cost estimate should include a full buildup of costs and rates used to establish the FFP cost estimate.” Will a basis of estimate (number of hours, labor category, fixed price labor rate, other direct costs, and profit) meet the requirement? Given this is a fixed price, competitive procurement, a fair and reasonable pricing determination can be made by a comparison of proposed prices received in response to this solicitation.

   Yes

4. Project Plan, Key Personnel and Resume. The request for detailed work history, experience and educational history is significant, but reasonable. Can you clarify “are required to pass a background check”? Also, the request for college transcripts for authentication of awarded degree is greater detail requested when compared to similar RFPs; are you flexible on this, and if not, please explain the justification.

   Only upon request by NASWA.

   Only before contract award.

5. Is there a possibility to push back the due date for proposal submission 1-2 weeks due to the college transcript requirement? Most universities take 5-10 business days to process and mail back to the alumni.

   September 10, 2018 by 5:00 PM ET to rfp_responses@itsc.org.

6. We would be delighted to provide a proposal for your requirements and thank you for reaching out to us. As a 3PAO (among many other things) we are indeed well suited for your NIST 800-53 requirements. After reading the full requirements certain contract items such as an audit of our financials would be objectionable. Also, some of our larger customers such as Conduent and Cisco Systems forbid their employees from providing references which may cause issues. If there is flexibility in your contract terms, we would be happy to supply a proposal. If those terms are not negotiable, we will respectfully decline the invitation.

   Any exceptions will be highlighted need to be clearly denoted, and will be addressed as of the evaluation process.

7. Reference Project Plan, paragraph a) – “Key Personnel and Resumes”. Does NASWA require the items listed in paragraph a) for all personnel that will perform under the contract or only the proposed key personnel?

   The vendor shall submit a resume for the Key Personnel who is being proposed as a part of this RFP response.

8. Reference page 9 that states that one (1) Key Full Time Equivalent (FTE) is required for this project. Is a full-time key person required during the entire period of performance of the anticipated contract or only during the audit period?

   FTE is only needed during the Audit itself, including the report generation and the POAM follow up, including the RAR generation.

9. Reference page 22, paragraph 6. "Audit" and Subpart F of 2 CFR 200 "Audit Requirements". We understand the requirement applies when the non-federal entity expends $750,000 or more during a fiscal year. Does the basis for determining federal awards expended apply to all federal government contracts or only grants, cooperative agreements, and cost reimbursement contracts? Does Subpart F apply to this anticipated fixed price contract?

   Does not apply as this is not a Federal contract. SIDES is not considered a Federal Government system. It is governed by representatives from state unemployment insurance agencies, employers, and third-party agencies. The system is state funded through the redirection of state unemployment insurance administrative funding to NASWA.

10. Reference 2 CFR 200.101 "Applicability", that states Subpart E "Cost Principles" does not apply to fixed amount awards. In subparagraph (2) it states that Subpart E applies to Federal award cost-reimbursement contracts. Please clarify whether or not Subpart E of 2 CFR 200 applies to this anticipated fixed price contract.

    Does not apply as this is a fixed price contract.

11. Developing a Plan of Action and Milestones is listed as vendor responsibility. Plans for remediation require the NASWA/Hosting resources to determine timelines and agreed upon activities for a complete POAM. While vendor can support the development of the POAM, it is our recommendation that this task be listed as shared responsibility amongst the vendor/NASWA and cloud infrastructure vendor(s)

    Vendors are requested to provide candidate POAMs which will be subject to review and approval/acceptance by NASWA.

12. Similarly, developing remediation strategies cannot be the audit vendor's responsibility given that these decisions are handled by the NASWA. Vendor can support the strategy and provide recommendations, however the strategy for remediation must be the responsibility of NASWA.

    Vendors are requested to recommend remediation strategies will be subject to review and approval/acceptance by NASWA.

13. We recommend that Task D precede Task C, POAM development requires risks to be documented and NASWA to be briefed and approve of the risk determination before a plan of action can be developed.

    Intent is for Vendor, NASWA and hosting vendor to work collaboratively on the POAMS as part of Task C, during which risks will be discussed. Task D is intended to be the final briefing, prior to start of remediation phase.

14. Reference Security Audit Requirements, Activities/Tasks: C – "Develop Candidate POAMs", E – "POAM Approval, Remediation and Security Plan Update", and F – "POAM Update Review". Does the National Association of State Workforce Agencies (NASWA) require the contractor to develop Plan of Action and Milestones (POA&Ms); or only review, test and provide feedback on existing POA&Ms? What is the expected level of effort for these tasks? What level of effort does NASWA anticipate being needed after conclusion of the assessment for ongoing contractor assistance with POA&M creation, remediation, tracking, and closure?

    For Task C it is expected that the contractor will enumerate the deficiencies found in the audit, consolidate any similar deficiencies where a common solution may be applied, develop recommendations(s) for remediation and provide a high-level prioritization identifying the most critical problems. During this period there will be communication with the NASWA and the Hosting, but the assessor has primary responsibility for this activity.

    For Task E, it is the customer responsibility for final decisions on what POAMs to address and the time frame for remediation, considering cost and other resources. During this period the customer will finalize the POAM selection, initiate remediation efforts, track these efforts and close the POAM when remediation is complete. The Security Plan will be updated by the customer to reflect POAM closure. Customer decisions in this area will be made available to the vendor at least 1 month (TBD) prior to the start of Task F.

    Task F calls for the assessor to determine how effective and complete the remediation efforts have been with respect to POAMS developed as a result of the initial assessment.

15. Is this a full SA&A with the objective of renewing the ATO every 3 years? What date is the ATO for SIDES and its' expiration?

    The scope of this RFP is to conduct an audit of standard controls defined by NIST800-53 for a Moderate system in order to obtain authority to operate per the SIDES Director. Future audits will be performed to continue retention of the authority to operate per the SIDES Director.

16. What organization is the Authorizing Agency for this NASWA/CESER Audit?

    NASWA

17. Who is the authorization authority?

    SIDES Director

18. Are there any requirements based on DOL or State of MD that SIDES need to comply with as part of this Audit, such as policies and procedures?

    The requirements are the NIST controls described in the RFP.

19. Can we use NASWA's existing licenses to perform security risk assessment (like vulnerability testing)?

    It is acceptable to audit vulnerability scans performed by hosting vendor, so no additional licenses are required.

    Vulnerability scans are performed on a regular schedule by the hosting vendor and in compliance with the NIST guidelines. It is acceptable for the auditing vendor to review the associated work instructions and the documentation of regular reviews and correction/mitigation of anything identified on the scans that shall be provided by the hosting vendor to confirm compliance.

20. Are there specific type of vulnerability tools preferred for the assessment that is currently used in the environment? Is it the responsibility of the vendor to provide the same tools for scanning?

    It is acceptable to audit vulnerability scans performed by hosting vendor, so no additional licenses are required.

    Vulnerability scans are performed on a regular schedule by the hosting vendor and in compliance with the NIST guidelines. It is acceptable for the auditing vendor to review the associated work instructions and the documentation of regular reviews and correction/mitigation of anything identified on the scans that shall be provided by the hosting vendor to confirm compliance.

21. Is NASWA providing vulnerability scans and Pen testing results for the audit? Or is vendor expected to perform these activities?

    NASWA will provide latest Pen test and vulnerability scan results. The vendor is not expected to perform their own penetration tests nor vulnerability scans.

    Production and test environment vulnerability scans are performed on a regular schedule by the hosting vendor and in compliance with the NIST

guidelines. The associated work instructions and the documentation of regular reviews and correction/mitigation of anything identified on the scans will be part of the materials provided to the auditing vendor to confirm compliance.

22. Will vulnerability scanning be done in the production environment?

    Production and test environment vulnerability scans are performed on a regular schedule by the hosting vendor and in compliance with the NIST guidelines. It is acceptable for the auditing vendor to review the associated work instructions and the documentation of regular reviews and correction/mitigation of anything identified on the scans that shall be provided by the hosting vendor to confirm compliance.

23. Will vulnerability scanning be required to be conducted during "off hours"?

    Production vulnerability scans are performed on a regular schedule by the hosting vendor and in compliance with the NIST guidelines. It is acceptable for the auditing vendor to review the associated work instructions and the documentation of regular reviews and correction/mitigation of anything identified on the scans that shall be provided by the hosting vendor to confirm compliance.

24. Are independent vulnerability scans required by the awarded vendor for the SIDES applications and subsystems using GFE?

    NASWA will provide latest Pen test and vulnerability scan results. The vendor is not expected to perform their own penetration tests nor vulnerability scans.

25. Has a Privacy Assessment been performed on the system in accordance with NIST requirements?

    No. No separate privacy assessment performed as the required privacy controls are in NIST 800-53 for MODERATE systems.

26. The SIDES application is hosted in a 3rd party data center. Are there security controls that are inherited from the 3rd party data center that will not be included in the scope of the assessment (e.g., Physical controls, Network Controls, etc.)?

    No. Security controls at the 3rd party data center will comply with industry standard security policies and procedures covered by NIST SP800-53

27. Does NASWA require the inclusion of any agency specific controls or controls additional to the NIST 800-53 security controls in the scope of the assessment?

    No. NIST SP800-53 Rev 4 controls for moderate system represents scope of the audit.

28. Is there a recording of the bidder's webinar that is available over the internet?

    Yes. However, please use written answers for reference purposes. Webinar is non-binding.

29. Will you detail all questions and answers in the written responses, not just those not addressed during today's session?

    Yes. All questions will be answered in detail in the official written responses and posted on the website.

30. Are there more details on the format of the proposal? Page count, etc.

    No. However please be concise and use structures stipulated in the RFP.

31. Does the auditor need to be a 3PAO?

    No.

32. Penetration testing is not required by the auditor?

    Penetration testing is out of scope for this RFP. Results from earlier penetration tests shall be included in the audit.

33. Can you please let us know in which states are the data center and failover sites hosted?

    SIDES is hosted in Blythwood, SC. Failover location is Irving, Texas.

34. Will a debrief be conducted of non-winners?

    As a courtesy, NASWA will provide an informal oral debrief to non-winners who request it.

35. How many physical locations/data centers are part of this effort?

    Two. One primary, plus a failover location, which also serves as storage location for backups.

36. Within the in-scope system components/Authorization boundary:
    a. How many on-site locations are in-scope?
        i. **Two. Primary and Failover sites.**
    b. How many interconnections are there?
        i. **50 States use and 28 Third Party Administrators interface with SIDES, using between 1 and 6 applications. Hub and spoke Broker architecture.**
        ii. **E-Response Website.**
    c. How many external facing IPs are there?
        i. **Two**
    d. How many Managed Service Providers are associated with the systems within the Authorization Boundary?
        i. **Hosting Vendor, plus one sub-contractor that manages the infrastructure and applications on behalf of the hosting vendor. A third sub-contractor is involved in application development.**
    e. Are there other 3rd party organizations that must be notified of the audit?
        i. **NASWA will notify states and USDOL ETA of audit results.**
    f. What types of coding languages are used in developing SIDES applications and services?
        i. **Java, JavaScript, oracle PL/SQL, .Net WCF**
    g. Has this system been evaluated against any other standards (HITRUST, ISO 2700X, SOC 2, etc.)?
        i. **No.**

37. Has SIDES been audited against FISMA requirements before?

    No.

38. Is there a complete System Security Plan?

    There is a complete security plan. It will be provided to the assessors as part of the documentation to be reviewed as part of the audit.

39. Are there complete policies and procedures that are in compliance with NIST 800-53 standards?

    Yes, but audit should include for identification of any gaps

40. Are there security interconnection agreements with all external parties utilizing the SIDES data and accessing the system?

    Participation agreements with states and TPAs that use the system.

41. Is the cloud infrastructure hosting the SIDES system FedRAMP accredited? Will complete documentation be provided as part of the audit effort?

    No. Implementation is not cloud based. SIDES is hosted on dedicated resources in a 3rd party data center.

42. Is remote work (at vendor facilities) acceptable to NASWA? With the assumption that the vendor will be onsite for interviews, audit, and planned meetings?

    The vendor would need to be onsite to access documents and conduct the audit at the data center. The access to proprietary NASWA and vendor FISMA/NIST control policy and procedures will be restricted to access onsite at the data center. The interviews with the system support staff and personnel responsible for the controls shall be conducted onsite at the data center in the presence of the SIDES onsite representatives; however, the interviews will be conducted via phone as most support personnel are remote from the data center.

    The expectation would be that the auditors would take notes documenting the policies and procedures as they relate to the NIST controls while they are conducting the assessment at the data center, and then use the notes to generate the audit report which would be composed at the auditing vendor facility.

43. It is our assessment that this project will require project manager, and 2 ½ information assurance specialists. Is that in line with your expectations from staffing/cost?

    Vendor must propose what they believe is required for a successful audit.

44. What are NASWA's requirements for the contractor in producing the final accreditation package, understanding that NASWA requires the contractor to deliver the Risk Assessment Report (RAR)?

    Please provide guidance to NASWA and the Hosting Vendor on what documentation should be included in the accreditation package.

45. Is the State Information Data Exchange System (SIDES) considered a Major Application?

    Yes. SIDES plays a major role in maintaining and improving the integrity of the UI Program.

46. Does SIDES have control inheritance or a common control package?

    No.

47. Reference the SIDES applications listed in Appendix A. Please clarify the specific scope of the required assessment. Is each SIDES application listed a separate website or a part of the same primary SIDES web application structure? Do the separate SIDES applications have separate logins? Do the SIDES application leverage two factor authentication? Are the 25 physical and virtual servers running Linux Operating Systems, the two-node database cluster for the SIDES database, 2 SIDES firewalls and 2 switches all a part of the assessment scope?

    There are separate WAR files for each SIDES application, both web sites and webservices. They are deployed as separate web applications and require separate logins. Two factor authentication is not implemented for SIDES. All servers run the Linux operating system. The 25 physical and virtual servers running Linux Operating Systems, the two-node database cluster, the 2 firewalls, and two switches are in scope.

48. Is this Request for Proposal (RFP) set-aside for small business participation only? We recommend that it be set-aside for small business as two or more small businesses are capable of performing the requirement.

    All qualified vendors are invited to respond.

49. What type of cloud service/ environment is in scope for this assessment and is this cloud service/environment FedRAMP authorized? (IAAS, PAAS, SAAS)

    This is not a cloud environment.

50. If this cloud service is FedRAMP authorized, will the awarded vendor have access to the FedRAMP package to leverage for the audit as to reuse “do once, use many time the package?

    Not Applicable. This is NOT a cloud environment.

51. If this cloud service is not FedRAMP authorized and the awarded vendor uses NIST 800-53 Rev 4 as the test cases, there will be missing controls specifically tailored for cloud services that won’t be tested/attested.
    The specific FedRAMP cloud compliance controls are not applicable at this time because this is not a cloud infrastructure.

52. Is an independent Penetration test IAW NIST 800-53 Rev 4 (CA-8) required for this project?

    No. Results of independent Pen Test will be provided.

53. How many environments are in scope for the SIDES assessment (production, development, test, etc.)?

    The production and test environment are within scope.

54. Is a PTA/PIA required for this project? Not listed in the deliverables for SA&A package as this is a FISMA requirement.

    SIDES is not formally subject to FISMA compliance. The presence of PII is recognized and incorporated in selection of MODERATE using SP800-60; this ensures inclusion of appropriate privacy controls.