Request for Proposal

Network and Web Application Security Assessment and Testing

State of Arizona Office of the Auditor General
10/20/2017

Table of contents

Introduction and background

State of Arizona Office of the Auditor General

Arizona Revised Statutes §41-1279.03 establishes the State of Arizona, Office of the Auditor General (Office), to be an independent source of impartial information concerning state and local governmental entities and to provide specific recommendations to improve those entities' operations. To fulfill our statutory duties, the Office must:

- Ascertain whether public entities are wisely using their resources–public money, personnel, property, equipment, and space;
- Determine whether public entities are complying with applicable laws, regulations, and governmental accounting and financial and reporting standards;
- Define standards and establish procedures for accounting and budgeting, as the Legislature requires; and
- Provide technical assistance to state and local governmental entities.

Purpose of the request for proposal

The Office is seeking consulting and technical assistance in conducting a security assessment of the network and a limited number of web applications developed and/or maintained by three institutions of higher education located in Arizona.[1] This assessment may include vulnerability assessments and automated and manual testing of potential problems to determine potential impact to network and system integrity with a special emphasis on the security of the electronic data these institutions collect and maintain. The Office anticipates the contractor will review at least one significant web application and the associated network servers and devices critical to these applications at each institution. In addition, the Office anticipates the contractor will test additional network servers and devices based on a risk-based review contractor and Office staff will perform centered on results of vulnerability scans that Office staff will perform before this engagement. Vulnerability scan results will be provided to the contractor after the contract is signed. This assessment will help identify potential security risks associated with these web applications and the IT environments in use at these institutions and will be used as the basis to form recommendations for improving security of the associated systems and the data these institutions maintain. The Office will also use these assessments to increase its staff's technical knowledge and experience in performing these types of reviews.

This assessment will be part of a larger review of information technology security management at the institutions the Office is auditing. The contractor will need to ensure that all information obtained during the engagement remains confidential and will be required to sign a confidentiality agreement.

[1] The specific institutions will be revealed to the selected contractor. The audited institutions are responsible for collecting and disbursing significant financial resources and handle a large volume of confidential and personally identifiable information.

The Office expects to receive proposals in the range of $50,000 to $75,000. Proposals above that range will be considered provided the contractor clearly explains the work to be done, the methodology to be employed, and the benefit expected to be gained to justify a proposal more than the expected range. Contractors are highly encouraged to itemize proposed services and rank the importance of the suggested services to the overall result.

The Office anticipates awarding the contract for this project by Friday, December 1, 2017. Work is expected to commence by Monday, December 11, 2017, and is anticipated to proceed until the final report's issuance, currently scheduled for Friday, June 29, 2018. The Office expects most of this proposal's test work to be completed by March 2, 2018, after which the contractor shall participate in meetings with the institutions involved and advise on and review report content.

The remainder of this document provides additional information regarding the anticipated scope and proposal requirements.

Requirements overview

Engagement requirements

The Office does not currently have a complete list of the network hosts and web applications or related systems in use at these institutions. The Office expects that such information will be prepared by the institutions and obtained through initial discovery and scanning the Office will perform, and that the information provided will be used to help the Office, with input from the contractor, to prioritize and select specific systems and applications to be reviewed. It is the Office's current understanding that each institution's web applications are developed, maintained, and managed independently from one institution to another.

The Office expects to assign at least one of its staff members full-time to work with the selected contractor conducting the network and web application assessments. The Office expects that, working with contractor guidance and assistance, Office staff will work alongside the contractor to perform some of the needed assessment work. Specifically, the Office expects its staff will perform initial host discovery and network scanning, and the contractor will help design and perform any automated and manual testing needed for both the network and selected web application systems.

The Office has conducted network, system, and web application testing in the past and does have some risk-based selection and assessment methodologies in place. However, the contractor shall review the Office's existing methodologies and suggest changes that may better align with current best practices and the requirements needed for this specific engagement.

The Office requires:

- Contractor input into the criteria and methodology for the selection of specific network hosts and web applications for further review;
- Contractor recommendations on best practices and development of specific steps and methodologies to be used to conduct the assessment and testing of the network hosts and web applications selected for review;
- Contractor assistance with direct testing of network hosts and web applications selected for review, particularly for development and execution of scripts, commands, and other techniques needed to perform test work;
- Contractor review of work performed by Office staff;
- Contractor expertise in developing remediation recommendations and criteria to support recommendations;
- Contractor participation in key meetings with executive-level and technical staff at each of the institutions to explain testing methodologies and results;
- Contractor maintain confidentiality of all information obtained during the assessment and sign a confidentiality agreement; and
- Contractor provide certificates of insurance prior to commencement of engagement.

The following additional information and specific examples relate to the above:

Criteria and methodology for selecting network hosts and web applications for review—The Office understands that the institutions operate and maintain potentially hundreds of web applications. The contractor will provide or assist the Office with updating its risk-based approach for selecting the network hosts and web applications to be further tested based on host discovery or vulnerability results.

Criteria and methodology for conducting the assessment—The Office expects that the contractor shall provide or assist the Office with updating its methodology for conducting network and web application assessments. The methodology shall comply with current best practices and be able to be followed in a logical and efficient manner.

Direct assistance with testing—The contractor shall guide and work with Office staff to perform the assessment work deemed necessary utilizing its current software tools.[2] In addition, the contractor shall perform some advanced technical and manual testing and shall be available to assist with technical questions and specific testing techniques, including:

- Assisting Office staff identify specific types of tests to perform based on the types of vulnerabilities identified.
- Performing and/or assisting Office staff exploit specific vulnerabilities found, such as SQL injection or cross-site scripting flaws, to determine whether the vulnerability is actually exploitable and the potential impact of the vulnerability on the security of the affected system(s) and data.
- Assisting Office staff understand unfamiliar terms or concepts encountered during the assessment.

The Office anticipates that the contractor will be able to provide most of this assistance by remote methods, such as conference calls, web-conferencing or desktop sharing sessions, brief phone or email conversations, scheduled training sessions, or other mutually agreed upon methods. However, some onsite presence during testing is anticipated, and the contractor shall respond and provide anticipated costs accordingly.

Review of work performed—The Office anticipates that Office staff will perform some of the assessment work. However, the contractor shall be available to review Office staff's work and provide feedback and suggestions for correction and/or improvement. This includes review of specific test work as well as written work products, report drafts, and the final report.

Develop Recommendations—The contractor shall assist the Office develop recommendations and supporting criteria needed to remediate the vulnerabilities discovered during the assessment. This may involve providing guidance to Office staff as to relevant and authoritative sources of information, researching specific remedies applicable to problems identified during the test work, and reviewing other information developed by Office staff (such as SDLC practices over web application development in operation at the institutions), etc.

[2] Current licensed tools used by the Office include: *Nessus Vulnerability Scanner and Burp Suite*. Primary open-source or freeware tools used may include: *Kali Linux*, *nmap*, *Metasploit Framework, Wireshark, or tcpdump*. Any additional open-source or freeware tools may be used as warranted by the testing being performed.

Participation in key meetings—The contractor shall participate in key meetings with Office executive-level and technical staff and staff at the audited institutions. The contractor shall assist in answering questions about the audit methodology, best-practice criteria, and recommendations. The Office anticipates that the contractor may be asked to participate in as many as eight to ten meetings with management and staff at the audited institutions, concentrated at the early and later stages of the audit, as well as other regular status meetings with Office staff. The Office anticipates that the contractor may be able to participate in many of these remotely but may require onsite visits for some of the critical meetings with institution management and staff.

Protection of information—The contractor shall ensure that all information obtained during the assessment remain confidential and will be required to sign a confidentiality agreement. The contractor shall provide assurance that any of its employees assigned to this work have undergone criminal background checks and have no criminal record.

The contractor shall agree to comply with and assume responsibility for employee compliance with the following requirements:

- All work will be performed under the Office's direction. The contractor will perform all work under the contractor's or the contractor's responsible employees' supervision.
- Any Office- or institution-held information that is made or becomes available to the contractor shall be used only for the purpose of carrying out the provisions of the contract entered into for the work associated with this RFP. Information the contractor obtains shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the contract's performance. Inspection by or disclosure by the contractor to anyone other than those prescribed by the Office is not authorized.
- Any Office- or institution-held information the contractor obtains shall be accounted for upon receipt and properly stored before, during, and after the assessment. In addition, all related output and products shall be given the same level of protection as required for the source material.
- No work performed under this contract shall be subcontracted without the Office's prior written approval.
- The contractor shall maintain a list of employees authorized to access to any information obtained or developed for the work associated with this RFP. The contractor shall provide this list to the Office upon request.
- The Office shall have the right to void the contract if the contractor fails to provide the above safeguards.

The contractor will be subject to criminal/civil sanctions if confidentiality laws of Office- or institution-held information obtained during the course of this assessment are violated. Penalties include potential fines and criminal prosecution. Additional information on specific sanctions defined in statutes applicable to the Office and the institutions will be provided after the contractor has been selected and will be incorporated in the contract.

Certificates of Insurance—Prior to beginning the work described herein, the contractor shall furnish certificates showing insurance in force as follows:

- Public Liability and Property Damage insurance in an amount not less than $2 million dollars ($2,000,000).

- Professional Liability Insurance in an amount not less than $1 million dollars ($1,000,000).

Excepting the Professional Liability coverage, insurance certificates shall name the State of Arizona AUDITOR GENERAL as an additional insured.

Technical and contractual contact

Contact information

Any questions concerning technical specification, contractual terms, and conditions or proposal format must be directed to either:

Name	Joseph Moore Director, IT Services	Melinda Gardner IT Audit Manager
Address	2910 N. 44th St. Suite 410 Phoenix, AZ 85018	
Phone	(602) 553-0333	(602) 553-9815
Fax	(602) 553-0051	
Email	jmoore@azauditor.gov	mgardner@azauditor.gov

Due Dates

A written confirmation of the contractor's intent to respond to this RFP is required by Friday, November 3, 2017. All proposals shall be in writing and are due by Friday, November 24, 2017, 4:00 P.M. MST. Any proposal received at the designated location after the required time and date specified for receipt shall be considered late and nonresponsive. Any late proposals will not be evaluated for award.

Contractors may submit questions to seek clarification on any element of this RFP. A separate contractors conference will not be held. Questions are to be submitted in writing to the contacts listed above, by mail or email. All questions are due by no later than Thursday, November 9, 2017 and will be answered by no later than Tuesday, November 14, 2017. Questions will not be accepted over the phone. All questions will be answered as soon as possible and will be made available to all interested contractors on a page designated for this purpose on the Arizona Auditor General website (http://www.azauditor.gov).

Schedule of events

	Event	Date
1.	RFP distribution to contractors	Friday, October 20, 2017
2.	Written confirmation of contractors with bid intention due (email is acceptable)	Friday, November 3, 2017
3.	Questions from contractors due	Thursday, November 9, 2017
4.	Responses to contractors' questions will be provided (Responses to all questions will be provided to all interested contractors. No individual responses will be provided)	Tuesday, November 14, 2017
5.	Proposal due date	Friday, November 24, 2017
6.	Contractor selection	Friday, December 1, 2017
7.	Anticipated commencement date (subject to change)	Monday, December 11, 2017
8.	Office report release date (subject to change)	Friday, June 29, 2018

Guidelines for proposal preparation

Proposal requirements

The Office expects to receive proposals in the range of $50,000 to $75,000. The Office will consider proposals above that range provided the contractor clearly explains the work to be done, the methodology that will be employed, and the benefit expected to be gained to justify a proposal more than the expected range. Contractors are highly encouraged to itemize proposed services and rank the importance of the suggested services to the overall result.

The Office anticipates awarding the contract for this project by Friday, December 1, 2017. Work is expected to commence by Monday, December 11, 2017, and is anticipated to proceed until the release of the Office's final report, scheduled for Friday, June 29, 2018.

The Office will award the contract to the most responsive contractor whose offer will be the most advantageous to the Office.

The State of Arizona Office of the Auditor General reserves the right to:

- Reject any or all offers and discontinue this RFP process without obligation or liability to any potential contractor;
- Accept other than the lowest-priced offer; and
- Award a contract on the basis of initial offers received, without discussions or requests for best and final offers.

Contractor's proposal shall include the parts set forth below. The contractor shall confine its submission to those matters sufficient to define its proposal and to provide an adequate basis for the Office's evaluation of the contractor's proposal.

The Office will incorporate the contractor's proposal in response to this RFP into the final agreement between the Office and the selected contractor. The submitted proposal shall include each of the following sections:

	Section description
1	Executive summary
2	Approach
3	Detailed and itemized pricing
4	Appendix: References
5	Appendix: Project team staffing
6	Appendix: Company overview

The detailed requirements for each of the above-mentioned sections are outlined below:

Executive summary

This section shall present a high-level synopsis of the contractor's responses to the RFP.

The executive summary shall be a brief overview of the engagement and shall identify the proposal's main features, benefits, and costs.

Approach

This section shall include details for how the contractor plans to specifically address elements listed in the requirements overview section above.

Detailed and itemized pricing

This section shall include an itemized price breakdown by objective/deliverable and the costs of any other expenses for which the contractor may bill. The Office will use an itemized list of costs to tailor services to fit funding resources and requirements, if necessary.

Appendix: References

This section shall include three (3) or more current references, including at least one reference from an organization for which the contractor has provided similar services to those proposed. Include company/agency name, contact name, contact title, entity address, contact telephone number, and client relationship synopsis.

Also disclose any work previously done for any governmental entity and institution of higher education in the State of Arizona.

Appendix: Project team staffing

This section shall include biographies and information about relevant experience of key staff and management personnel who will be involved with the project. Specifically, note experience conducting network security and web application security assessments in an institution of higher education environment, or one in which large amounts of highly confidential and sensitive information is maintained. List only the personnel who you anticipate will be performing work associated with this engagement. Affirm that no employees working on the engagement have ever been convicted of a felony. The contractor shall also ensure that no individuals working on the engagement have any impairment of independence in appearance or fact related to the specific institutions being audited.

Appendix: Company overview

This section shall include:

- Official registered name, address, main telephone number, toll-free numbers, and fax numbers.
- Key contact name, title, address, email address, direct phone, and fax numbers.
- Person authorized to contractually bind the organization for any proposal against this RFP.
- Brief history, including year established and number of years of offering services similar to those proposed.

Evaluation factors for award

The Office will base any award to be made pursuant to this RFP upon the proposal with appropriate consideration given to operational, technical, cost, and management requirements. The Office will evaluate offers based upon the contractor's responsiveness to the RFP and the total price quoted for all items the RFP covers. The selected contractor shall agree to the Office of the Auditor General's contract terms and conditions.

The following elements will be the primary considerations in evaluating all submitted proposals in selecting a contractor.

	Evaluation factors
1	Completion of all required elements of this RFP.
2	The extent to which the contractor's proposed solution fulfills the State of Arizona Office of the Auditor General's stated requirements as set out in this RFP.
3	An assessment of the contractor's ability to deliver the indicated service in accordance with the specifications set out in the RFP.
4	The contractor's stability, experiences, and record of past performance in delivering such services.
5	Availability of sufficient high-quality contractor personnel with the required skills and experience for the specific approach proposed.
6	Overall cost of the contractor's proposal.

The State of Arizona Office of the Auditor General may, at its discretion and without explanation to the prospective contractors, at any time, choose to discontinue this RFP without obligation to such prospective contractors.