



Office of the Washington State Auditor

STATE OF WASHINGTON

**Request for Quotations and Qualifications
(RFQQ)**

Security Assessment Services

**Preproposal Teleconference February 9, 2021 at 11:00 a.m. Local Time
Olympia, Washington**

**Proposals Due February 26, 2021 at 2:00 p.m. Local Time
Olympia, Washington**

Solicitation Coordinator Charleen Patten
Phone (564) 999-0941
E-Mail: contractmanager@sao.wa.gov

Office of the Washington State Auditor
3200 Sunset Way S.E.
PO Box 40031
Olympia, WA 98504-0031

TABLE OF CONTENTS

CHAPTER 1 - INTRODUCTION & DEFINITIONS	3
CHAPTER 2 - INSTRUCTIONS TO PROPOSERS	10
CHAPTER 3 - PROPOSAL SECTIONS	20
CHAPTER 4 - EVALUATION AND CONTRACT AWARD	26
EXHIBIT A – CERTIFICATIONS AND ASSURANCES.....	29
EXHIBIT B – REFERENCE WORKSHEET.....	31
EXHIBIT C – REQUIREMENTS CHECK LIST.....	32
EXHIBIT D – SAMPLE CONTRACT FOR PROFESSIONAL SERVICES.....	33
ATTACHMENT A – GENERAL TERMS AND CONDITIONS	39
ATTACHMENT B – SAMPLE TASK ORDER.....	47
ATTACHMENT C - Sample – DATA SHARING ADDENDUM.....	48
EXHIBIT E – STATE AUDITOR’S OFFICE (SAO) SECURITY QUESTIONNAIRE	55
EXHIBIT F – CONFIDENTIALITY AND NONDISCLOSURE AGREEMENT	57
EXHIBIT G – PROCUREMENT EVALUATION FOR EXECUTIVE ORDER 18-03 CERTIFICATION FORM.....	59

CHAPTER 1 - INTRODUCTION & DEFINITIONS

A. BACKGROUND

The State Auditor's Office (SAO) conducts cyber security performance audits. These cyber security audits involve assessing how well select state agencies and local governments are protecting their confidential information and systems from internal and/or external threats. The audits review certain state agencies' and local governments' information security posture or preparedness and exposure to cyber-attacks by performing such tests as covert and overt vulnerability assessment and penetration tests of select networks, applications and information systems. The audits could also include a review of state agencies' or local governments' systems to determine how well they are configured and monitored to detect and audit suspicious or unauthorized activity.

Local governments volunteer, then are prioritized based on the order they volunteer with some preference based on risk. State agencies are selected based on risk, with some preference given to volunteers.

State agencies and local governments provide Washington state citizens with a variety of services, such as education, law enforcement, regulatory oversight, utility services, and health services. Many state agencies and local governments also offer their customers web facing functionality, including web based reporting, payment, account management, and information searches. The state agencies and local governments that might be included in these audits can vary in size, from a few employees to thousands of employees.

In Washington, state law assigns the Office of the Chief Information Officer (OCIO) responsibility for developing and establishing IT security policies and standards and for monitoring state agency compliance with those standards. The state's Chief Information Officer reports directly to the Governor and is the Director of Washington Technology Solutions (WaTech). Individual state agencies are responsible for complying with the state's Information Technology (IT) security standards. WaTech also provides state agencies with enterprise IT security services and is the home of the state's Chief Information Security Officer.

Unlike the state, local governments are not required to adhere to standardized IT security guidance or report and coordinate with WaTech. The majority of local governments operate with a centralized IT organizational model with limited decentralization of selected functions. A common example would be a centralized IT department that provides IT security strategic direction, leadership and services with individual departments within the local government having responsibility for setting and maintaining application level security for selected applications.

B. OUR AUDIT AUTHORITY

In November 2005, voters approved Initiative 900

<https://sao.wa.gov/performance-audits/about-performance-audits/> giving the Washington State Auditor's Office (SAO) the authority to conduct independent, comprehensive performance audits of government agencies on behalf of citizens. The purpose of these audits is to ensure accountability and help ensure that tax dollars are spent as cost effectively as possible. Performance audits can examine the economy, efficiency and effectiveness of the policies, management, fiscal affairs and operations of state and local governments.

C. PURPOSE

The purpose of this Request for Quotations and Qualifications (RFQQ) is to competitively establish a contract with a qualified Vendor(s) interested in performing work on information technology (IT) security penetration tests for multiple state agencies and/or local governments. This assessment will be used by the State Auditor's Office to report on the selected state agencies' and/or local governments' security posture and to make recommendations for State and local government IT security programs. The SAO may contract with one or more Vendors as a result of this RFQQ.

The work may include, but not be limited to the following areas:

- reconnaissance of in-scope systems and networks
- simulate malicious computer and system attacks, including social engineering
- network and web application security testing
- wireless device assessments
- exploit development and execution

D. SCOPE AND OBJECTIVES

The contractor(s) will work collaboratively with the State Auditor's Office to conduct covert and/or overt penetration testing on select state agency and/or local government internal and external networks, applications, and information systems. The purpose of the penetration testing is to both assess select agencies' and local governments' risk of being compromised by a malicious attacker and to identify and recommend steps for preventing such attacks.

It is the intent of these audits to focus on systems impacting financial resources and confidential data, or on mission-critical systems that serve state agency or local government operations, from an external and internal perspective.

The State Auditor's Office will identify up to 12 state agencies per year of varying sizes to be included in the state cyber security audits. The state agencies included in these audits are located in Olympia, Washington and, depending how the audits are scoped, may include work at one or more agencies' remote sites located around the state of Washington.

The State Auditor's Office will identify up to 12 local governments per year of varying sizes to be included in the local cyber security audits. Inclusion of a local government in an audit is subject to local government approval. If more local governments are interested, the total number of local governments in this contract could be increased. If no local governments agree to have this work done, the local government component of this contract will be cancelled. The local governments included in these audits may be located anywhere in Washington State.

Work will be performed by the apparent successful proposer unless there is a conflict with a state agency or local government in accordance with [Exhibit A - Certifications and Assurances #2](#), in which case the work for that state agency or local government may be assigned to the next successful vendor.

The State Auditor's Office will collaborate with the contractor and state agencies or local governments to identify the networks, applications and information systems to be included in the scope of testing for each state agency or local government.

E. Deliverables

Identify areas for testing.

Together with the State Auditor's Office and the state agency or local government, perform preliminary analysis and identify areas to focus penetration testing. Testing may also include a review of prior testing findings to confirm remediation.

Develop Rules of Engagement (ROE) for external and internal penetration testing for each state agency and local government.

Each ROE includes detailed guidelines and constraints regarding the internal and external penetration testing execution. The ROE documents will be tailored to include specific details for each state agency or local government and must be established and approved by SAO and the state or local government under audit. For state agencies, the state Chief Information Security Officer (CISO) or the state CISO's designee must also approve the ROE before testing begins.

Conduct Testing

The consultant will conduct testing in accordance with the rules of engagement. Testing will be completed in close consultation with the SAO audit manager, or the Audit Manager's designee, and the SAO IT Security Specialist Manager or the Specialist Manager's designee.

The consultant will update SAO and the state agency or local government on the progress of the work daily throughout testing. Any critical findings will be communicated to SAO within 24 clock hours of their identification. Critical findings are those defined as potentially having an extreme impact to an entire entity and very likely to be exploited.

The SAO will schedule and oversee all meetings and interactions with state agency and/or local government executives and staff. A representative from SAO will accompany the Consultant on any interviews or site visits.

Provide knowledge transfer

The contractor will provide the training to transfer knowledge in the area of penetration testing to the SAO staff upon request by the SAO. Successful knowledge transfer will be verified by SAO IT security specialist staff.

Report Results

Detailed results should be reported to SAO assigned audit manager, or designee, on an ongoing basis as testing progresses:

- a. Communicate any critical findings within 24 clock hours of their identification
- b. Participate in status meetings.
- c. Provide weekly progress reports to the auditee and the SAO throughout the duration of the ongoing individual penetration engagements.
- d. Draft a detailed results document for each individual state agency and/or local government selected for audit and discuss results with the audit manager.
- e. Work in partnership with the audit manager to establish an agreed-upon standard reporting format. The report will include:
 1. Separate sections for management and technical audiences;
 2. An executive summary that presents findings, conclusions and recommendations;
 3. Testing methodology and a description of procedures used - testing methodologies should be described at a level of detail so that they are re-creatable using screen prints as necessary;
 4. All test results and findings, including identification of tests performed that did not identify issues;

5. Ranked results with a standard rating scale (likelihood and significance) detailing the seriousness of each finding and remediation prioritization;
6. Detailed information about how each issue can be fixed and the level of effort to fix;
7. A description of the implications or impact of not fixing each of the issues noted; and
8. An overall assessment based on the work performed for each agency and/or government including strengths and opportunities for improvement.

SAO will review the contractor's written products and provide feedback on desired changes. Written products are not considered complete until SAO has accepted the work. The contractor will be available to discuss results and information in the detailed results document with the SAO audit manager and state agency and/or local government staff on an ongoing basis by phone, and if deemed necessary, in face to face meetings.

F. MINIMUM QUALIFICATIONS

The following minimum qualifications are intended to ensure the proposer has adequate experience and expertise.

1. Proposers must possess at least five years of experience in providing the proposed penetration testing consulting services on a scale similar to a carrier class network.
2. Experience with large and small organizations in both government and private industries and U.S. federal government security clearance is a plus. The proposer must demonstrate that their staff collectively possess recent experience conducting IT security assessment services described below:
 - i. Vulnerability Assessments: Demonstrated experience in vulnerability assessments that include web applications, network, and source code. Qualifications could include at least one or more of the following certifications: Global Information Assurance Certification (GIAC), Web application Penetration Tester (GWAPT), Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH) or equivalent certifications as determined by SAO.
 - ii. Wireless: Demonstrated experience in auditing and assessing wireless networks. Qualifications could include GIAC Assessing and Auditing Wireless Networks (GAWN)
 - iii. Penetration testing experience, including exploitation of discovered vulnerabilities in test environments or non-invasive/passive testing in production environments containing highly sensitive information. Qualifications could include: Web application Penetration Tester (GWAPT), Offensive Security Certified Professional (OSCP), Exploit Researcher and Advanced Penetration Tester (GXPN)
 - iv. Expert-level knowledge of complex network design and architecture.
3. Ability and capacity to deliver services proposed.
4. Skills to communicate clearly and effectively both orally and in writing.
5. Skills to communicate effectively to a highly technical and non-technical audience, to include executives.
6. Contractor shall certify no contractor employee providing services to the state shall have been convicted of (a) a felony; or (b) a misdemeanor involving violence, sexual

misconduct, or dishonesty. For each contractor employee (U.S. Citizen and Non U.S. Citizen) Contractor shall:

Prior to the start date of any consultant employee hired in a “temporary to regular” status capacity, complete a Washington state criminal background check and a criminal background check covering all states of residence for: (a) ten year period or (b) for so long as the state records are available.

A proposer who does not meet these minimum qualifications will be deemed nonresponsive and will not receive further considerations.

G. REQUIREMENTS

1. The proposer must be aware of and comply with the Washington State Ethics in Public Service laws and rules. Refer to Chapter 42.52 Revised Code of Washington and Chapter 292 Washington Administrative Code, <http://apps.leg.wa.gov/rcw/default.aspx?Cite=42.52> and <http://apps.leg.wa.gov/WAC/default.aspx?cite=292>.
2. The proposer, if awarded the contract, must have or will obtain all necessary licenses to do business in the State of Washington. Refer to this link for guidance: <http://www.dol.wa.gov/business/>
3. The proposer will provide three relevant client references from past engagements.
 - a. These references will include the company’s name, contact person’s name, title, address, and phone number (see [EXHIBIT B – REFERENCE WORKSHEET](#)).
 - b. The Proposer’s submission of reference information constitutes permission for the State Auditor’s Office to contact the references indicated and others who may have pertinent information regarding prior experience and ability to perform the services contemplated in this solicitation.
4. If the consultant uses subcontractors, each subcontractor will be required to meet the same data security and background check requirements and sign the same nondisclosure agreement in [EXHIBIT F](#) as the primary consultant.

H. PERIOD OF PERFORMANCE

Any contract resulting from this RFQQ is tentatively scheduled to begin on or about May 1, 2021, with the period of performance ending December 31, 2023. For each audit, Task Orders will be issued (see Attachment B) with specific start and end dates for each engagement. Amendments extending the period of performance, if any, will be at the sole discretion of the State Auditor’s Office up to three additional years. Contract extensions may include extending the number of state agencies and/or local governments covered under the contract, as well as changes to the total contract value.

2. STANDARD DEFINITIONS

A. AUDITED ENTITY

The state agency or local government to be audited.

B. AUDIT MANAGER/PROGRAM MANAGER

The State Auditor’s Office employee or their delegate assigned to review the work and coordinate with the contractor.

C. CONTRACT

Refers to the legally enforceable agreement between the State Auditor’s Office and the contractor.

D. CONTRACTOR

The firm, provider, organization, individual or other entity, performing service(s) under this contract, and shall include all personnel of the contractor.

E. CONTRACTOR'S REPRESENTATIVE

An individual designated by the proposer or contractor to act on its behalf and with the authority to legally bind the proposer or contractor concerning the terms and conditions set forth in the solicitation and contract documents.

F. CONSULTANT

An independent, outside party able to provide SAO with work product, ideas, alternatives, best practices, data, and information related to the project(s).

G. GAO

The United States Government Accountability Office.

H. GOVERNMENT AUDITING STANDARDS

Standards established for audits of government organizations, programs, activities, and functions, and of government assistance received by contractors, nonprofit organizations, and other nongovernmental organizations. These standards, often referred to as Government Auditing Standards (GAGAS) or the Yellow Book, are to be followed by auditors and audit organizations when required by law, regulation, agreement, contract, or policy. These standards pertain to auditors' professional qualifications, the quality of audit effort, and the characteristics of professional and meaningful audit reports.

Government Auditing Standards can be accessed at: <https://www.gao.gov/products/GAO-18-568G>

I. PERFORMANCE AUDIT

Performance audit is defined in the Government Auditing Standards, Yellow Book.

J. PROPOSAL

A written response to this solicitation.

K. PROPOSER

An individual or organization submitting a response to this solicitation.

L. REQUEST FOR QUOTATIONS AND QUALIFICATIONS (RFQQ).

Formal procurement document in which services needed are identified and firms are invited to provide: 1) their qualifications and 2) hourly rates.

M. RCW

The Revised Code of Washington (laws of Washington State).

N. REPORTS

- **Detailed Findings**

A written detailed summary of results for each audited state agency or local government, including the methodologies used, observations, conclusions, and actionable recommendations for the audited entity(ies).

- **Final Report**

The State Auditor's Office will create and publish its own report.

O. RISK FACTOR

An observable or measurable indicator of conditions or events that could adversely affect an organization or the achievement of expected results or objectives.

P. SOLICITATION COORDINATOR

An individual designated by the State Auditor's Office to act on behalf of the state to administer the solicitation process.

Q. STATE AUDITOR'S OFFICE (SAO)

The State Auditor's Office shall mean any division, section, office, unit or other entity of the State Auditor's Office; or any of the officers or other officials lawfully representing the State Auditor's Office.

R. SUBCONTRACTOR

An individual or firm not in the employment of the contractor, who is performing all or part of the services under this contract under a separate contract with the contractor. The terms "subcontractor" and "subcontractors" means subcontractor(s) in any tier.

S. VULNERABILITY

Weakness in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat resulting in a negative impact to system confidentiality, integrity, or availability.

T. WAC

Washington Administrative Code. The administrative rules developed by the Washington Department of Commerce under WAC 194-37 are recognized as requirements of the Energy Independence Act.

U. WASHINGTON'S ELECTRONIC BUSINESS SOLUTION (WEBS)

An Internet vendor registration and bid notification system. The system offers one online site where vendors should register to receive State Auditor's Office and other governmental bid notifications.

V. YELLOW BOOK

Government Auditing Standards, July 2018 Revision, GAO-18-568G (or current version).

CHAPTER 2 - INSTRUCTIONS TO PROPOSERS

This section contains instructions regarding the preparation and submission of proposals.

1. SOLICITATION COORDINATOR

The Solicitation Coordinator is the sole point of contact at State Auditor's Office for this procurement. All communication between the proposer and State Auditor's Office will be with the Solicitation Coordinator, as follows:

Charleen Patten
Washington State Auditor's Office
3200 Sunset Way SE
PO Box 40031
Olympia WA 98504-0031
E-mail Address: contractmanager@sao.wa.gov
Telephone Number: (564) 999-0941

Physical Address for Hand Delivery or Courier Service:

Washington State Auditor's Office
3200 Sunset Way SE
Olympia WA 98504-0031

Any other communication will be considered unofficial and nonbinding on the State Auditor's Office. Proposers are to rely only on written statements issued by the Solicitation Coordinator or designee. Communication directed to parties other than the Solicitation Coordinator or his designee may result in disqualification of the proposer.

2. PROPOSER'S RESPONSIBILITIES

- A. Read and understand the solicitation document and all attachments.
- B. Seek clarifications if necessary.
- C. Become familiar with and abide by applicable federal laws and rules and Washington State statutes and regulations.
- D. Proposers interested in participating in the pre-proposal teleconference on February 9, 2021 (see schedule below), must call (360) 407-3780 prior to 11:00 a.m. local time in Olympia, Washington. The PIN code is 166923#.

3. ESTIMATED SCHEDULE OF PROCUREMENT ACTIVITIES

Event	Local Time in Olympia, Washington	Date
Issue Request for Quotes and Qualifications	12:00 pm	February 1, 2021
Pre-proposal teleconference (Highly recommended but not required).	11:00 am	February 9, 2021
Last date for questions regarding solicitation.	5:00 pm	February 9, 2021
Issue addendum, including question and answers, to RFQQ (if applicable)	5:00 pm	February 12, 2021
Last date for complaints regarding solicitation	5:00 pm	February 23, 2021
Issue addendum to RFQQ (if applicable)	5:00 pm	February 25, 2021
Proposals due	2:00 pm	February 26, 2021
Proposal evaluation begins	8:00 am	March 1, 2021
Hold Oral Interviews (if needed)	TBD	Week of March 17, 2021
Announce “Apparent Successful Contractor(s)” and send notification via fax or e-mail to unsuccessful proposers.	TBD	Week of March 22, 2021
Hold debriefing conferences (as required)	TBD	Week of March 22, 2021

THE STATE AUDITOR’S OFFICE RESERVES THE RIGHT TO REVISE THIS SCHEDULE

4. VENDOR QUESTIONS AND ANSWERS

Specific questions concerning this solicitation must be submitted in writing to the Solicitation Coordinator at the address specified in Chapter 2.1 of this solicitation. E-mail submission of questions is preferred. Any oral communications from the RFQQ Solicitation Coordinator will be considered unofficial and non-binding on SAO. The Solicitation Coordinator must receive questions no later than the time and date specified in Chapter 2.3 titled “**Schedule of Procurement Activities.**” All vendor questions and answers will be posted via WEBS by February 12 by 5 PM.

5. COMPLAINT PROCEDURE AND FORMAT

Complaints concerning this solicitation must be submitted in writing (phone calls will not be accepted) to the Solicitation Coordinator at the address specified in **Chapter 2.1** of this solicitation. E-mail submission of complaints is acceptable. The Solicitation Coordinator must receive complaints no later than the time and date specified in **Chapter 2.3** titled “**Schedule of Procurement Activities.**”

Proposers submitting complaints will follow the procedures described below. Complaints that do not follow these procedures will not be considered. This complaint procedure constitutes the sole administrative remedy available to proposers under this procurement.

All complaints must be in writing and signed by the complaining party or an authorized agent. The complaint must state the grounds for the complaints with specific facts and complete statements of the action(s) being complained. A description of the relief or corrective action being requested should also be included. All complaints will be addressed to the Solicitation Coordinator.

Only complaints stipulating an issue of fact concerning the following subjects will be considered:

- a) The solicitation unnecessarily restricts competition;
- b) The solicitation evaluation or scoring process is unfair or flawed; or
- c) The solicitation requirements are inadequate or insufficient to prepare a response.

Upon receipt of a complaint, the State Auditor’s Office will review and respond within 3 business days. The response will be posted on WEBS. The agency head will be notified of all complaints and be provided a copy of the agency’s response. The complaint may not be raised again during the protest period. There is no appeal process for complaints.

6. REQUIRED REGISTRATION (WEBS)

This solicitation will be issued via Washington’s Electronic Business Solution (WEBS).

Proposers are required to register in WEBS <http://des.wa.gov/Pages/default.aspx/>. In WEBS, the RFQQ can be located under the following commodity codes:

- 918-28 Computer Hardware Consulting
- 918-29 Computer Software Consulting
- 918-30 Computer Network Consulting
- 918-71 IT consulting
- 918-93 Security/Safety Consulting
- 920-65 System Requirements Quality Assurance Review

Downloading the solicitation from WEBS ensures any communications and addenda issued in reference to this solicitation are received by proposers planning to respond with a proposal. It is the proposer’s responsibility to check WEBS for addenda or modifications prior to submitting their proposal. The State and the State Auditor’s Office accept no liability and will provide no accommodation to proposers who fail to check for addenda and submit inadequate or incorrect responses. Proposers should contact WEBS Customer Service (360) 902-7400 (webcustomerservice@des.wa.gov) with any WEBS questions.

7. AMENDMENT TO THE SOLICITATION

In the event that it becomes necessary to revise any part of this solicitation, an amendment will be issued on WEBS. Questions and answers that are submitted to the Solicitation Coordinator and other pertinent information will be provided as an addendum to the solicitation. The State

Auditor's Office reserves the right to cancel or to reissue the solicitation in whole or in part, prior to execution of a contract.

If a conflict exists between addenda, amendments, or between an amendment and the solicitation, the document issued last will take precedence.

8. MINORITY & WOMEN-OWNED BUSINESS PARTICIPATION

In accordance with the legislative findings and policies set forth in Chapter 39.19 RCW, the State of Washington encourages participation in all of its contracts by firms certified by the Office of Minority and Women's Business Enterprises (OMWBE). Participation may be either on a direct or indirect basis in response to this solicitation. However, no preference will be included in the evaluation of proposals, no minimum level of minority and women business enterprises' participation will be required as a condition for receiving an award and proposals will not be rejected or considered nonresponsive on that basis. Any affirmative action requirements set forth in federal regulations or statutes included or referenced in the contract documents will apply.

The established annual procurement participation goals for this type of project are ten percent for minority business enterprises and four percent for women business enterprises. These goals are voluntary. Proposers may contact OMWBE at (360) 664-9750 for more information. Information on OMWBE can also be accessed at: www.omwbe.wa.gov

9. GENERAL STANDARDS FOR INDEPENDENCE AND IMPAIRMENTS (REFERENCE GAO-12-331G)

All properly submitted proposals will be screened for GAO Government Auditing Standards 2018 or latest (<https://www.gao.gov/products/GAO-18-568G>) General Standards for Independence. GAO Government Auditing Standards chapter defines independence as:

"In all matters relating to the GAGAS engagement, auditors and auditor organizations must be independent from an audited entity." Independence comprises:

- a. Independence of Mind:** The state of mind that permits the conduct of an engagement without being affected by influences that compromise professional judgment, thereby allowing an individual to act with integrity and exercise objectivity and professional skepticism.
- b. Independence in Appearance:** The absence of circumstances that would cause a reasonable and informed third party to reasonably conclude that the integrity, objectivity, or professional skepticism of an audit organization or member of the engagement team had been compromised.

As part of their response to solicitations, proposers will be required to identify nonaudit services (see <https://www.gao.gov/assets/700/693136.pdf>) let and/or performed within the last four years on behalf of all in-scope audited entities (defined in Government Auditing Standards). Proposers will include a list as part of [Exhibit A, Certifications and Assurances](#). This includes any subcontractors that may be employed by the proposer in performance of the contract. If no such services were performed for the audit entity, proposers will so indicate in [Exhibit A, Certifications and Assurances](#). Failure of proposers to so identify non-audit services performed on behalf of the audited entity as specified in this section will be deemed nonresponsive and their bids will be rejected. If the State Auditor's Office learns of such non-audit services subsequent to awarding the contract, and those non-audit services were not disclosed to the State Auditor's Office by the proposer, the State Auditor's Office may choose not to pay the proposer for work performed under the contract.

10. PROPRIETARY INFORMATION - PUBLIC DISCLOSURE

Materials submitted in response to this solicitation will become the property of the State Auditor's Office.

- A.** RCW 42.56, Public records: <http://apps.leg.wa.gov/rcw/default.aspx?Cite=42.56>

- B.** Washington Governor's Executive Order 16-01, issued January 5, 2016, Privacy Protection and Transparency in State Government:

http://www.governor.wa.gov/sites/default/files/exe_order/eo_16-01.pdf

Bidders are discouraged from submitting proprietary information in their proposal. Any information in the proposal which the proposer desires to claim as proprietary and exempt from public disclosure under the provisions of RCW 42.56 must be clearly designated in its proposal. **The proprietary information must be marked with the words "Proprietary Data" along with a statement of the basis for such claim of exemption.**

The State Auditor's Office will consider a proposer's request for exemption from disclosure; however, the State Auditor's Office will make the decision predicated upon RCW 42.56. Marking the entire proposal exempt from disclosure will not be honored. The proposer must be reasonable in designating information as proprietary. If any information is marked proprietary in the proposal, the State Auditor's Office's responsibility to notify will be limited to request(s) for disclosure made within a period of five years from the date of award.

If any information or materials that the proposer has marked as "Proprietary Data" are the subject of a public disclosure request, the State Auditor's Office's only obligation will be to notify the proposer that the request has been made and provide the proposer an opportunity to seek a court injunction against the requested disclosure. The proposer will have five (5) business days to respond to the State Auditor's Office's notice with its intent to seek a court injunction against the requested disclosure. If the State Auditor's Office receives no response from the proposer within the timeframe specified in this section, the materials and information will be released consistent with the State Auditor's Office policies and procedures under State law.

All requests for copies of contract files should be PublicRecords@sao.wa.gov.

11. PREPARATION AND SUBMISSION OF PROPOSAL

- A. Due Date and Time:** Proposers may submit proposals via email. The proposal, whether emailed or mailed, must be received by the State Auditor's Office no later than the date and time specified in the schedule of procurement activities (see **Chapter 2.3**). All times are considered local time for Olympia, Washington. The envelope should be clearly marked to the attention of the Solicitation Coordinator, who is the State Auditor's Office's sole point of contact for this procurement.

Late proposals will not be accepted and will be automatically disqualified from further consideration. Postmarks will not be accepted. Proposers who mail proposals should allow normal mail delivery time to ensure timely receipt of their proposals by the Solicitation Coordinator. Proposers assume all risk for the method of delivery chosen. The State Auditor's Office assumes no responsibility for delays caused by any delivery service. The proposals must respond to the procurement requirements. Do not respond by referring to material presented elsewhere. The proposal must be complete and must stand on its own merits.

- B. Format:** To receive consideration, proposals must conform to the format specified by the State Auditor's Office. Hardcopy proposals must be legible and be filled out in ink or with an electronic printer or other similar office equipment and properly signed by an authorized representative of the proposer. Electronic signatures will be accepted. The cover page will show the proposal number, title of the procurement and submission date. Each section will be clearly labeled and separated (with tabs if printed). All changes and/or erasures will be initialed in ink. Unsigned proposals will be rejected.

The electronic version of the proposal must be submitted in Word, Excel or PDF format. No proposals will be accepted via fax. **Email submissions must not exceed 10MB. If necessary proposers should submit proposals in more than one email.**

Proposal must be organized in sections as shown below (See Chapter 3 for subheadings and explanations for each section):

1. Letter of Submittal (Pass/Fail)
2. Quotation (Scored)
3. Qualifications (Scored)
4. Customer References (Pass/Fail)
5. Resumes (Scored)
6. Signed Certification and Assurances (Exhibit A) (Pass/Fail)
7. Sample report (Scored) **Note: report should be cleansed of confidential information. See Section VII on pgs. 24 and 25 of this RFQQ for details.**
8. Security questionnaire ([Exhibit E](#)) (Pass/Fail)
9. Confidentiality and Nondisclosure Agreement ([Exhibit G](#)) (Pass/Fail)
10. Procurement Evaluation for Executive Order 18-03 Certification Form (Scored)

Proposals will be prepared as instructed and delivered in the order given above (see [Exhibit C, Requirements Checklist](#)). Proposers will title and number each item in the same way it appears in each section of **Chapter 3** of this RFQQ.

The letter of submittal, quotation and qualifications will not exceed 25 combined total pages. The following are not included in the 25-page limit: customer references, resumes, signed certification assurances, sample report, security questionnaire, confidentiality and nondisclosure agreement and Procurement Evaluation for Executive Order 18-03, Customer References.

Identification:

Proposals must be submitted in a sealed envelope or email attachment to the addressed as shown below:

Proposer's Return Address
Solicitation Number: K646-RFQQ-2011
Solicitation Coordinator Name: Charleen Patten

State Auditor's Office Address
3200 Sunset Way S.E.
PO Box 40031
Olympia, WA 98504-0031
Email: Contractmanager@sao.wa.gov

Late proposals will not be accepted and will be automatically disqualified from further consideration. The proposals must respond to the procurement requirements. Failure to respond to any portion of the procurement document may result in rejection of the proposal as nonresponsive.

12. CONTRACT AND GENERAL TERMS & CONDITIONS

The apparent successful proposer will be expected to enter into a contract that is substantially the same as [Exhibit D - Sample Contract for Services](#). **In no event is a proposer to submit its own standard contract terms and conditions in response to this solicitation.** Proposers may submit exceptions as allowed in [Exhibit A - Certifications and Assurances](#); however, exceptions must be limited to terms that would prevent the proposer from contracting with the State Auditor's Office. The State Auditor's Office will review requested exceptions and accept or reject them at its sole discretion.

13. COSTS TO PROPOSE

The State Auditor's Office will not be liable for any costs incurred by the proposer in preparation of a proposal submitted in response to this solicitation, in conducting a presentation, or any other activities related to responding to this solicitation.

14. ERRORS AND OMISSIONS IN PROPOSAL

The State Auditor's Office will not be liable for any errors or omissions in proposals. Proposers will not be allowed to alter or supplement their proposal documents after the proposal due date.

15. NO OBLIGATION TO CONTRACT

This RFQQ does not obligate the State of Washington or the State Auditor's Office to contract for services specified herein.

16. SIGNATURES

The **Letter of Submittal**, the **Certifications and Assurances Form (Exhibit A)**, **Confidentiality and Nondisclosure Agreement (Exhibit F)** and **Procurement Evaluation for Executive Order 18-03 Certification Form (Exhibit G)** must be signed and dated by a person authorized to legally bind the proposer contractually, e.g., the President or Chief Executive Officer if a corporation, the managing partner if a partnership, or the proprietor if a sole proprietorship.

17. RESPONSIVENESS

All proposals will be reviewed by the Solicitation Coordinator to determine compliance with administrative requirements and instructions specified in this solicitation. Failure to comply with any part of the solicitation may result in rejection of the proposal as nonresponsive.

The State Auditor's Office reserves the right to require clarification, additional information, and materials in any form relative to any or all of the provisions or conditions of this solicitation. The State Auditor's Office also reserves the right, however, at its sole discretion to waive minor irregularities.

18. PROPOSAL REJECTION

Solely, the State Auditor's Office will make a determination of clarity and completeness in the responses to any of the provisions in this solicitation. Proposers are specifically notified that failure to comply with any part of the solicitation may result in rejection of the proposal as nonresponsive. The State Auditor's Office reserves the right at its sole discretion to reject any and all proposals received without penalty and not to issue a contract as a result of this solicitation.

19. FAILURE TO COMPLY

The proposer must provide a response to all sections specified as mandatory requirement (MR) and pass/fail. Failure to comply with any part of the State Auditor's Office's request for proposal may

result in the firm's proposal being disqualified (and not scored) for being nonresponsive to the State Auditor's Office's request.

20. ACCEPTANCE PERIOD

Proposals will provide 60 days from the due date for receipt of proposals for acceptance by the State Auditor's Office.

21. CONTRACT FORMATION

A submitted proposal is an offer to contract with the State. A proposal becomes a contract when officially accepted in writing by the State through a contract. All proposals submitted become the property of the State and the State Auditor's Office and may be deemed public records as defined in RCW 42.56.

22. MOST FAVORABLE TERMS

The State Auditor's Office reserves the right to make an award without further discussion of the proposal submitted. Therefore, the proposal should be submitted initially on the most favorable terms that can be proposed. There will be no best and final offer procedure. In addition, if the proposer is selected as an apparent successful contractor, the State Auditor's Office reserves the right to enter into contract negotiations with the apparent successful proposer, which may include discussion regarding the terms of the proposal. Contract negotiations may result in incorporation of some, or all, of the proposal. The proposer should be prepared to accept this solicitation for incorporation into a contract resulting from this solicitation. It is also understood that the proposal will become part of the official procurement file.

23. AWARD

Upon award, notification will be sent by the Solicitation Coordinator in writing via e-mail to all participating proposers. The State Auditor's Office reserves the right to contract with more than one vendor. Additional information may be obtained by reviewing the purchase/contract file after award. Award results will not be given over the phone. Award of this contract does not guarantee work.

24. INSURANCE COVERAGE

The successful proposer will provide insurance coverage, as set out in this section. Contractor (and any Subcontractor not covered under Contractor coverages that meet the insurance coverage requirements set out in this section) must meet insurance coverage requirements. The intent of the required insurance is to protect the State Auditor's Office and state and/or local government agencies selected for audit should there be any claims, suits, actions, costs, damages or expenses arising from any negligent or intentional act or omission of the contractor or its agents, while performing under the terms of this contract. The contractor will submit to the State Auditor's Office within 15 days of the contract effective date, a certificate of insurance which outlines the coverage and limits defined in the Insurance section. The contractor will submit renewal certificates as appropriate during the term of the contract.

The contractor will maintain insurance coverage which will be maintained in full force and effect during the term of this contract, as set forth below.

- a. **Commercial General Liability (CGL) Insurance Policy:** Provide a Commercial General Liability covering the risks of bodily injury (including death), property damage and personal injury, including coverage for contractual liability, with a limit of not less than \$1,000,000 per occurrence.

- b. **Automobile Liability:** In the event that services delivered pursuant to this contract involve the use of vehicles, either owned or not owned by the contractor, automobile liability insurance will be required. The minimum limit for automobile liability is: \$1,000,000 per occurrence, using a Combined Single Limit for bodily injury and property damage.
- c. **Errors and Omissions/Professional Liability:** Contractor shall maintain Errors and Omissions insurance covering contractor's services, without exclusion or limitation for claims arising out of data breaches which may arise as a result of the services. Coverage with limits of not less than \$1,000,000 per occurrence, continue such coverage for six (6) years beyond the expiration or termination of this Contract.
- d. **Cyber Security Insurance:** The Contractor shall maintain both first party and third party Cyber Security Insurance covering data breaches, network damage, cyber extortion and other claims or damages which may arise in connection with IT security assessment services with limits not less than \$2,000,000 per claim or occurrence. The contractor will continue to carry this insurance for three years past the end of the engagement.
- e. **Workers Compensation Insurance:** Workers compensation coverage with Washington statutory limits and employer's liability coverage of not less than \$500,000 for employers' liability. The contractor will at all times comply with all applicable workers compensation, occupational disease, and occupational health and safety laws, statutes and regulations to the full extent applicable. The State of Washington will not be held responsible in any way for claims filed by the contractor or their employees for services performed under the terms of the contract.
- f. **Employers Liability Insurance:** In addition, the contractor shall maintain employers' liability insurance, including but not limited to coverage for employee fraud and dishonesty with limits not less than \$1,000,000 per occurrence.
- g. **Umbrella Insurance:** Commercial umbrella liability insurance affording excess coverage above the primary policies noted in above, with limits not less than \$1,000,000 per occurrence.
- h. **Additional Provisions:**
 - 1. **Additional Insured:** The insurance required will be issued by an insurance company/ies authorized to do business within the State of Washington, and, with the exception of the Errors and Omission policy, will name the State of Washington, its agents and employees as additional named insureds under the insurance policy/ies. All policies will be primary to any other valid and collectable insurance.
 - 2. **Cancellation:** The State Auditor's Office will be provided 30 calendar days written notice before cancellation or nonrenewal of any insurance referred to herein. The contractor will instruct the insurers to give the State Auditor's Office 30calendar days' advance notice of any insurance cancellation or nonrenewal action.
 - 3. **Identification:** Policy must reference the State's contract number and the State Auditor's Office.
 - 4. **Insurance Carrier Rating:** All insurance and bonds should be issued by companies admitted to do business within the State of Washington and have a rating of A-, Class VII or better in the most recently published edition of Best's Reports. Any exception will be reviewed and approved by the State Auditor's Office's Risk Manager or the Risk Manager of the Department of Enterprise Services, before the contract is accepted or work may begin. If an insurer is not admitted, all insurance policies and procedures for issuing the insurance policies must comply with RCW 48.15 and WAC 284-15.
 - 5. **Excess Coverage:** By requiring insurance herein, the State does not represent that coverage and limits will be adequate to protect the contractor, and such coverages and

limits will not limit contractor's liability under the indemnities and reimbursements granted to the State in this contract.

25. COMMITMENT OF FUNDS

The State Auditor or his or her delegates are the only individuals who may legally commit to the expenditures of funds or approve payment terms for work delivered under a contract resulting from this solicitation.

CHAPTER 3 - PROPOSAL SECTIONS

This chapter contains instructions regarding the preparation and submission of proposals. The proposer must provide all information requested in the exact order specified below. [Exhibit C](#) is provided for the proposer's convenience in providing the following information. Please use the checklist for the appropriate category.

Each proposer's Qualifications will be identified in sufficient detail to convey to members of the evaluation team the proposer's abilities, knowledge, experience and skills.

Proposals that do not sufficiently demonstrate expertise will be rejected.

SECTION I – LETTER OF SUBMITTAL – Mandatory Required (MR)/ (PASS/FAIL)

A. ORGANIZATION SUMMARY (MR)

The proposer must provide a summary of the organization/firm/individual's pertinent expertise, skills, client base and services that are available for this project.

B. BUSINESS IDENTIFICATION (MR)

The proposers must provide an overview of their firm/organization, including, but not limited to the following:

- ✓ Organization/firm's name, address and main business location
- ✓ The location of the facility from which the proposer would operate, including the telephone, fax and e-mail address
- ✓ Organization/firm's start-up date.

C. COMPANY OFFICERS (MR)

The proposer must provide the names, addresses, and telephone numbers of principal officers (President, Vice President, Treasurer, Chairperson of the Board of Directors, etc.).

D. PRIMARY CONTACT (MR)

The proposer must include who within the firm/organization will have prime responsibility and final authority for the work under the proposed contract. Include the following:

- ✓ Name
- ✓ Title or position
- ✓ Address
- ✓ E-mail address
- ✓ Telephone and fax numbers.

E. LEGAL STATUS (MR)

The proposer must specify the legal status of the Organization/Firm (sole proprietorship, partnership, corporation, etc.) and the year the entity was organized to do business as the entity now exists.

F. FORMER EMPLOYEE STATUS (MR)

If any employee of the proposer was an employee of the State of Washington or a Washington local government during the **past 24 months**, or is now an employee of the State of Washington or Washington local government, identify the individual

by name, state agency or local government previously or currently employed by, job title or position held and separation date.

H. OMWBE STATUS (MR)

Minority and women-owned businesses are encouraged to participate. Please identify if the contractor or any subcontractors are a minority and women-owned business. Please provide the OMWBE certification number.

G. CONTRACT TERMINATIONS (MR)

If the proposer has had a contract terminated for default in the **past five years**, describe such incident. Termination for default is defined as notice to stop performance due to the proposer's nonperformance or poor performance. Issue of performance may have been:

- ✓ Not litigated due to inaction on the part of the proposer, or
- ✓ Litigated and such litigation determined that the proposer was in default.

Proposers will submit full details of the terms for default. Proposers will identify the other party, its name, address, and phone number, and present the proposer's position on the matter. The State Auditor's Office will evaluate the facts and may, at its sole discretion, reject the proposal on the grounds of the past experience.

If the proposer has experienced no such termination for default in the **past five years**, so indicate.

H. TAX INFORMATION (MR)

The proposer must provide its Federal Employer Tax Identification number and the Washington Uniform Business Identification (UBI) number issued by the State of Washington Department of Revenue.

I. SUBCONTRACTOR QUALIFICATIONS (MR)

For each subcontractor, the proposer must address the submittal questions set forth in A – C and E – I above.

The proposer must include a statement that if awarded the contract as the primary contractor, the proposer will accept full responsibility for successful performance of the entire scope of work.

J. STATEMENT OF ACCEPTANCE OF TECHNICAL REQUIREMENTS (MR)

The Letter of Submittal will include a statement that the proposer accepts all of the elements and requirements identified in Section III, Qualifications Section, and be signed by the principal, partner or appropriate obligating authority.

K. COMPLIANCE WITH INSURANCE REQUIREMENTS (MR)

Each proposer must indicate in the Letter of Submittal and, as a condition of contract award, that it will submit to the State Auditor's Office within 15 days of the contract effective date, a certificate of insurance which outlines the coverage and limits as defined in the Insurance section.

SECTION II – QUOTATIONS SECTION MANDATORY REQUIRED (MR) (SCORED)

A. COST PROPOSAL (MR)

The State Auditor's Office requires two price quotes for this RFQQ.

- 1) Proposers must provide a single, not-to-exceed, "blended hourly rate" price quote for the contract term. Proposers shall be bound by the hourly rate they quote in this RFQQ. The rates quoted will be considered "not-to-exceed" rates.
- 2) Because the specific state agencies and/or local governments are not identified, bidders are instructed to provide a bid (price quote) for the sample state agency listed below as well.

Proposers must consider the following when completing the Price Proposal:

- Overtime rates are not allowed.
- Quote all-inclusive rates in United States dollars to include travel and all expenses to accommodate working with State Auditor's Office. Consultants are required to collect and pay Washington State taxes as applicable.

The Proposal must contain a comprehensive description of services including the following elements:

- **Project Approach/Methodology (MR)** – Include a complete description of the proposed approach and methodology for completing the testing, performing the analysis and preparing the report.
- **Work Plan (MR)** – Include all project requirements and the proposed tasks, services, activities, etc. necessary to accomplish the testing in the scope of the project defined in this RFQQ. This section of the technical proposal must contain sufficient detail to convey to members of the evaluation team the proposer's knowledge of the subjects and skills necessary to successfully complete the testing for this project. Include any required involvement of State Auditor's Office staff.
- **Project Schedule (MR)** – Include a project schedule indicating when the testing would be completed and when deliverables, would be provided. Bidders will consider that documentation detailing the testing completed to identify issues, including screen shots as necessary, is required to support the detailed testing results communicated to agencies.
- **Deliverables (MR)** – Fully describe content and format of deliverables to be submitted under the proposed contract.

For purposes of this estimate, the sample state agency is defined as having 1,000 employees; may have both structured and unstructured data, servers, workstations, network devices, mobile systems, firewalls, virtual private networks and other systems prevalent in an enterprise environment; has some internal development of web facing functions with reliance on third party vendors for some functions; and has confidential data that may include FERPA, PII, HIPAA, criminal justice and payment card information. In addition, the proposer should provide an estimated number of hours expected to be required to complete all deliverables for a sample state agency audit.

The size and complexity of each selected state agency and/or local government will vary.

The evaluation process is designed to award a contract to the Consultant(s) whose proposal best meets the requirements of this RFQQ.

B. COMPUTATION

The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price.

The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. This means that the overall score for the cost proposal will account for the robustness of the proposer's qualifications as well as their proposed price. We will include both the blended hourly rate and the price quote in scoring the cost proposal. The cost proposal will be worth up to 10 percent of the total possible points – see the table in Chapter 4.4 of this RFQQ.

SECTION III – QUALIFICATIONS SECTION (MR) (SCORED)

The Qualifications Section of the proposal must contain information that will demonstrate to the evaluation committee the Firm/Staff understanding of the types of services proposed, the ability to accomplish them, and the ability to meet tight timeframes. Firm experience will be scored based on the capacity and experience of the firm to perform work similar to the tasks described in this RFQQ. Staffing will be scored on how the proposer staffs the project to perform work similar to the tasks described in this RFQQ, including the number of staff and the mix or make of the team and their various levels of experience.

Recent experience with both government and private industries is a plus for both firm experience and staffing. Describe Vendor's experience and qualifications (in terms of Firm Experience and Staffing), especially with respect to performing work similar to the tasks described in this RFQQ. Provide experiences comparable to:

- Vulnerability Assessments: Demonstrated experience in leading and/or participating in vulnerability assessments that include web applications, network, and source code. Qualifications could include at least one or more of the following certifications: Global Information Assurance Certification (GIAC), Web application Penetration Tester (GWAPT), Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH);
- Wireless: Demonstrated experience in auditing and assessing federated wireless networks. Qualifications could also include GIAC Assessing and Auditing Wireless Networks (GAWN);
- Non-invasive penetration testing experience of production environments, or identically structured pre-production or test environments, containing highly sensitive information. Qualifications should include: Web application Penetration Tester (GWAPT), Offensive Security Certified Professional (OSCP), Exploit Researcher and Advanced Penetration Tester (GXPN); and
- Expert-level knowledge of complex network design and architecture.

In scoring this section, SAO may favor those Vendors describing experience providing services to state agencies or local governments.

The Vendor must describe at least five (5) representative projects the Vendor has performed for customers during the three (3) years preceding the Proposal due date. Describe completed projects only; projects where the services are in the process of being put in place will not satisfy this requirement. The Vendor and their key team members must have had primary responsibility for the various phases of the projects including analysis, testing, document review, implementation and reporting. Do not exceed two (2) typewritten, single-sided pages for each project's description. Each description should include, at a minimum, the project's purpose (i.e., Project Statement), the project's deliverables, the project's duration, and the results.

Scores for this section will be based upon, but not limited to, the degree to which the Vendor demonstrates direct experience with all aspects of performing penetration testing in large, medium and small networked organizations, and broad expertise with this type of work. Importance is given to the specific project role the Vendor has performed, as well as the scope

and complexity of the projects in which the Vendor has participated. Both depth and breadth of experience are important.

- Provide resumes (in Section V), which include information on the individuals' particular skills related to penetration testing, education, certifications experience, significant accomplishments and any other pertinent information.
- Demonstrate skills to communicate clearly, concisely and effectively both verbally and in writing.
- Describe the firm's methods for maintaining staff qualifications.
- Management approach, methodology and implementation strategies for managing and delivering their product.
- Describe their ability and capacity for delivering services proposed.
- Sample report (Scored) Note: report should be cleansed of confidential information.

SECTION III-a – QUALIFICATIONS SECTION (Optional and separate from Section III)

As a separate part of the response to this section we are interested to hear the consultant's perspective on what risks the potential contractor cannot control in this project.

Additionally, we would like the consultant's perspective on services that would add value to our proposed scope of work, but that we did not request.

SECTION IV – CUSTOMER REFERENCES (MR)/ (PASS/FAIL)

The proposer must supply names, addresses, email addresses and telephone numbers of a minimum of three nonproposer-owned customer references for which the proposer has recently completed work. *Proposers are discouraged from listing current State Auditor's Office employees as references.* Note what type of work was performed by the proposer for the reference, and how it is relevant to the work/activity proposed in this solicitation, and provide a sample of the work if different from work samples provided by requirement. By signing [Exhibit A - Certifications and Assurances](#), the proposer and proposed staff grant the State Auditor's Office permission to independently contact references and others who may have pertinent information. [Exhibit B - Reference Worksheet](#) is provided for proposers to list their references.

Each reference will be asked about the approach proposers used to deliver services and the quality of services delivered. The State Auditor's Office will not accept terms for contacting references other than those stated above.

SECTION V – RESUMES (MR) (SCORED)

The proposer must provide resumes for key staff and include information on each individual's specific skills, experience, certifications significant accomplishments and responsibilities assumed on other similar projects related to the services proposed.

SECTION VI – CERTIFICATIONS AND ASSURANCES (MR)/ (PASS/FAIL)

Section VI must include a signed Certifications and Assurances form, see: [Exhibit A - Certifications and Assurances](#) (MR)

SECTION VII – SAMPLE REPORT (MR) (SCORED)

The proposer must provide one sample report that discusses work, and its related results, in areas similar to those that are referenced in the first set of bulleted items in Section III above.

This sample report may either be an actual report that the proposer has delivered to a previous client, as long as the contents have been redacted according to any applicable laws, regulations, or agreements with that client, or it may be a mock report that the proposer has generated specifically for their response to this RFQQ.

This sample report will be scored based on how well its components respond to items listed under item “d.” under “Report Results” on page 5 of this RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.

SECTION VIII – SECURITY QUESTIONNAIRE (MR)/ (PASS/FAIL)

The proposer must provide a completed State Auditor’s Office (SAO) Security Questionnaire (see [Exhibit E](#)). If selected, the vendor may be asked to provide verification of responses provided to the questionnaire which may include: security audits such as a SOC 2 report or any IT security reviews completed by an external auditor; additional questions; or onsite verification.

SECTION IX – CONFIDENTIALITY AND NONDISCLOSURE AGREEMENT (MR)/ (PASS/FAIL)

The proposer must provide a completed State Auditor’s Office (SAO) Confidentiality and Nondisclosure agreement (see [Exhibit F](#)).

SECTION X - PROCUREMENT EVALUATION FOR EXECUTIVE ORDER 18-03 CERTIFICATION FORM (MR) (Scored)

Pursuant to RCW 39.26.160(3) (best value criteria) and consistent with [Executive Order 18-03 – Supporting Workers’ Rights to Effectively Address Workplace Violations](#) (dated June 12, 2018), Office of the Washington State Auditor will evaluate bids for best value and provide a bid preference in the of 5 points to any bidder who certifies, pursuant to the certification attached as [Exhibit G – Contract Certification for Executive Order 18-03 – Worker’s Rights](#), that their firm does NOT require its employees, as a condition of employment, to sign or agree to mandatory individual arbitration clauses or class or collective action waiver.

CHAPTER 4 - EVALUATION AND CONTRACT AWARD

1. EVALUATION PROCEDURE

ALL MANDATORY REQUIREMENTS OF THE RFQQ MUST BE MET IN ORDER FOR THE PROPOSAL TO BE EVALUATED.

The proposer is specifically notified that failure to comply with any part of the solicitation may result in rejection of the proposal as nonresponsive. The State Auditor's Office also reserves the right, at its sole discretion, to waive minor irregularities.

Responsive proposals will be evaluated strictly in accordance with the requirements stated in the RFQQ and any amendments/addenda issued. The evaluation of proposals will be accomplished by an evaluation team to be designated by the State Auditor's Office, which will determine the ranking of proposals.

During proposal evaluation, the State Auditor's Office reserves the right to make reasonable inquiry to determine the responsiveness of any proposer. Requests may include, but not be limited to, compliance to standards for independence, financial statements, credit ratings, references, record of past performance, and on-site inspection of proposer's facilities. Failure to respond to said request(s) will be sufficient reason to consider the proposal nonresponsive.

2. CLARIFICATION OF PROPOSAL

The Solicitation Coordinator may contact a proposer for clarification of any portion of the proposal.

3. PASS/FAIL EVALUATIONS

Proposers failing the Letter of Submittal, Customer References, Signed Certifications and Assurances or Samples of Work, Security Questionnaire and Signed Nondisclosure Agreement sections will be viewed as not meeting the mandatory requirements and will be eliminated from further consideration.

4. EVALUATION CRITERIA

The following weights will be assigned to each proposal for evaluation purposes:

Section Title	Percentage of Points
Letter of Submittal	Pass/Fail
Quotations Section (Cost Proposal)	10 percent
Qualifications Section – Firm Experience	35 percent
Qualifications Section – Staffing	25 percent
Customer References	Pass/Fail
Resumes	10 percent
Signed Certifications & Assurances	Pass/Fail
Sample Report	15 percent
Security Questionnaire	Pass/Fail
Signed Nondisclosure Agreement	Pass/Fail
Executive Order 18-03	5 percent
Total	100 Percent

5. ORAL PRESENTATIONS MAY BE REQUIRED

Written proposals and oral presentations, if necessary, will be used in selecting the winning proposal. The State Auditor's Office, at its sole discretion, may elect to select the top-scoring finalists from the written evaluation for an oral presentation. Should the State Auditor's Office elect to hold oral interviews, the State Auditor's Office will contact the finalists to schedule a date, time and will be performed using a web-based conference call.

Commitments made by the proposer at the oral interview, if any, will be considered binding. The oral interview will determine the apparent successful proposer. The scoring committee makes a recommendation to the Director of Performance Audit, who names the apparent successful proposer.

5. NOTIFICATION TO PROPOSERS

Both successful and unsuccessful proposers will be notified via e-mail.

6. DEBRIEFING OF UNSUCCESSFUL PROPOSERS

Proposers who submitted a proposal and were not selected will be given the opportunity for a debriefing conference. The Solicitation Coordinator must receive a written request from the unsuccessful proposer for a debriefing conference within three (3) business days after the Notification of Unsuccessful Proposer letter is e-mailed. The request for a debriefing can be in hard copy or via e-mail. The debriefing will be held within three (3) business days of the request unless the State Auditor's Office schedules otherwise.

Discussion will be limited to a critique of the requesting proposer's proposal. Comparisons between proposals or evaluations of the other proposals will not be allowed. Debriefing conferences may be conducted using a web-based conference call or on the telephone and will be scheduled for a maximum of one hour.

7. PROTEST PROCEDURE AND FORMAT

This procedure is available to proposers who (1) submitted a response to this solicitation document and (2) have participated in a debriefing conference. Upon completing the debriefing conference, the proposer is allowed five (5) business days to file a protest of the procurement with the Solicitation Coordinator. Protests may be submitted by facsimile or e-mail, but must be followed by the original document.

Proposers protesting this procurement will follow the procedures described below. Protests that do not follow these procedures will not be considered. This protest procedure constitutes the sole administrative remedy available to proposers under this procurement.

All protests must be in writing and signed by the protesting party or an authorized agent. The protest must state the grounds for the protest with specific facts and complete statements of the action(s) being protested. A description of the relief or corrective action being requested should also be included. All protests will be addressed to the Solicitation Coordinator.

Only protests stipulating an issue of fact concerning the following subjects will be considered:

- A matter of bias, discrimination or conflict of interest on the part of the evaluator.
- Errors in computing the score.
- Noncompliance with procedures described in the procurement document.

Protests not based on procedural matters will not be considered. Protests will be rejected as without merit if they address issues such as: 1) an evaluator's professional judgment on the quality of a

proposal, or 2) State Auditor's Office's assessment of its own and/or other agencies' needs or requirements.

Upon receipt of a protest, a protest review will be held by the State Auditor's Office. The State Auditor's Office will designate three individuals who were not involved in the procurement to consider the record and all available facts and issue a decision within five business days of receipt of the protest. If additional time is required, the protesting party will be notified of the delay. In the event a protest may affect the interest of another proposer that submitted a proposal, such proposer will be given an opportunity to submit its views and any relevant information on the protest to the Solicitation Coordinator.

The final determination of the protest will:

- Find the protest lacking in merit and uphold the State Auditor's Office's action; or
- Find only technical or harmless errors in the State Auditor's Office's acquisition process and determine the State Auditor's Office to be in substantial compliance and reject the protest; or
- Find merit in the protest and provide State Auditor's Office options which may include:
 - Correct the errors and re-evaluate all proposals, and/or
 - Reissue the solicitation document and begin a new process, or
 - Make other findings and determine other courses of action as appropriate.

If the State Auditor's Office determines that the protest is without merit, the State Auditor's Office will enter into a contract with the apparent successful contractor. If the protest is determined to have merit, one of the alternatives noted in the preceding paragraph will be taken.

EXHIBIT A – CERTIFICATIONS AND ASSURANCES

I/we make the following certifications and assurances as a required element of the proposal to which it is attached, understanding that the truthfulness of the facts affirmed here and the continuing compliance with these requirements are conditions precedent to the award or continuation of the related contract(s):

1. I/we declare that all answers and statements made in the proposal are true and correct.
2. I/we certify that non-audit services have not been performed on behalf of state agencies or local governments in Washington State (see <http://www.gao.gov/govaud/iv2011gagas.pdf>) at any time during the previous **four years** by our firm or by any individual relative to this proposal.

Or

I/we are disclosing that non-audit services have been performed during the previous **four years** by our firm on behalf of state agencies or local governments in Washington State. I/we understand that additional assurances will be required related to the nature of the non-audit services provided to state agencies or local governments selected for inclusion in the audit to certify that I/we meet Government Auditing Standards 2018, General Standards for Independence.

Date	Audited Entity	Describe non-audit services provided	Audited entity contact

3. The contractor warrants that all persons performing work under this contract and any subcontracts are free from personal and external impairments to independence.
4. The prices and/or cost data have been determined independently, without consultation, communication, or agreement with others for the purpose of restricting competition. However, I/we may freely join with other persons or organizations for the purpose of presenting a single proposal.
5. The attached proposal is a firm offer for a period of 60 days following receipt, and it may be accepted by the State Auditor's Office without further negotiation (except where obviously required by lack of certainty in key terms) at any time within the 60-day period.
6. The project staff and subcontractors identified in Section III – Staffing will be assigned for the duration of the project. We agree that no substitutions or deletions of project personnel will occur without first requesting and the receiving approval, in writing, from the State Auditor's Office.
7. In preparing this proposal, I/we have not been assisted by any current or former employee of the State of Washington, or any current or former employee of a local government in the State of Washington, whose duties relate (or did relate) to this proposal or prospective contract, and who was assisting in other than his or her official, public capacity. Neither does such a person nor any member of his or her immediate family have any financial interest in the outcome of this proposal. (Any exceptions to these assurances are described in full detail on a separate page and attached to this document.)
8. I/we understand that the State Auditor's Office will not reimburse me/us for any costs incurred in the preparation of this proposal. All proposals become the property of the State Auditor's Office, and I/we claim no proprietary right to the ideas, writings, items, or samples, unless so stated in this proposal.
9. Unless otherwise required by law, the prices and/or cost data which have been submitted have not been knowingly disclosed by the proposer and will not knowingly be disclosed by him/her prior to submission, directly or indirectly to any other proposer or to any competitor.
10. I/we agree that submission of the attached proposal constitutes acceptance of the solicitation contents and the attached Special Terms and Conditions, and General Terms and Conditions. If there are any necessary exceptions to these terms, I/we have described those exceptions in detail on a page attached to this document.

11. No attempt has been made or will be made by the proposer to induce any other person or firm to submit or not to submit a proposal for the purpose of restricting competition.
12. I/we grant the State Auditor's Office the right to contact references and others, who may have pertinent information regarding the proposer's prior experience and ability to perform the services contemplated in this procurement.
13. Bidder Responsibility Criteria; Bidder certifies that Bidder has not, within the three-year period immediately preceding the date of release of this competitive solicitation, been determined by a final and binding citation and notice of assessment issued by the state of Washington Department of Labor and Industries or through a civil judgment to have willfully violated state minimum wage laws (RCW 49.48.082; Chapters 49.46 RCW, 49.48 RCW, or 49.52 RCW). Bidder attests under penalty of perjury that the foregoing statement is true and correct.
14. I/we identify the following firm principals as participants in the Washington State 2008 Early Retirement Factor Program...

PARTICIPANTS

☐ NO PARTICIPANTS

On behalf of the firm submitting this proposal, my name below attests to the accuracy of the above statements.

Signature of Proposer

Title

Date

EXHIBIT B – REFERENCE WORKSHEET**REFERENCE**

Type of Services Performed

Firm/Organization:

Reference Name:

Contact Person 1:

Contact 1 Phone #:

Fax #:

E-mail address:

Contact Person 2:

Contact 2 Phone #:

Fax #:

E-mail Address:

Type of Business:

Number of Employees at
Reference Business:Number of different business
locations supported:

EXHIBIT C – REQUIREMENTS CHECK LIST

Upon completion of the proposal verify the entire proposal conforms to the requirements outlined in Chapter 3 and that it is organized into seven sections:

- 1) Letter of Submittal (MR)/ (Pass/Fail)
- 2) Quotations (MR) (Scored) Cost Proposal
- 3) Qualifications (MR) (Scored)
- 4) Customer References (MR)/ (Pass/Fail)
- 5) Resumes (MR) (Scored)
- 6) Signed Certification and Assurances (Exhibit A) (MR)/ (Pass/Fail)
- 7) Sample Report (MR) (Scored)
- 8) State Auditor’s Office (SAO) Security Questionnaire (MR)
- 9) Signed Nondisclosure Agreement (Exhibit G), (MR)/ (Pass/Fail)
- 10) Procurement Evaluation for Executive Order 18-03 Certification Form (MR) (Scored)

Standard Instructions to Proposers	CHECK
Section I. Letter of Submittal (MR)/(Pass/Fail)	
A. Organization Summary	
B. Business Identification	
C. Company Officers	
D. Primary Contact	
E. Legal Status	
F. Previous State Contracts	
G. Former Employee Status	
H. Contract Termination	
I. Tax Information	
J. Compliance with Insurance Requirements	
Section II. Quotation Section (MR) (Scored) Cost Proposal	
A. Not-to-Exceed Hourly Price Quote	
B. Sample Agency Project Price Quote	
Section III. Qualifications Section (MR) (Scored)	
A. Firm Experience	
B. Staffing	
Section IV. Customer References (MR)/(Pass/Fail)	
Section V. Resumes (MR) (Scored)	
Section VI. Signed Certifications and Assurances (Exhibit A), (MR)/(Pass/Fail)	
Section VII. Sample Report, (MR) (Scored)	
Section VIII. State Auditor’s Office (SAO) Security Questionnaire (MR)/(Pass/Fail)	
Section IX. Signed Nondisclosure Agreement (Exhibit G), (MR)/(Pass/Fail)	
Section X. Procurement Evaluation for Executive Order 18-03 Certification Form (MR) (Scored)	

EXHIBIT D – SAMPLE CONTRACT FOR PROFESSIONAL SERVICES



Office of the Washington State Auditor

CONTRACT NO. [K###-C-YYMM]

CONTRACT FOR PROFESSIONAL SERVICES

BETWEEN

OFFICE OF THE WASHINGTON STATE

AND

[VENDOR NAME]

This Contract is made and entered into by and between the Washington STATE AUDITOR'S OFFICE and the below named CONTRACTOR.

[VENDOR NAME]

[Vendor Street Address]

[City, ST, Zip]

[Phone Number]

[Email or web address]

1. PURPOSE

The purpose of this contract is to conduct penetration testing by a subject matter expert as part of a Yellow Book performance audit that addresses the performance audit objective contained in Chapter 1.1.C of RFQQ No. K646-RFQQ-2011 in the manner specified in the final Performance Statement of Work within each Task Order.

2. SCOPE OF WORK

A. The contractor will provide services and staff, and otherwise do all things necessary for or incidental to the performance of work, as set forth each Performance Statement of Work, attached hereto and incorporated by reference. However, the State Auditor's Office reserves the right to modify the final Performance Statements of Work, including deleting tasks, after completing the planning process and at critical points during the course of the contract.

B. All written work of the contractor will be expected to be of a professional quality acceptable to the State Auditor's Office. In written reports, the contractor's findings and conclusions must be clearly documented as resulting from fieldwork and data analysis done for this audit. Recommendations must be logically related to the findings and conclusions and must recognize practical and fiscal constraints.

C. Attachment B, attached hereto and incorporated by reference, contains the General Terms and Conditions governing work to be performed under this contract, the nature of the working relationship between the State Auditor's Office and the contractor, and specific obligations of both parties.

3. PERIOD OF PERFORMANCE

The period of performance of any contract resulting from this RFQQ is tentatively scheduled to begin on or after [Date] or date of execution, whichever is later, and to end on or before [Date]. Task Orders will be issued for each engagement. Amendments extending the period of performance, if any, will be at the sole discretion of the State Auditor's Office. The State Auditor's Office reserves the right, at its discretion, to extend the contract for up to an additional three-year period.

Contract extensions may include extending the number of state agencies and/or local governments covered under the contract, as well as changes to the total contract value.

4. COMPENSATION

Total compensation payable to the contractor for satisfactory performance of the work under this contract will not exceed [\$Price]. The contractor's compensation for services rendered will be based on the schedule set forth in the budget. If the State Auditor's Office decides to modify the final Performance Statement of Work, including deleting tasks, after completing the planning process or at critical points during the course of the contract, the parties will negotiate in good faith whether to make an adjustment to the compensation set forth in the budget.

However, if the contractor violates the Government Auditing Standards independence standards during performance of the audit, the State Auditor's Office may choose not to compensate the contractor for work performed under this contract.

5. BILLING PROCEDURES AND PAYMENT

The State Auditor's Office will pay the contractor upon State Auditor's Office acceptance of services provided and receipt of properly completed invoices, which will be submitted to the Contract Manager in accordance with the schedule in the budget.

The invoices will describe and document, to the State Auditor's Office's satisfaction, an itemized description of the work performed and the progress of the audit by deliverable as compared to the final Performance Statement of Work, and fees. The invoice will include reference to Contract _____.

Payment will be considered timely if made by the State Auditor's Office within thirty (30) calendar days after receipt and acceptance of properly completed invoices. However, payment for each billing will be made after the State Auditor's Office's determination that it is satisfied with the overall progress of the

contractor and the quality of each deliverable. If the State Auditor's Office determines the contractor has not made satisfactory progress in accordance with the budget, the State Auditor's Office may, in its sole discretion, withhold payments or terminate the contract.

6. RETAINAGE

Ten percent of each payment will be withheld pending completion of each task order entered into under the Contract.

However, if the contractor violates the Government Auditing Standards independence standard during the conduct of the audit, the State Auditor's Office may choose not to compensate the contractor for any of the work performed under this contract.

7. NO ADVANCE PAYMENT

No payments in advance or in anticipation of services or supplies to be provided under this contract will be made by the State Auditor's Office.

8. CONTRACT MANAGEMENT

The Contract Manager for each of the parties will be the contact person for all communications and billings regarding the performance of this contract.

Contract Manager for the CONTRACTOR is:

Contract Manager Name

Contractor Name

Address

City, State Zip Code

Phone: () E-mail

address:

Contract Manager for the STATE AUDITOR'S OFFICE is:

State Auditor's Office Contract Coordinator

3200 Sunset Way SE

P.O Box 40031

Olympia, WA, 98504-0031

Phone: (564) 999-0941

E-mail address: contractmanager@sao.wa.gov

9. CONTRACTOR'S PERSONNEL

- A. State Auditor's Office reserves the right to reject any of the contractor's employees, or suppliers. Any and all costs or expenses associated with replacement of any person or entity will be borne by the contractor.

- B. State Auditor's Office may, in the exercise of its discretion and judgment, identify certain of the contractor's employees as key personnel, and if so, the contractor will take all necessary steps to assure that said contractor's employees are available and assigned to the work as long as said employees are employed by the contractor.
- C. The contractor may not change or replace any of the staff assigned to this contract without prior approval of State Auditor's Office, which approval will not be unreasonably withheld.
- D. The contractor warrants that it is available to perform the work within the time specified and that all work will be performed on a priority basis. The contractor will begin work promptly and will perform the work in a continuous and diligent manner, and contractor will not interrupt the work except as may be provided under this contract.
- E. The contractor will be responsible to ensure that all its employees are properly trained, certified, or licensed as appropriate and are properly qualified by education and experience to perform the work. The contractor will avoid overstaffing the work or shuffling personnel assigned to said work.
- F. The contractor and their employees agree not to recruit any personnel from the State Auditor's Office or from the audited entity for a period of 12 months after conclusion of the performance audit.
- G. Parties performing, or offering to perform, professional services under this contract who are CPAs or CPA firms licensed in this or other states and/or jurisdictions may become subject to the authority of the Washington State Board of Accountancy, RCW 18.04 and WAC 4-25 and must be in good standing with said Board.

Accordingly, parties to this contract who are licensed individual CPAs and/or licensed CPA firms:

Consent to the jurisdiction of the Washington State Board of Accountancy for matters referred by the State Auditor provided such matters are within the Board's authority, and in such cases, if the individual licensee(s) offering or performing professional services hereunder and the firm that employs such persons are not licensed in this state said persons simultaneously consent, to the appointment of the state board which issued the certificate or license as agent for service of process in any action or proceeding against said individual CPAs, CPA firm, or representatives of the CPA firm arising from any transaction or operation connected with or incidental to professional services under this contract.

10. COORDINATION AND COOPERATION

- A. The contractor will cooperate with the State Auditor's Office and other firms, if any, to ensure that the work is properly performed on schedule. Contractor will collaborate with any other firms and coordinate its work with the work of such other firm(s), if any, which could affect the work, the contractor will proceed in such manner as not to interfere or delay the progress of the work as a whole.
- B. If any part of the contractor's work depends for proper execution or results upon the work of any other contractor(s), the contractor will inspect and promptly report in writing to the State Auditor's Office any defects in the work of such other contractor that renders it unsuitable for such proper execution or results. Failure of the contractor to do so will constitute its acceptance of the other firm's work as fit and proper for the reception of contractor's work, except as to defects that may develop in the other firms' work after the execution of the contractor's work.
- C. In cases of disagreement or disputes between the contractor and other firm(s) which could delay or interfere with the work due to the failure to collaborate and cooperate or which cannot be resolved between contractor and the others involved, the State Auditor's Office will be given prompt written notice specifying in detail the disagreement or dispute. In such cases, the State Auditor's Office will have the right to determine the proper method of coordinating the work, and the State Auditor's Office's decisions in this regard will be final, binding, and conclusive.

D. Notwithstanding the existence of a dispute or disagreement between the State Auditor's Office and the contractor, the contractor will diligently and without interruption proceed with the work at such rates of progress as will ensure full completion of the work on time.

E. The contractor will accommodate the Audit Manager's monitoring and management of the contract by meeting weekly to discuss work progress and products as measured against the approved and final Performance Statement of Work. In these meetings, the contractor will communicate to the Audit Manager any issues or opportunities identified.

F. The contractor will assist the Audit Manager in his or her communication with the audited agency. The contractor will accompany the Audit Manager as needed to meet with agency personnel to discuss the status of the audit, pending request for assistance, understanding of audit matters, and to communicate any potential issues.

11. FRAUD, IRREGULARITIES, OR OTHER AUDIT ISSUES

If irregularities, fraud, or other significant audit issues, which may impact the audit, are suspected, the contractor must immediately notify the State Auditor's Office. The contractor will also notify State Auditor's Office of any other potential audit issues and topics that are discovered on a weekly basis as part of the weekly reporting process.

12. SUPERVISION AND COORDINATION

The contractor will:

- Comply with GAO Yellow Book requirements associated with the supervision of all employees in implementing and completing all audit requirements specified herein.
- Designate a representative(s) with the authority to legally commit the contractor's firm. All communications given or received from the contractor's representative will be binding on the contractor.
- Promote and offer to the State Auditor's Office only those services as stated herein and allowed for by contractual requirements. Violation of this condition will be grounds for contract termination.

Covid Protocol

- In the event contracted staff will be physically onsite with SAO or auditee staff, contracted staff will follow all SAO COVID 19 protocols. Specifically, contract staff may be required to wear a mask. Additionally, prior to entering any SAO or auditee location, each contracted staff may be required to complete an attestation health form to confirm the following:
 1. I am not experiencing any symptoms of COVID-19 such as fever, cough, shortness of breath, fatigue, muscle aches or body aches, headache, new loss of taste or smell, sore throat, congestion, nausea or vomiting, or diarrhea, that I CANNOT attribute to another health condition.
 2. In the last fourteen (14) days, I have not been within six (6) feet of anyone (including family members) with confirmed or suspected cases of COVID-19.
 3. Additionally, the contractor will contact the SAO Contract Manager within 24 hours if contracted staff test positive for COVID 19 within 14 days after the last day they were in close contact with SAO or auditee staff.

13. INSURANCE

The contractor will provide insurance coverage as set forth in the RFQQ No. K646-RFQQ-2011. The intent of the required insurance is to protect the state and local governments should there be any claims, suits, actions, costs, damages or expenses arising from any negligent or intentional act or omission of the contractor or its agents, while performing under the terms of this contract. The contractor will provide insurance coverage, which will be maintained in full force and effect during the term of this contract.

14. ASSURANCES

The State Auditor's Office and the contractor agree that all activity pursuant to this contract will be in accordance with all the applicable current federal and state laws, rules, and regulations.

15. ORDER OF PRECEDENCE

Each of the documents listed below is by this reference hereby incorporated into this contract. In the event of an inconsistency in this contract, the inconsistency will be resolved by giving precedence in the following order:

- Applicable federal and state of Washington statutes and regulations;
- The terms of the basic contract and all attachments incorporated herein including
 - Special Terms and Conditions as contained in this basic contract instrument;
 - Attachment A – General Terms and Conditions;
 - Attachment B – Task Order
- RFQQ K646-RFQQ-2011
- The contractor's proposal dated _____, and
- Any other provision, term or material incorporated herein by reference or otherwise incorporated.

16. ENTIRE AGREEMENT

This contract, including referenced attachments and other documents, represents all the terms and conditions agreed upon by the parties. No other statements or representations, written or oral, will be deemed a part hereof.

If any provision of this contract violates any statute or rule of law of the state of Washington, it is considered modified to conform to that statute or rule of law.

17. APPROVAL

This contract will be subject to the written approval of the State Auditor's Office's authorized representative and will not be binding until so approved. The contract may be altered, amended, or waived only by a written amendment executed by both parties.

THIS CONTRACT is executed by the persons signing below, who warrant they have the authority to execute the contract.

[VENDOR NAME]

STATE AUDITOR'S OFFICE

Signature: _____

Signature: _____

Date: _____

Date: _____

Name/Title: _____

Name/Title: _____

APPROVED AS TO FORM:

Assistant Attorney General

Date

ATTACHMENT A – GENERAL TERMS AND CONDITIONS

1. Definitions

As used throughout this contract, the following terms shall have the meaning set forth below:

- A. “State Auditor’s Office” (SAO) shall mean any division, section, office, unit or other entity of the State Auditor’s Office, or any of the officers or other officials lawfully representing the State Auditor’s Office.
- B. “Agent” shall mean the State Auditor’s Office Contract Manager, and/or the delegate authorized in writing to act on the Manager’s behalf.
- C. “Contractor” shall mean that firm, provider, organization, individual or other entity performing service(s) under this contract, and shall include all employees of the contractor.
- D. “Subcontractor” shall mean one not in the employment of the contractor, who is performing all or part of those services under this contract under a separate contract with the contractor. The terms “subcontractor” and “subcontractors” means subcontractor(s) in any tier.

2. Access to Data

In compliance with RCW 39.26.180 the contractor shall provide access to data generated under this contract to the State Auditor’s Office at no additional cost.

3. Advance Payments Prohibited

No payments in advance of or in anticipation of goods or services to be provided under this contract shall be made by the State Auditor’s Office.

4. Amendments

This contract may be amended by mutual agreement of the parties. Such amendments shall not be binding unless they are in writing and signed by personnel authorized to bind each of the parties.

5. Americans with Disabilities Act (ADA) of 1990, Public Law 101-336, 28 CFR Part 35

The contractor must comply with the ADA, which provides comprehensive civil rights protection to individuals with disabilities in the areas of employment, public accommodations, state and local government services, and telecommunications.

6. Assignment

Neither this contract, nor any claim arising under this contract, shall be transferred or assigned by the contractor without prior written consent of the State Auditor’s Office.

7. Attorneys’ Fees

In the event of litigation or other action brought to enforce contract terms, each party agrees to bear its own attorney fees and costs.

8. Confidentiality/Safeguarding of Information

Contractor acknowledges that some of the material and information that may come into its possession or knowledge in connection with this contract or its performance may consist of information that is exempt from disclosure to the public or other unauthorized persons under either chapter 42.56 RCW or other state or federal statutes (“Confidential Information”).

The contractor will not use or disclose any information concerning the State Auditor’s Office, information which may be classified as confidential, for any purpose not directly connected with the administration of this contract, except with prior written consent of the State Auditor’s Office, or as may be required for peer review or by law, legal process, or AICPA Consulting Standards.

Confidential information may include, but is not limited to, proprietary processes or modeling used by a utility's third-party consultant to develop its Conservation Potential Assessment supporting the biennial conservation target, utility customer, or utility or SAO employee information such as residential addresses, e-mail addresses, and telephone numbers, Social Security Numbers, financial profiles, credit card information, driver's license numbers, medical data or protected health information, law enforcement records, agency source code or object code, or agency security data.

Contractor agrees to implement physical, electronic, and managerial safeguards to prevent unauthorized access to Confidential Information.

Immediately upon expiration or termination of this contract, contractor will destroyed all information including Confidential Information not required to be retained by professional standards.

Any breach of this provision may result in termination of the contract and the demand for return of all Confidential Information. The contractor agrees to indemnify and hold harmless the State Auditor's Office for any damages related to the contractor's unauthorized use of confidential information.

All documents received by the SAO and used or retained under this contract are public records. The SAO will release these documents as required by the Public Records Act, Chapter 42.56 RCW, or other process of law.

9. Conflict Of Interest

The State Auditor's Office may, in its sole discretion, by written notice to the contractor terminate this contract if it is found after due notice and examination by the State Auditor's Office that there is a violation of RCW 42.52, Ethics in Public Service.

10. Copyright Provisions

Unless otherwise provided, all materials produced under this contract shall be considered "works for hire" as defined by the U.S. Copyright Act and shall be owned by the State Auditor's Office. The State Auditor's Office shall be considered the author of such materials. In the event the materials are not considered "works for hire" under the U.S. Copyright laws, contractor hereby irrevocably assigns all right, title, and interest in materials, including all intellectual property rights, to the State Auditor's Office effective from the moment of creation of such materials.

Materials means all items in any format and includes, but is not limited to, data, reports, documents, pamphlets, advertisements, books, magazines, surveys, studies, computer programs, films, tapes, and/or sound reproductions. Ownership includes the right to copyright, patent, register and the ability to transfer these rights.

For materials that are delivered under the contract, but that incorporate pre-existing materials not produced under the contract, contractor hereby grants to the State Auditor's Office a nonexclusive, royalty-free, irrevocable license (with rights to sublicense others) in such materials to translate, reproduce, distribute, prepare derivative works, publicly perform, and publicly display. The contractor warrants and represents that contractor has all rights and permissions, including intellectual property rights, moral rights and rights of publicity, necessary to grant such a license to the State Auditor's Office. The contractor will maintain its ownership of its pre-existing materials, such as methodologies, including any improvements or enhancements the contractor makes to its pre-existing materials.

The State Auditor's Office recognizes that: (A) valuable formulae, designs, drawings, and research data obtained by the State Auditor's Office within five years of the request for disclosure are exempt from disclosure when disclosure would produce private gain and public loss (RCW 42.56.270(1)); and (B) intellectual property and proprietary information may also be covered by the Washington Trade Secrets Act, chapter 19.108 RCW.

Where a request for documents potentially protected under these laws is made, the State Auditor's Office shall notify the contractor that the request has been made and provide the Contractor an opportunity to seek a court injunction against the requested disclosure. The Contractor will have five (5) business days to respond to the State Auditor's Office's notice with its intent to seek a court injunction against the requested disclosure. If the State Auditor's Office receives no response from

the Contractor within five (5) business days, the materials and information will be released consistent with the State Auditor's Office policies and procedures under State law. Once notified of the contractor's intent to seek a court injunction, the contractor shall have ten (10) business days to obtain an injunction and provide a copy to the State Auditor's Office. If the State Auditor's Office does not receive a copy of an injunction within these ten (10) business day, it may release the requested documents.

Contractor shall exert all reasonable effort to advise the State Auditor's Office at the time of delivery of all known or potential copyright provisions or intellectual property or proprietary information protections applicable to any document or portion of any document produced in the performance of this contract. Contractor may mark any documents furnished to the State Auditor's Office as follows:

NOTICE: The information herein has been prepared for the use of the State Auditor's Office and no others. The information contains data that is copyrighted by © _____, all rights reserved, or may be subject to intellectual property or proprietary information protections.

Nothing contained in this section affects or modifies the State Auditor's Office obligation to disclose public records under Chapter 42.56 RCW or other applicable law.

The contractor shall exert all reasonable effort to advise the State Auditor's Office, at the time of delivery of materials furnished under this contract, of all known or potential invasions of privacy contained therein and of any portion of such document that was not produced in the performance of this contract.

The State Auditor's Office shall receive prompt written notice of each notice or claim of infringement received by the contractor with respect to any data delivered under this contract. The State Auditor's Office shall have the right to modify or remove any restrictive markings placed upon the data by the contractor.

11. Covenant Against Contingent Fees

The contractor warrants that no person or selling agent has been employed or retained to solicit or secure this contract upon an agreement or understanding for a commission, percentage, brokerage or contingent fee, excepting bona fide employees or bona fide established agents maintained by the contractor for securing business.

The State Auditor's Office shall have the right, in the event of breach of this clause by the contractor, to annul this contract without liability or, in its discretion, to deduct from the contract price or consideration or recover by other means the full amount of such commission, percentage, brokerage or contingent fee.

12. Disallowed Costs

The contractor is responsible for any audit exceptions or disallowed costs incurred by its own organization or that of its subcontractors.

13. Disputes

Except as otherwise provided in this contract, when a dispute arises between the parties and it cannot be resolved, either party may request a dispute hearing with a team of three (which shall be comprised of one independent individual selected by the contractor, one independent individual selected by the State Auditor's Office Director of Audit, and one shall be a State Auditor's Office Director not responsible for the contract.) Disputes shall be resolved as quickly as possible.

The request for a dispute hearing must:

- A. Be in writing;
- B. State the disputed issue(s);
- C. State the relative positions of the parties;
- D. State the contractor's name, address, and contract number; and
- E. Be mailed or sent electronically to the State Auditor's Office Contract Manager within 3 working days after the parties agree that they cannot resolve the dispute.

The Contract Manager shall send a written answer to the contractor's statement to the contractor within 5 working days.

The panel shall review the written statements and reply in writing to both parties within 10 working days. The panel may extend this period if necessary by notifying the parties.

The parties agree that this dispute process shall precede any action in a judicial or quasi-judicial tribunal.

The State Auditor's Office and contractor agree that, the existence of a dispute notwithstanding, they will continue without delay to carry out all their respective responsibilities under this contract, which are not affected by the dispute. Both parties agree to exercise good faith in the dispute resolution and to settle disputes prior to using the dispute resolution panel whenever possible.

14. Duplicate Payment

The State Auditor's Office shall not pay the contractor, if the contractor has charged or will charge the State of Washington or any other party under any other contract or agreement, for the same services or expenses.

15. Force Majeure

Neither party will incur any liability to the other if its performance of any obligation under this agreement is prevented or delayed by causes beyond its control and without the fault or negligence of either party. Causes beyond a party's control may include, but are not limited to, acts of God or war, changes in controlling law, regulations, orders or the requirements of any governmental entity, natural disasters, fire, epidemics and quarantines. Each party shall notify the other orally within five (5) days and in writing within ten (10) days of the date on which the party becomes aware, or should have reasonably become aware, that such cause would prevent or delay its performance under the agreement. Such notification shall (i) describe fully such cause(s) and its effect on performance, (ii) state whether performance is prevented or delayed and (iii) if performance is delayed, state a reasonable estimate of the duration of the delay. The party claiming force majeure shall have the burden of proving that such cause(s) delayed or prevented its performance despite its diligent efforts to perform and shall produce such supporting documentation as the other party may reasonably request.

16. Governing Law

This contract shall be construed and interpreted in accordance with the laws of the State of Washington, and the venue of any action brought hereunder shall be in the Superior Court for Thurston County.

17. Indemnification

To the fullest extent permitted by law, the contractor shall indemnify, defend, and hold harmless state, agencies of state and all officials, agents and employees of state, from and against all claims for injuries or death arising out of or resulting from the performance of the contract.

"Claim," as used in this contract, means any financial loss, claim, suit, action, damage, or expense, including but not limited to attorney's fees, attributable for bodily injury, sickness, disease, or death, or injury to or destruction of tangible property including loss of use resulting there from. The contractors' obligations to indemnify, defend, and hold harmless includes any claim by the contractors' agents, employees, representatives, or any subcontractor or its employees.

The contractor expressly agrees to indemnify, defend and hold harmless the State for any claim arising out of or incident to the contractor's or any subcontractor's performance or failure to perform the contract. The contractor's obligation to indemnify, defend, and hold harmless the state shall not be eliminated or reduced by any actual or alleged concurrent negligence of the State or its agents, agencies, employees and officials.

The contractor waives its immunity under Title 51 RCW to the extent it is required to indemnify, defend and hold harmless the state and its agencies, officials, agents or employees.

18. Independent Capacity of the Contractor

The parties intend that an independent contractor relationship will be created by this contract. The contractor and his or her employees or agents performing under this contract are not employees or agents of the State Auditor's Office. The contractor will not hold himself/herself out as or claim to be an officer or employee of the State Auditor's Office or of the State of Washington by reason hereof, nor will the contractor make any claim of right, privilege or benefit that would accrue to such employee under law. Conduct and control of the work will be solely with the contractor.

19. Industrial Insurance Coverage

The contractor shall comply with the provisions of Title 51 RCW, Industrial Insurance. If the contractor fails to provide industrial insurance coverage or fails to pay premiums or penalties on behalf of its employees, as may be required by law, the State Auditor's Office may collect from the contractor the full amount payable to the Industrial Insurance accident fund. The State Auditor's Office may deduct the amount owed by the contractor to the accident fund from the amount payable to the contractor by the State Auditor's Office under this contract, and transmit the deducted amount to the Department of Labor and Industries, (L&I) Division of Insurance Services. This provision does not waive any of L&I's right to collect from the contractor.

20. Licensing, Accreditation and Registration

The contractor shall comply with all applicable local, state and federal licensing, accreditation and registration requirements/standards, necessary for the performance of this contract.

21. Limitation of Authority

Only the Agent or Agent's delegate by writing (delegation to be made prior to action) shall have the express, implied, or apparent authority to alter, amend, modify, or waive any clause or condition of this contract. Furthermore, any alteration, amendment, modification, or waiver or any clause or condition of this contract is not effective or binding unless made in writing and signed by the Agent.

22. Noncompliance with Nondiscrimination Laws

In the event of the contractor's non-compliance or refusal to comply with any nondiscrimination law, regulation or policy, this contract may be rescinded, canceled or terminated in whole or in part, and the contractor may be declared ineligible for further contracts with the State Auditor's Office. The contractor shall, however, be given a reasonable time in which to cure this noncompliance. Any dispute may be resolved in accordance with the "Disputes" procedure set forth herein.

23. Nondiscrimination

During the performance of this contract, the contractor shall comply with all federal and state nondiscrimination laws, regulations and policies.

24. Publicity

The contractor agrees to submit to the State Auditor's Office all advertising and publicity matters relating to this contract wherein the State Auditor's Office's name is mentioned or language used from which the connection of the State Auditor's Office's name may, in the State Auditor's Office's judgment, be inferred or implied. The contractor agrees not to publish or use such advertising and publicity matters without the prior written consent of the State Auditor's Office.

25. Records Maintenance

The contractor shall maintain books, records, documents, data and other evidence relating to this contract and performance of the services described herein, including but not limited to accounting procedures and practices that sufficiently and properly reflect all direct and indirect costs of any nature expended in the performance of this contract.

Contractor shall retain such records for a period of six years following the date of final payment. At no additional cost, these records, including materials generated under the contract, shall be subject at all reasonable times to inspection, review or audit by the State Auditor's Office, personnel duly authorized by the State Auditor's Office, and federal and state officials so authorized by law, regulation or agreement. If any litigation, claim or audit is started before the expiration of the six (6)

year period, the records shall be retained until all litigation, claims or audit findings involving the records have been resolved.

26. Registration with Department of Revenue

The contractor shall complete registration with the Washington State Department of Revenue and be responsible for payment of all taxes due on payments made under this contract.

27. Right of Inspection

The contractor shall provide right of access to its facilities to the State Auditor's Office, or any of its officers, or to any other authorized agent or official of the State of Washington or the federal government, at all reasonable times, in order to monitor and evaluate performance, compliance, and/or quality assurance of the work performed.

28. Savings

In the event funding from state, federal, or other sources is withdrawn, reduced, or limited in any way after the effective date of this contract and prior to normal completion, the State Auditor's Office may terminate the contract under the "Termination for Convenience" clause, without the ten day notice requirement, subject to renegotiation at the State Auditor's Office's discretion under those new funding limitations and conditions.

29. Severability

The provisions of this contract are intended to be severable. If any term or provision is illegal or invalid for any reason whatsoever, such illegality or invalidity shall not affect the validity of the remainder of the contract.

30. Site Security

While on the State Auditor's Office premises, contractor, its agents, employees or subcontractors shall conform in all respects with physical, fire or other security policies or regulations.

31. Subcontracting

Neither the contractor nor any subcontractor shall enter into subcontracts for any of the work contemplated under this contract without obtaining prior written approval of the State Auditor's Office. In no event shall the existence of the subcontract operate to release or reduce the liability of the contractor to the State Auditor's Office for any breach in the performance of the contractor's duties. This clause does not include contracts of employment between the contractor and personnel assigned to work under this contract.

The contractor is solely responsible and liable for ensuring that all of the terms, conditions, assurances and certifications set forth in this contract are incorporated into any partnering or subcontracting relationships with other entities for work related to this contract. Liability includes management responsibility and quality assurance for work performed and financial responsibility for payments to and by partner organizations or subcontractor to others. Contractor and its subcontractors agree not to release, divulge, publish, transfer, sell or otherwise make known to information obtained during performance of this contract without the express written consent of the State Auditor's Office or as provided by law.

32. Taxes

All payments accrued because of payroll taxes, unemployment contributions, any other taxes, insurance or other expenses for the contractor or its staff shall be the sole responsibility of the contractor.

33. Termination for Cause

In the event the State Auditor's Office determines the contractor has failed to comply with the conditions of this contract in a timely manner, the State Auditor's Office has the right to suspend or terminate this contract. Before suspending or terminating the contract, the State Auditor's Office shall notify the contractor in writing of the need to take corrective action. If corrective action is not taken within 30 calendar days, the contract may be terminated or suspended.

In the event of termination or suspension, the contractor shall be liable for damages as authorized by law including, but not limited to, any cost difference between the original contract and the replacement or cover contract and all administrative costs directly related to the replacement contract, e.g., cost of the competitive bidding, mailing, advertising and staff time.

The State Auditor's Office reserves the right to suspend all or part of the contract, withhold further payments, or prohibit the contractor from incurring additional obligations of funds during investigation of the alleged compliance breach and pending corrective action by the contractor or a decision by the State Auditor's Office to terminate the contract. A termination shall be deemed a "Termination for Convenience" if it is determined that the contractor: (1) was not in default; or (2) failure to perform was outside of his or her control, fault or negligence. The rights and remedies of the State Auditor's Office provided in this contract are not exclusive and are, in addition to any other rights and remedies, provided by law.

34. Termination for Convenience

Except as otherwise provided in this contract, the State Auditor's Office may, by 10 calendar days written notice, beginning on the second day after the mailing, terminate this contract, in whole or in part. If this contract is so terminated, the State Auditor's Office shall be liable only for payment required under the terms of this contract for services rendered or goods delivered prior to the effective date of termination.

35. Termination Procedures

Upon termination of this contract, the State Auditor's Office, in addition to any other rights provided in this contract, may require the contractor to deliver to the State Auditor's Office any property specifically produced or acquired for the performance of such part of this contract as has been terminated. The provisions of the "Treatment of Assets" clause shall apply in such property transfer.

The State Auditor's Office shall pay to the contractor the agreed upon price, if separately stated, for completed work and services accepted by the State Auditor's Office, and the amount agreed upon by the contractor and the State Auditor's Office for (i) completed work and services for which no separate price is stated, (ii) partially completed work and services, (iii) other property or services that are accepted by the State Auditor's Office, and (iv) the protection and preservation of property, unless the termination is for default, in which case the agent shall determine the extent of the liability of the State Auditor's Office. Failure to agree with such determination shall be a dispute within the meaning of the "Disputes" clause of this contract.

The State Auditor's Office may withhold from any amounts due the contractor such sum as the agent determines to be necessary to protect the State Auditor's Office against potential loss or liability. The rights and remedies of the State Auditor's Office provided in this section shall not be exclusive and are in addition to any other rights and remedies provided by law or under this contract.

After receipt of a notice of termination, and except as otherwise directed by the agent, the contractor shall:

- A. Stop work under the contract on the date, and to the extent specified, in the notice;
- B. Place no further orders or subcontracts for materials, services, or facilities except as may be necessary for completion of such portion of the work under the contract that is not terminated;
- C. Assign to the State Auditor's Office, in the manner, at the times, and to the extent directed by the agent, all of the rights, title, and interest of the contractor under the orders and subcontracts so terminated, in which case the State Auditor's Office has the right, at its discretion, to settle or pay any or all claims arising out of the termination of such orders and subcontracts;
- D. Settle all outstanding liabilities and all claims arising out of such termination of orders and subcontracts, with the approval or ratification of the agent to the extent agent may require, which approval or ratification shall be final for all the purposes of this clause;

- E. Transfer title to the State Auditor's Office and deliver in the manner, at the times, and to the extent directed by the agent any property which, if the contract had been completed, would have been required to be furnished to the State Auditor's Office;
- F. Complete performance of such part of the work as shall not have been terminated by the agent; and
- G. Take such action as may be necessary, or as the agent may direct, for the protection and preservation of the property related to this contract, which is in the possession of the contractor and in which the State Auditor's Office has or may acquire an interest.

36. Treatment of Assets

- A. Title to all property furnished by the State Auditor's Office shall remain in the State Auditor's Office. Title to all property furnished by the contractor, for the cost of which the contractor is entitled to be reimbursed as a direct item of cost under this contract, shall pass to and vest in the State Auditor's Office upon delivery of such property by the contractor. Title to other property, the cost of which is reimbursable to the contractor under this contract, shall pass to and vest in the State Auditor's Office upon (i) issuance for use of such property in the performance of this contract, or (ii) commencement of use of such property in the performance of this contract, or (iii) reimbursement of the cost thereof by the State Auditor's Office in whole or in part, whichever first occurs.
- B. Any property of the State Auditor's Office furnished to the contractor shall, unless otherwise provided herein or approved by the State Auditor's Office, be used only for the performance of this contract.
- C. The contractor shall be responsible for any loss or damage to property of the State Auditor's Office that results from the negligence of the contractor or that results from the failure on the part of the contractor to maintain and administer that property in accordance with sound management practices.
- D. If any the State Auditor's Office's property is lost, destroyed or damaged, the contractor shall immediately notify the State Auditor's Office and shall take all reasonable steps to protect the property from further damage.
- E. The contractor shall surrender to the State Auditor's Office all property of the State Auditor's Office prior to settlement upon completion, termination or cancellation of this contract.
- F. All reference to the contractor under this clause shall also include contractor's employees, agents or subcontractors.

ATTACHMENT B – SAMPLE TASK ORDER

TASK ORDER OFFICE OF THE WASHINGTON STATE AUDITOR (SAO)		<u>Task Order #</u>	<u>Contract #</u>	
		<u>Type of Services</u>	<u>Date Issued</u>	
		Subject Matter Expertise		
Title: Security Assessment Services		Contractor:		
This Task Order is issued under the provisions of an SAO agreement. The services authorized are within the scope of services set forth in the <i>Purpose</i> of the contract. All rights and obligations of the parties shall be subject to and governed by the terms of the contract, including any subsequent modifications, which are hereby incorporated by reference.				
Purpose Security Assessment Services:				
Statement of Tasks/Objectives and Deliverables: 1. Objectives: 2. Deliverables: Deliverables are subject to review and approval by SAO prior to payment. Approval and payment of deliverables will indicate acceptance of complete deliverables.				
Start Date	x/x/20xx (or upon execution of this agreement)	End Date	x/x/20xx	
<u>Budget</u>				
Description / Task		Est. Hours	Unit Cost	Total
SAO shall pay an amount up to but not to exceed				
Contractor's Approval		State Auditor's Office Approval		
_____ (Signature) Authorized Representative (Date) Name: Title:		_____ (Signature) SAO Authorized Representative (Date) Name: Title:		
T/O Manager		T/O Manager		
Telephone No.		Telephone No.		
Email:		Email:		

ATTACHMENT C - Sample – DATA SHARING ADDENDUM

This Data Sharing Addendum is executed by and between the State Auditor’s Office (SAO) and Contractor name this _____ day of Date (“Addendum”) and amends and supplements the Contract NO. _____ (“Agreement”) to define the data handling requirements associated with the Service provided by CONTRACTOR NAME and is otherwise subject to all terms and conditions of the Agreement.

PURPOSE OF THE ADDENDUM

The purpose of this Addendum is to allow CONTRACTOR NAME, a contractor working for the State Auditor’s Office, to access information technology infrastructure and computer security information from state agencies and local governments for the purpose of conducting IT Security testing in accordance with Contract NO. _____.

DEFINITIONS

“state agencies” shall mean those state agencies specifically identified as assessment targets by SAO in the rules of engagement documents in connection with contract no. _____

“local governments” shall mean those local governments specifically identified as assessment targets by SAO in the rules of engagement documents in connection with contract no. _____

“Data Encryption” refers to ciphers, algorithms or other encoding mechanisms that will encode data to protect its confidentiality. Data encryption can be required during data transmission or data storage depending on the level of protection required for this data.

“Data Storage” refers to the state data is in when at rest. Data shall be stored on secured environments.

“Data Transmission” refers to the methods and technologies to be used to move a copy of the data between systems, networks, and/or workstations.

“Disclosure” means to permit access to or release, transfer, or other communication of personally identifiable information contained in education or employment records by any means including oral, written, or electronic means, to any party except the party identified or the party that provided or created the record (34 CFR 99.3).

“Rules of Engagement” means the document developed and approved by SAO and the state agency or local government subject to security testing to define the terms of security testing conducted by CONTRACTOR NAME. A separate rules of engagement document will be developed for each state agency or local government.

“Washington State Office of the Chief Information Officer’s information technology security standards” refers to standards under 141.10 – Securing Information Technology Assets Standards, which all state agencies are required to follow per RCW 43.41A.027. The standards are found at this link <https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets>.

DESCRIPTION OF DATA TO BE SHARED

In the course of conducting security testing CONTRACTOR NAME may discover information regarding state agency and/or local government IT infrastructure and security of computer and telecommunications systems. This is classified as Category 3, confidential information, as described by the Washington State Office of the Chief Information Officer's Information Technology Security Standards, 141.10. section 4.1 Data classification.

DATA TRANSMISSION

To ensure data is encrypted during data transmission, all data transfers to/from CONTRACTOR NAME shall be transmitted using the State Auditor's Office secure FTP Service with login and hardened password security or other SAO approved secure method that complies with OCIO standard 141.10.

DATA SECURITY

All IT security information provided by state agencies and/or local governments shall be stored on a secure environment with access limited to the least number of staff needed to complete the IT security work under contract.

1. Protection of Data

CONTRACTOR NAME agrees to store data on one or more of the following media and protect the data as described:

1) Workstation Hard disk drives. Data stored on local workstation hard disks. Access to the data will be restricted to authorized users by requiring logon to the local workstation using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. The workstation hard drive must be full-disk encrypted to protect state agency and/or local government data in the event the device is stolen.

2) Data stored on hard disks mounted on network servers or in a 'cloud' environment. Access to the data will be restricted to authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism. Backup copies for data recovery purposes must be encrypted if recorded to removable media.

3) Optical discs (e.g. CDs, DVDs, Blu-Rays) in local workstation optical disc drives. Data provided by SAO or the state agencies and/or local governments on optical discs which will be used in local workstation optical disc drives and which will not be transported out of a secure area. When not in use for the Agreement purpose, such discs must be locked in a drawer, cabinet or other container to which only authorized users have the key, combination or mechanism required to access the contents of the container. Workstations which access state agency and/or local government data on optical discs must be located in an area which is accessible only to authorized individuals, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

4) Paper documents. Any paper records must be protected by storing the records in a secure area which is only accessible to authorized individuals. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

5) Access via remote terminal/workstation over the Public Internet is permitted only in accordance with provisions outlined in the rules of engagement document approved for each state agency and/or local government subject to testing.

6) Data storage on portable devices or media.

a) When state agency and/or local government data is stored by CONTRACTOR NAME on portable devices, the data shall be given the following protections:

- i. Encrypt the data with a key length of at least 256 bits
- ii. Control access to devices with a unique user ID and password or stronger authentication method such as a physical token or biometrics.
- iii. Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.
- iv. Physically protect the portable device(s) and/or media by:
 - Keeping them in locked storage when not in use;
 - Using check-in/check-out procedures when they are shared; and
 - Taking frequent inventories.

b) When being transported outside of a secure area, portable devices and media with confidential state agency and/or local government data must be under the physical control of CONTRACTOR NAME staff with authorization to access the data.

c) Portable devices include, but are not limited to; handhelds/PDAs, Ultramobile PCs, flash memory devices (e.g. USB flash drives, personal media players), portable hard disks, and laptop/notebook computers, and smart phones.

d) Portable media includes, but is not limited to; optical media (e.g. CDs, DVDs, Blu-Rays), magnetic media (e.g. floppy disks, tape, Zip or Jaz disks), or flash media (e.g. CompactFlash, SD, MMC).

2. Safeguards Against Unauthorized Access and Re-disclosure

CONTRACTOR NAME shall exercise due care to protect all Personally Identifiable information from unauthorized physical and electronic access. THE CONTRACTOR shall establish and implement the following minimum administrative, technical and physical safeguards for maintaining the confidentiality, availability and integrity of information provided by either party pursuant to this Agreement:

- 1) Access to the information provided by agencies will be restricted to only those authorized staff, officials, and agents of the parties who need it to perform their official duties in the performance of the work requiring access to the information as detailed in the purpose of this Agreement.
- 2) CONTRACTOR NAME will store the information in an area that is safe from access by unauthorized persons during duty hours as well as non-duty hours or when not in use.
- 3) CONTRACTOR NAME will protect the information in a manner that prevents unauthorized persons from retrieving the information by means of computer, remote terminal or other means.

4) CONTRACTOR NAME shall take precautions to ensure that only authorized personnel and agents are given access to on-line files containing confidential or sensitive data.

5) CONTRACTOR NAME shall instruct all individuals with access to the Personally Identifiable Information regarding the confidential nature of the information, the requirements of Use of Data and Safeguards Against Unauthorized Access and Re-Disclosure clauses of this Addendum, and the sanctions specified in federal and state laws against unauthorized disclosure of information covered by this Addendum.

6) CONTRACTOR NAME shall take due care and take reasonable precautions to protect state agency and/or local government data from unauthorized physical and electronic access. Both parties will strive to meet or exceed the requirements of the State of Washington's policies and standards for data security and access controls to ensure the confidentiality, availability, and integrity of all data accessed.

3. Data Segregation

1) State agency and/or local government data must be segregated or otherwise distinguishable from non-state agency and/or non-local government data. This is to ensure that when no longer needed by CONTRACTOR NAME, all state agency and/or local government data can be identified for return or destruction. It also aids in determining whether state agency and/or local government data has or may have been compromised in the event of a security breach.

2) State agency and/or local government data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-state agency and/or non-local government data. Or,

3) State agency and/or local government data will be stored in a logical container on electronic media, such as a partition or folder dedicated to state agency and/or local government data. Or,

4) State agency and/or local government data will be stored in a database which will contain no non-state agency and/or non-local government data. Or,

5) State agency and/or local government data will be stored within a database and will be distinguishable from non-state agency and/or non-local government data by the value of a specific field or fields within database records. Or,

6) When stored as physical paper documents, state agency and/or local government data will be physically segregated from non-state agency and/or non-local government data in a drawer, folder, or other container.

7) When it is not feasible or practical to segregate state agency and/or local government data from non-state agency and/or non-local government data, then both the state agency and/or local government data and the non-state agency and/or non-local government data with which it is commingled must be protected as described in this Addendum.

If CONTRACTOR NAME or its agents detect a compromise or potential compromise in the IT security for this data such that confidential information may have been accessed or disclosed without proper authorization, CONTRACTOR NAME shall give notice to SAO within one (1) business day of discovering the compromise or potential compromise. SAO will then notify the affected state agency and/or local government from where the data originated.

4. Non-Disclosure of Data

1) Individuals will access data gained by reason of this Agreement only for the purpose of this Agreement. Section 8 of the General Terms and Conditions of this contract include requirements for the handling of confidential information and require CONTRACTOR NAME to sign a non-disclosure agreement, see Exhibit G.

2) SAO may at its discretion disqualify at any time any person authorized access to confidential information by or pursuant to this Agreement. Notice of disqualification shall be in writing and shall terminate a disqualified person's access to any information provided by SAO pursuant to this Agreement immediately upon delivery of notice to CONTRACTOR NAME. Disqualification of one or more persons by SAO does not affect other persons authorized by or pursuant to this Agreement.

USE OF DATA

1. Data provided by the state agencies and/or local governments will remain the property of the state agencies and/or local governments and will be returned to the state agencies and/or local governments or destroyed when the work for which the information was required has been completed.
2. This Agreement does not constitute a release of the data for CONTRACTOR NAME's discretionary use, but may be accessed only to carry out the responsibilities specified herein. Any ad hoc analyses or other use of the data, not specified in this Agreement, is not permitted without the prior written agreement of SAO. CONTRACTOR NAME shall not disclose, transfer, or sell any such information to any party, except as provided by law. CONTRACTOR NAME shall maintain the confidentiality of all Personally Identifiable Information and other information gained by reason of this Agreement.
3. CONTRACTOR NAME is not authorized to update or change any state agencies' and/or local governments' data, and any updates or changes shall be cause for immediate termination of this Agreement.
4. Neither Washington State nor the agencies or local governments guarantee the accuracy of the data provided. All risk and liabilities of use and misuse of information provided pursuant to this Agreement are understood and assumed by CONTRACTOR NAME.
5. Data provided by state agencies and/or local governments cannot be linked with other data or data sets as a way to determine the identity of individuals or employers; the data in any data set shall be used for statistical purposes only.
6. Data provided by the state agencies and/or local governments cannot be re-disclosed or duplicated unless specifically authorized in this Agreement.
7. The requirements in this section shall survive the termination or expiration of this Addendum or any subsequent agreement intended to supersede this Addendum.

DISPOSITION OF DATA

a. Upon termination of the agreement, or when directed by the SAO audit manager, CONTRACTOR NAME shall dispose of the data received and provide written notification of disposal. Failure to do so may prevent data sharing agreements with the organization in the future.

b. Upon the destruction of State agencies' and/or local governments' data, CONTRACTOR NAME shall certify the disposition, and the process used to dispose of the data, and submit it to SAO within fifteen (15) days of the date of disposal.

c. Acceptable destruction methods for various types of media include:

- 1) For paper documents containing confidential or sensitive information, a contract with a recycling firm to recycle confidential documents is acceptable, provided the contract ensures that the confidentiality of the data will be protected. Such documents may also be destroyed by on-site shredding, pulping, or incineration.
- 2) For paper documents containing Confidential Information requiring special handling, recycling is not an option. These documents must be destroyed by on-site shredding, pulping, or incineration.
- 3) If confidential or sensitive information has been contained on optical discs (e.g. CDs, DVDs, Blu-ray), the data recipient shall either destroy by incineration the disc(s), shredding the discs, or completely deface the readable surface with a coarse abrasive.
- 4) If confidential or sensitive information has been stored on magnetic tape(s), the data recipient shall destroy the data by degaussing, incinerating or crosscut shredding.
- 5) If data has been stored on server or workstation data hard drives or similar media, the data recipient shall destroy the data by using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data, degaussing sufficiently to ensure that the data cannot be reconstructed, or physically destroying disk(s).
- 6) If data has been stored on removable media (e.g. floppies, USB flash drives, portable hard disks, or similar disks), the data recipient shall destroy the data by using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data, degaussing sufficiently to ensure that the data cannot be reconstructed, or physically destroying disk(s).

Additional information on approved media sanitization methods can be found in National Institute of Standards and Technology Special Publication 800-88, Revision 1 (NIST SP-800-88 R1).

ON-SITE OVERSIGHT AND RECORDS MAINTENANCE

CONTRACTOR NAME agrees that SAO shall have the right, at any time, to monitor, audit and review activities and methods in implementing the Agreement in order to assure compliance therewith, within the limits of CONTRACTOR NAME's technical capabilities.

The Office of the State Auditor, federal auditors, and any persons duly authorized by the parties shall have full access to and the right to examine any of these materials during this period.

SIGNATURES

The signatures below indicate agreement between the parties.

OFFICE OF THE STATE AUDITOR

Signature

Printed Name

Title

Date

CONTRACTOR NAME

Signature

Printed Name

Title

Date

EXHIBIT E – STATE AUDITOR’S OFFICE (SAO) SECURITY QUESTIONNAIRE

Please answer with as much description and detail as possible to the following questions. Questions and requests for information are in support of SAO compliance requirements derived from OCIO Standard No. 141.10. This standard can be retrieved from: <https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets>.

Physical and Environmental Protection

1. Please describe the physical attributes and controls used to protect computer hardware, documents and all related material that could or will be associated with any contracted data exchange between the State Auditor’s Office and the audited entity.
2. Will your organization be storing any contract related data on other systems in addition to workstations such as servers or cloud service providers? If so, describe the physical security and controls in order to protect contract related data.
3. Will your organization’s assigned agents associated with any contract with SAO be accessing and storing any contract data on mobile devices such as phones and tablets. If so, describe any controls used to protect contract related data on those devices.

Network Security *(Regarding any systems that will be storing, processing or used for transitory (email for example) functions with contract related data)*

1. If applicable, how will your organization apply and enforce network controls to protect segments and individual systems with each segment in order to prevent unauthorized access to contract related data.
2. How does your organization ensure that systems are up-to-date with latest software security patches and updates? Please explain your organization’s patch management process and provide your organization’s patch management policy.
3. Please provide your organization’s password policy.

Operations Management

1. Describe your organizations media handling and disposal process? Please provide your associated policy if applicable.
2. Does your organization have a data backup processes in place that will capture and backup any data related to the contract? If so, please describe the backup process and procedures and any controls (e.g., encryption) used to protect contract related data in backup systems? Please provide your associated policy if applicable.

Security Monitoring and logging

1. What type of auditing capabilities, features and settings does your organization enable on systems such as security event logs? Please provide your organization’s policy associated to this question.
2. How long are logs retained on any system that will be handling contract related data?

Incident Response - In the event of any confirmed compromised or breach of data related to protected contract related data, explain or provide your organization’s Incident Response protocol or plan. Please provide all associated organizational policies with this question.

Data Security

1. Please explain any controls (encryption; role-based security for example) your organization uses to protect contract related data on systems such as servers to prevent unauthorized access to data-at-rest.
2. Will your organization be using any system(s) for data transfer or transmission such as file transfer or email type systems to transmit contract related data? If so, please describe all controls that will ensure the data exchange is secure and that data cannot be deciphered during transmission.

EXHIBIT F – CONFIDENTIALITY AND NONDISCLOSURE AGREEMENT

CONFIDENTIALITY AND NONDISCLOSURE AGREEMENT

This Confidential and Nondisclosure Agreement ("Agreement") is entered into by and between the State Auditor's Office, an agency of Washington State government ("SAO"), and ("Recipient").

Recipient acknowledges that SAO has certain confidential or sensitive information and/or material. Recipient requires access to this information or material to complete the IT Security Audit. SAO agrees to release this information to Recipient for those purposes pursuant to the terms and conditions contained in this Agreement. Recipient agrees to the terms and conditions herein.

NOW THEREFORE, in consideration of the above premises and the promises contained herein, the parties agree as follows:

1. Whenever used in this Agreement, the term "Confidential Information" will mean (i) information exempt from disclosure to the public or other unauthorized persons under either chapter 42.56 RCW or other state or federal statutes, unless otherwise identified as non-confidential at the time of disclosure; or (ii) any other information which SAO has identified to Recipient in writing as confidential at the time of disclosure or within thirty (30) days after disclosure; or (iii) information which would ordinarily be considered confidential or proprietary in the light of the circumstances surrounding disclosure. Confidential Information may take the form of (but is not limited to) plans, calculations, charts, concepts, know-how, inventions, licensed technology, design sheets, design data, diagrams, system design, materials, hardware, manuals, drawings, processes, schematics, specifications, instructions, explanations, research, test procedures and results, equipment, identity and descriptions of components or materials used, social security numbers, protected health information, personally identifiable information, IT security test results or any other material or information supplied by or on behalf of SAO, or that is disclosed to or becomes known by Recipient as a result of its dealings with SAO. Confidential Information may be in tangible or intangible form. SAO's failure to expressly identify Confidential Information as such shall not in any way lessen or negate Recipient's obligation to keep such information confidential in accordance with this Agreement.
2. Notwithstanding the foregoing, the term "Confidential Information", shall not be construed to include information that (i) is or becomes readily available in public records or documents, other than as a result of a disclosure by Recipient or other entity acting on behalf of Recipient, or (ii) which can be documented to have been known by Recipient prior to its disclosure by SAO, or (iii) which is disclosed pursuant to applicable law, judicial action or government regulations, including without limitation the Washington State Public Records Act, RCW 42.56, et seq.
3. The Recipient acknowledges that the Confidential Information is confidential and proprietary information of State of Washington (SOW) and local governments and that its protection is essential to the security and mission of SOW and local governments. The purpose of this agreement is to enable SAO to make disclosure of the Confidential Information to the Recipient while still maintaining rights in and control over the Confidential Information. The purpose is also to preserve confidentiality of the Confidential Information and to prevent its unauthorized disclosure. It is understood that this agreement does not grant Recipient an express or implied license or an option on a license, or any other rights to or interests in the Confidential Information.
4. The Recipient shall, and require its employees, officers, independent contractors, and subcontractors, and any other entities acting on its behalf (collectively "Affiliates") to:
 - (a) copy, reproduce or use Confidential Information only for the purpose described herein and not for any other purpose unless specifically authorized to do so in writing by SAO; and
 - (b) not permit any other person to use or disclose the Confidential Information for any purpose other than those expressly authorized by this Agreement; and
 - (c) disclose such Confidential Information only to those of its Affiliates who require knowledge of the same for the purpose described herein; provided such Affiliates are obligated to maintain the confidentiality of the Confidential Information and otherwise comply with the terms of this Agreement; and
 - (d) implement physical, electronic and managerial safeguards to prevent unauthorized access to or use of Confidential Information, including without limitation, providing Affiliates a copy of the terms of this

Agreement. Such restrictions will be at least as stringent as those applied by the Recipient to its own most valuable confidential and proprietary information.

5. The acts or omissions of Recipient's Affiliates with respect to the Confidential Information shall be deemed to be acts or omissions of Recipient.
6. Recipient will not remove, obscure or alter any confidentiality or trade secret notation from the Confidential Information without SAO's prior written authorization.
7. Confidential Information will remain the exclusive property of SAO; upon completion of the project described in Section 1, or whenever requested by SAO, Recipient will promptly destroy or return to SAO all Confidential Information and all copies thereof, including summaries, reports or notes based thereon, unless otherwise expressly authorized by SAO in writing.
8. Recipient agrees that the breach of the terms of this Agreement would cause irreparable damage to SOW and/or local governments and their citizens. Therefore, Recipient agrees that if it should breach its obligations hereunder, Recipient will defend, indemnify, and hold SAO harmless from actual damages from losses that result from its breach, including the notification requirements of RCW 42.56.590. This includes attorneys' fees and costs of suit. Also, SAO has the right to seek an order to restrain Recipient from breaching this agreement. If SAO does seek such an order, Recipient agrees at this time to waive any claim or defense that SAO has an adequate remedy at law or in damages.
9. This Agreement will be construed and enforced in all respects in accordance with the laws of the State of Washington. The parties consent to the exclusive jurisdiction of the Superior Court of the State of Washington and exclusive venue in Thurston County, Washington.
10. Term. The Term of this Agreement shall be three years from the date of the last signature, provided however, the obligations of confidentiality shall continue and survive this Agreement.

APPROVED

State of Washington
State Auditor's Office

APPROVED

Recipient: _____

Signature

Signature

Print or Type Name

Print or Type Name

Title

Date

Title

Date

Address

Phone

EXHIBIT G – PROCUREMENT EVALUATION FOR EXECUTIVE ORDER 18-03 CERTIFICATION FORM

CONTRACTOR CERTIFICATION EXECUTIVE ORDER 18-03 – WORKERS' RIGHTS WASHINGTON STATE GOODS & SERVICES CONTRACTS

Pursuant to the Washington State Governor's Executive Order 18-03 (dated June 12, 2018), the Office of the Washington State Auditor's Office is seeking to contract with qualified entities and business owners who certify that their employees are not, as a condition of employment, subject to mandatory individual arbitration clauses and class or collective action waivers.

Solicitation No. K646 RFQQ 2011

I hereby certify, on behalf of the firm identified below, as follows (check one):

 NO MANDATORY INDIVIDUAL ARBITRATION CLAUSES AND CLASS OR COLLECTIVE ACTION WAIVERS FOR EMPLOYEES. This firm does NOT require its employees, as a condition of employment, to sign or agree to mandatory individual arbitration clauses or class or collective action waivers.

OR

 MANDATORY INDIVIDUAL ARBITRATION CLAUSES AND CLASS OR COLLECTIVE ACTION WAIVERS FOR EMPLOYEES. This firm requires its employees, as a condition of employment, to sign or agree to mandatory individual arbitration clauses or class or collective action waivers.

I hereby certify, under penalty of perjury under the laws of the State of Washington, that the certifications herein are true and correct and that I am authorized to make these certifications on behalf of the firm listed herein.

FIRM NAME: _____

Name of Contractor/Bidder – Print full legal entity name of firm

By: _____

Signature of authorized person

Print name of person make certifications of firm

Title: _____

Title of person signing certificate

Place: _____

Print City and state where signed

Date: _____

