

Statement of Work
to
Contract PSCXXXXX
for

Appellate Courts
Information Technology (IT) Security Reviews
&
Assessments

The successful proposer will demonstrate an understanding of the objectives for the Appellate Courts IT Security Reviews and Assessments and will provide AOC with an approach that demonstrates understanding of industry best practices and experience in similar projects. Vendor must propose to provide AOC with services and deliverables in the following categories:

- *Project Management.*
- *Penetration Testing – Internal and External.*
- *Vulnerability Risk Assessment and Analysis.*
- *Social Engineering Mechanism.*
- *AOC Security Roadmap.*
- *AOC IT Security Policy - Update Policies.*

These services and related tasks are described in more detail in the following sections. ATTACHMENT A must be used as a reference to properly prepare a response to the procurement. Following select of the Apparent Successful Vendor (ASV), the Statement of Work (SOW) will be mutually negotiated by ASV and AOC. A final version of the SOW will be incorporated in to the contract prior to execution by both parties.

This Statement of Work (SOW) is made and entered by and between the Administrative Office of the Courts (“AOC”), and *[Vendor]* (“Vendor”), for Information Technology (IT) Security Review and Assessment for the Washington State Appellate Courts.

This SOW incorporates by reference the terms and conditions of Contract Number PSC/*[XXXXXX]* in effect between the AOC and Vendor. In case of any conflict between this SOW and the Contract, the Contract shall prevail. AOC and Vendor agree as follows:

1. Introduction

The primary deliverables under this SOW are related to Information Technology Security Reviews and Assessments for the Washington State Appellate Courts. The services provided under this SOW are required as AOC continuously must meet the demands of court customer changes and modifications, which may introduce vulnerabilities that were previously non-existent. Consequently, periodic audit of information systems must be carried out by an independent, competent party. Keeping AOC’s existing systems running as securely as possible is a top priority for AOC and the courts.

2. Project or Task Objectives

Vendor must provide services and deliverables, and otherwise do all thing necessary for or incidental to the performance of work as set forth under this SOW for all services as provided below:

- Project Management.
- Penetration Testing – Internal and External.
- Vulnerability Risk Assessment and Analysis.
- Social Engineering Mechanism.
- Appellate Courts IT Security Roadmap.
- Analysis and Development of AOC IT Security Policies, Standards, and Plans.

3. Scope of Work and Deliverables

Vendor shall provide Services and staff, and otherwise do all things necessary for or incidental to the performance of work, as set forth below.

Vendor shall produce the Deliverables as provided in the Tasks as described below.

Task 1: Vendor Project Management

The scope of Task 1 shall include the following required activities:

- 1) Be the primary point of contact to AOC on all IT Security-related guidance, issues, and concerns.
- 2) Conduct an initial planning meeting with AOC prior to the start of the project.
- 3) Complete change-request documentation as required.
- 4) Manage AOC expectations and satisfaction throughout the project.
- 5) Schedule and coordinate the necessary resources to support the project.
- 6) Identify, escalate and document project issues as necessary.
- 7) Provide Vendor team guidance and planning.
- 8) Create and maintain a project plan in conjunction with AOC and measure weekly progress against mutually agreed-upon milestones.
- 9) Participate, along with Vendor team staff, in regularly scheduled Team update/status meetings (as determined needed by the Team).
- 10) Prepare written status reports for AOC at mutually agreed-upon intervals.
- 11) Attend weekly status meeting onsite at AOC or remotely, as pre-planned with the AOC Project Manager; delegation to other Vendor staff only with prior approval by AOC Project Manager.

Deliverables -Task 1

Deliverables related to Task 1 shall be completed no later than *[Month Date]*, 2015.

- 1) Provide bi-weekly project status report to AOC PM for review and consideration.
- 2) Participate in project team status meetings.

- 3) Present Final Risk Assessment and Analysis Report to ISD Management and other stakeholders, as required.
- 4) Present Final IT Security Policies, Standards and Plans to ISD Management and other stakeholders, as required.
- 5) Present Final Appellate Courts IT Security Roadmap to ISD Management and other stakeholders, as required.

Task 2: Penetration Testing

A vital component in the assessment of the efficiency of perimeter defenses for a network environment is an external vulnerability and network penetration test. In order to conduct daily work functions, any business must maintain a connection to the Internet which requires protections such as firewalls and other security precautions. Additionally, as the primary provider of systems to our court stakeholders it is critical to look at all information available about AOC from the Internet to ensure private data remains confidential. Penetration testing be conducted for the Appellate Courts of Washington State.

Task 2a: External /Internet Penetration Testing Assessment

Vendor shall complete the External/Internet Penetration Testing with very little information provided by AOC itself. Vendor shall complete assessment by imitating a “hacker” with no inside information regarding AOC systems present or technologies currently in use.

Vendor shall complete the External/Internet Penetration Testing Assessment using the following test types:

- 1) Search for publicly available information using Internet, newsgroup postings, etc.
- 2) Search domain registration for useful information.
- 3) Retrieve public Domain Name Service (DNS) records.
- 4) Identify systems accessible over the Internet (i.e., web, email, etc.).
- 5) Conduct port scans.
- 6) Identify running services.
- 7) Conduct Simple Network Management Protocol (SNMP) scans.
- 8) Identify operating systems if possible.
- 9) Identify web and email service versions.

- 10) Enumerate systems if possible.
- 11) Attempt to utilize remote access protocols if available.
- 12) Email server analysis (i.e., open relay, anonymous email, etc.).
- 13) Web server analysis (i.e., default configuration, sample scripts, etc.).
- 14) Website and web application analysis.
- 15) Conduct vulnerability scans of systems and network devices.
- 16) Exploit systems when possible.
- 17) Evaluate test results and identify false positives.

Task 2b: Internal/Physical Penetration Assessment

Vendor shall complete the Internal/Physical Penetration Testing by simulating an attack originating from within AOC's network perimeter defenses with very little information provided by AOC itself. Vendor shall complete assessment by imitating a "hacker" with no inside information regarding AOC systems present or technologies in use.

Vendor shall complete the Internal/Physical Penetration Testing Assessment using the following test types:

- 1) Internal DNS configuration.
- 2) Identify subnets and network architecture.
- 3) Systems enumeration.
- 4) Default or weak authentication configurations.
- 5) Port scans.
- 6) Identify running services.
- 7) Validate authentication requirements for non-public information.
- 8) Test system patch levels for currency.
- 9) Identify weak protocols used in the environment.
- 10) Conduct vulnerability scans of systems and network devices.
- 11) Conduct scanning for wireless networks belonging to the customer organization and assess any vulnerabilities associated with the service or connected resources.
- 12) Exploit systems when possible.
- 13) Evaluate test results and identify false positives.

Deliverables - Task 2

Deliverables related to Task 3 shall be developed comprehensively for the Appellate Court of Washington State and completed no later than *[Month Date]*, 2014.

- 1) Submit *draft* External Penetration Testing Assessment Report to AOC Project Manager for review and consideration.

- 2) Submit *draft* Internal Penetration Testing Assessment Report to AOC Project Manager for review and consideration.
- 3) Submit *final* External Penetration Testing Assessment Report to AOC Project Manager for review and final acceptance.
- 4) Submit *final* Internal Penetration Testing Assessment Report to AOC Project Manager for review and final acceptance.

Task 3: Vulnerability Risk Assessment and Analysis

The required activities to complete the Vulnerability Risk Assessment and Analysis shall require full collaboration between Vendor and AOC PM as well as other organizational personnel to ensure comprehensive testing of all aspects of information security for the Appellate Court of Washington State has been analyzed.

- 1) Perform risk assessments, which will document reasonable and foreseeable threats to the AOC and the Appellate Courts and well as controls in place to migrate those threats.
- 2) Controls will be tested through sampling to determine effectiveness.
- 3) Vulnerability risk assessment and analysis shall include, but not limited to, the following test types:
 - a. Validate physical security controls around sensitive systems.
 - b. Verify environmental protection against, fire, flood and other hazards.
 - c. Verify antivirus software deployment and maintenance.
 - d. Review user account administration procedures and practices.
 - e. Review firewall filtering rule configurations.
 - f. Validate separation of suited and dual control issues.
 - g. Assess encryption methodologies used.
 - h. Validate controls over software licensing.
 - i. Evaluate data destruction procedures.

Deliverables - Task 3

Deliverables related to Task 3 shall be developed comprehensively for the Appellate Court of Washington State and completed no later than *[Month Date]*, 2014.

- 1) Submit draft Risk Assessment and Control Design Review Report to AOC Project Manager for review and consideration.
- 2) Submit draft Control Testing and Gap Analysis to AOC Project Manager for review and consideration.
- 3) Submit final Risk Assessment and Control Design Review Report to AOC Project Manager for review and final acceptance.
- 4) Submit final Control Testing and Gap Analysis to AOC Project Manager for review and final acceptance.

Task 4: Social Engineering Mechanisms

Vendor shall conduct an assessment of the security awareness of employees to determine additional network vulnerabilities and potential risks. Vendor through random sampling will conduct this assessment using the following tests:

- 1) Vendor staff will pose as Appellate Court staff or other authorized individuals and attempt to gain access to sensitive areas of the organization's infrastructure.
- 2) Vendor staff will perform an email-based attack attempting to entice Appellate Courts into opening or downloading an attachment from an external email address or providing sensitive data such as their authentication credentials.
- 3) Vendor staff will perform a telephone-based testing of Appellate Courts awareness by requesting passwords or other sensitive information of employees over the phone.

Deliverables - Task 4

Deliverables related to Task 4 shall be developed comprehensively for the Appellate Courts of Washington State and completed no later than *[Month Date]*, 2014.

- 1) Submit *draft* Social Engineering Mechanism Report which includes findings and recommendations for remedy to AOC Project Manager for review and consideration.
- 2) Submit *final* Social Engineering Mechanism Report to AOC Project Manager for review and final acceptance.

Task 5: Appellate Courts IT Security Roadmaps

Vendor will review the recently completed courts assessment and develop recommendations for remediation of negative findings. Following each court assessment, vendor is expected to analyze the results of the vulnerability and penetration tests, and formalize all IT findings, along with recommendations for remediation. Vendor will develop a long range strategy in the form of an IT Security Roadmap for each court assessed.

Deliverables - Task 5

Deliverables related to Task 5 shall be completed no later than *[Month Date]*, 2015.

- 1) Submit *draft* IT Security Roadmap for each court, which includes findings and recommendations for remedy to AOC Project Manager for review and consideration.
- 2) Submit *final* IT Security Roadmap to AOC Project Manager for review and final acceptance.

Task 6: Analysis and Development of AOC IT Security Policies, Standards, and Plans

The scope of Task 6 shall require Vendor to conduct a comprehensive review and evaluation of existing AOC IT security policies, standards, and procedures. Vendor will compare the AOC documentation to industry standards and best practices. Vendor will determine where gaps, inconsistencies, or shortcomings exist in the AOC IT Security policies, standards, and procedures, and present recommended changes or new verbiage to address shortcomings. Vendor is required to

deliver an updated information security policy, with associated standards and plans that incorporates and references current industry standards and best practices.

- 1) All tasks shall be completed by Vendor CISSP or CISM qualified staff resource(s).
- 2) Identify gaps and report findings to AOC PM with recommendations for remediation.

Deliverables - Task 6

Deliverables related to Task 6 shall be completed no later than *[Month Date]*, 2015.

- 1) Submit draft Policy, Standards, and Plans Review and Evaluation Report identifying gaps and providing recommendations for remediation to AOC Project Manager for review and consideration.
- 2) Submit final Policy, Standards, and Plans Review and Evaluation Report identifying gaps and providing recommendations for remediation to AOC Project Manager for review and final acceptance.
- 3) Submit draft AOC IT Security Policy, Standards, and Plans - Update which incorporates and references current industry standards and best practices to AOC Project Manager for review and consideration.
- 4) Submit final AOC IT Security Policy, Standards, and Plans – Update which incorporates and references current industry standards and best practices to AOC Project Manager for review and final acceptance.

4. Timeline and Period of Performance

The period of performance for this project will start on within five (5) business days of contract execution with AOC with the SOW tasks to be completed no later than *[Month Date]*, 2015. AOC has the right to extend or terminate this SOW at its sole discretion.

5. Task Deliverables Schedule

Acceptance criteria is set forth in Section 14 of Contract PSCXXXXX . At a minimum, Vendor shall provide each draft deliverable to AOC Project Manager for review and consideration no later than the due date set forth in the Task Deliverables Schedule below. If requires additional modifications to a draft deliverable, AOC Project Manager will notify Vendor Project Manager of all required edits before AOC Project Manager will provided acceptance of any such deliverable as final. Documents provided to AOC Project Manager as FINAL deliverables shall be marked as such and shall be due no later than the due date set forth in the Task Deliverables Schedule below.

The table below will be completed based on the dates provided by Vendor in the Project Plan and schedule submitted as part of any proposal. If selected as ASV, Vendor should expect potential contract negotiations with AOC regarding adjustment to proposed deliverable due dates.

Task No.	Task Deliverables	Deliverable Due Date
1	Project Management Bi-weekly Status Report	Bi-weekly, 5 PM PST Monday
1	Attend IT Security Project Team Meeting	Weekly, as required
2a	Draft External Penetration Testing Assessment Report	<i>MM/DD/YYYY</i>
2b	Draft Internal Penetration Testing Assessment Report	<i>MM/DD/YYYY</i>

2a	Final External Penetration Testing Assessment Report	<i>MM/DD/YYYY</i>
2b	Final Internal Penetration Testing Assessment Report	<i>MM/DD/YYYY</i>
3a	Draft Risk Assessment and Control Design Review Report	<i>MM/DD/YYYY</i>
3b	Draft Control Testing and Gap Analysis	<i>MM/DD/YYYY</i>
3a	Final Risk Assessment and Control Design Review Report	<i>MM/DD/YYYY</i>
3b	Final Control Testing and Gap Analysis	<i>MM/DD/YYYY</i>
4	Draft Social Engineering Mechanism Report	<i>MM/DD/YYYY</i>
4	Final Social Engineering Mechanism Report	<i>MM/DD/YYYY</i>
5	Draft Appellate Courts IT Security Roadmaps	<i>MM/DD/YYYY</i>
5	Final Appellate Courts IT Security Roadmaps	<i>MM/DD/YYYY</i>
6	Draft AOC IT Security Policy, Standards & Plans Review and Evaluation Report	<i>MM/DD/YYYY</i>
6	Final AOC IT Security Policy, Standards & Plans Review and Evaluation Report	<i>MM/DD/YYYY</i>
6	Draft AOC IT Security Policy, Standards & Plans - Update	<i>MM/DD/YYYY</i>
6	Final AOC IT Security Policy, Standards & Plans - Update	<i>MM/DD/YYYY</i>

Changes to this SOW shall be mutually agreed upon in writing and incorporated into the contract through execution of an amendment signed by both parties.

6. Compensation and Payment

AOC shall pay Vendor an amount not to exceed [_____] dollars (\$____) [*specify maximum dollar amount*] for the performance of all activities necessary for or incidental to the performance of work as set forth in this SOW. Vendor's compensation for services rendered shall be based on Vendor's Prices as set forth in *Table 2 – Payment Schedule* below.

Task No.	Key Deliverables*	Payment
2a	FINAL External Penetration Testing Assessment Report	<i>xx,xxx</i>
2b	FINAL Internal Penetration Testing Assessment Report	<i>xx,xxx</i>
3a	FINAL Risk Assessment and Control Design Review Report	<i>xx,xxx</i>
3b	FINAL Control Testing and Gap Analysis	<i>xx,xxx</i>
4	FINAL Social Engineering Mechanism Report	<i>xx,xxx</i>
5	FINAL Appellate Courts IT Security Roadmaps	<i>xx,xxx</i>
6	FINAL AOC IT Security Policy, Standards & Plans Review and Evaluation Report	<i>xx,xxx</i>
6	FINAL AOC IT Security Policy, Standards & Plans - Update	<i>xx,xxx</i>
	Contract Total	<i>\$ xx,xxx</i>

*Costs associated with services related to Vendor Project Management shall be considered inclusive of these deliverables.

Table 2 – Payment Schedule

AOC shall not reimburse Vendor for any travel and other expenses incurred in performing work under this SOW.

7. Vendor Staff, Roles and Responsibilities

Vendor staff will hold the following key project positions including roles and responsibilities as provided below:

[Identify Vendor staff who will be involved, naming individuals key to the project, and describe in detail their roles and responsibilities. Expand the table below, as required.]

Vendor Key Staff Name	Title
<Name>	Project Manager
<Name>,	Technical Security Lead

Vendor's Personnel

For work to be performed for AOC, AOC reserves the right to reject any of the Vendor employees. Any and all costs or expenses associated with replacement of any person or entity shall be borne by the Vendor.

Vendor may not change or replace any of the staff assigned to this Contract without prior approval of AOC, which approval will not be unreasonably withheld. Vendor is not responsible for delays or repeated tasks caused by factors outside its control. These factors include, but are not limited to, availability of AOC personnel, equipment, and telecommunication provider services.

Vendor will use commercially reasonable efforts to take into account AOC's schedule, but in all events the performance of Services is subject to the availability of Vendor personnel and resources, as determined by Vendor.

Vendor shall 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. Vendor shall avoid overstaffing the work or shuffling personnel assigned to said work.

During all work effort required to be performed under this SOW, Vendor is responsible to monitor all required certifications for assigned employees, maintain to proof of certification renewals during the term of the SOW.

Vendor will conduct work in the most appropriate location based on access requirements and costs associated with travel. Therefore, the external assessment and web application assessment will be conducted remotely to AOC's offices.

Vendor will perform discovery of AOC's Internet-accessible networks and systems, but will confirm this information with the customer before proceeding. Notification will be provided by the Vendor through email with a follow-up voice call to both the primary and secondary AOC SME contacts.

Vendor will participate in presentations for AOC executive management and the steering committees, as required.

Vendor will provide the applicable and necessary labor, consultation, materials, project management and/or tools to perform the Services and provide the Deliverables described herein.

Vendor Project Manager

Vendor Project Manager shall be responsible for defining the project scope and estimate, building the detailed project plan, monitoring and directing project activities as they relate to the project scope and project plan. He shall be required to document scope changes through the change management process, and coordinating the daily tasks of the project team. Vendor Project Manager contact information is provided below.

Vendor Project Manager: *<Last Name, First Name>*

Address: *Street Address, City, State, Zip Code+4*

Phone: *(XXX) XXX-XXXX* Fax: *(XXX) XXX-XXXX* Email: *<email address>*

Vendor Account Manager

Vendor Account Manager will be the principal point of contact for AOC concerning Vendor's performance under this Contract. Vendor shall notify the Project Manager, in writing, when there is a new Vendor Account Manager assigned to this Contract. The Vendor Account Manager contact information is:

Vendor Account Manager: *<Last Name, First Name>*

Address: *Street Address, City, State, Zip Code+4*

Phone: *(XXX) XXX-XXXX* Fax: *(XXX) XXX-XXXX* E-mail: *<email address>*

Additional Requirements (Optional)

<This optional section can be completed following contract negotiations with ASV. >

8. AOC Staff, Roles and Responsibilities

AOC Project Manager, *<Name>*, for this project shall be responsible for coordinating resources and staff in support of project activities, and will provide technical assistance and guidance for the business and technology areas of the project. AOC Project Manager will make final project decisions and have acceptance signoff authority for all project deliverables.

9. Additional Terms and Conditions Specific to this SOW

Vendor will work collaboratively with all necessary project leadership, project staff and project partners assigned to this project. Work products produced by the Vendor for AOC will become the property of AOC. Vendor must be able to work collaboratively with AOC and project partners to gain understanding of their business needs.