



## REQUEST FOR QUALIFICATIONS & QUOTATIONS

ACQ-2014-0929-RFQQ

### QUESTIONS & ANSWERS DOCUMENT

NOVEMBER 4, 2014

The Administrative Office of the Courts published the Request of Qualifications and Quotations, ACQ-2014-0929-RFQQ, on October 24, 2014 for the Appellate Courts IT Security Reviews & Assessments. As required under RFQQ Section 1.8 – Acquisition Schedule, answers to Vendor submitted questions are provided below.

- Q1: Section 4.5.2 states: “Vendor must acknowledge acceptance of these minimum requirements. Vendor must submit samples of penetration assessments for both internal and external testing produced by proposed Technical Security Lead for similar security consulting engagements. Vendor must submit samples of a vulnerability risk assessment and analysis produced by proposed Technical Security Lead for similar security consulting engagements.” In order to best meet AOC’s requirements, we would propose a multi-disciplinary security team that would include a Technical Security Lead and a separate Penetration Testing Lead. Can this requirement be reworded to accommodate security risk assessment and penetration samples produced by two separate members of the security team?
- A1: This section is specific to validation of the proposed Security Technical Lead’s skills, knowledge and experience. Samples are used by the evaluation team in determining the level of expertise of the Vendor’s proposed Security Technical Lead.
- Q2: Regarding section 5.4, how many individual Appellate Court locations are in scope for this engagement? Are these locations connected by a central MPLS or other network that would accommodate centralized vulnerability scanning?
- A2: There are four physical locations in scope for this engagement. Each Appellate Court location is connected to the Enterprise domain, but they are not configured such that a thorough assessment can be performed from a centralized location. On-site visits to each physical location will be necessary to complete vulnerability scanning.

- Q3: Section 5.8.2 states: “Vendor will required to simulate an attack originating from AOC’s network perimeter defenses with very little information provided by AOC itself.” Given that this requirement is titled “Internal Penetration Testing, is the attack to emanate from within the perimeter (connected to an internal switch port) or is this meant to be a continuation of the external testing?
- A3: See RFQQ Section 5.8.2 as modified under RFQQ Amendment No. 1.
- Q4: What is the network size or node count, # of employees, and how many locations would you like to test for the Social Engineering engagement?
- A 4: Social Engineering engagement will occur at all four (4) sites. The node count for each site varies, but will not exceed 254 per physical location.
- Q5: How many pages of documentation will need to be reviewed for section 5.7?
- A5: Approximately 1000 pages of documentation will need to be reviewed as related to RFQQ Section 5.7.
- Q6: How many external IP addresses are associated with the external Penetration Testing?
- A6: 254 external IP addresses are associated with external Penetration Testing for each of the four (4) court locations.
- Q7: How many physical locations will need to be physically visited to perform the internal penetration test?
- A7: There are five (5) physical locations --each court location and the AOC network operations center—which will need to be physically visited to perform the internal penetration testing.
- Q8: How many IP addresses are internal that will be included with the Internal Penetration Testing?
- A8: 254 external IP addresses are associated with Internal Penetration Testing for each of the four (4) court locations.
- Q9: How many Active IP addresses are expected on the internal penetration test?
- A9: The number of Active IP addresses varies. AOC estimates there are from 50 to 150 at each site.
- Q10: How many locations need to be assessed for the physical security controls of sensitive systems?

A10: All four (4) court locations will need to be assessed for these physical security controls.

Q11: Will vulnerability scans include such devices as printers, desktops and laptops on the internal networks?

A11: Yes.

Q12: Will each site require a separate internal and/or external scan?

A12: Yes.

Q13: Has a previous data classification been completed?

A13: Yes.

Q14: In reference to Attachment A, page 4, what does “customer organization” refer to?

A14: Customer Organization means “belonging to or managed by” the court site being assessed.

Q15: Does the AOC plan to include penetration tests that might simulate DoS or DDos attacks that might bring down systems?

A15: No.

Q16: Please define “threat resistance validation” requirements.

A16: This requirement has been removed from the RFQQ. See Attachment A-1 as modified under RFQQ Amendment No. 1.

Q17: Is AOC including the Supreme Court in the scope of this RFQQ, or just the Appellate courts?

A17: The Appellate Courts include the Supreme Court. For more information, see RFQQ Section 1.3.4.

Q18: How many external web applications are in scope?

A18: None

Q19: How many internal servers and network devices are in scope?

A19: For the scope of this project, there are no less than three (3) internal servers, and no more than twelve (12) network devices.

Q20: How many wireless networks? Access points?

A20: At least two (2) wireless authorized networks at each court site. There are an undetermined number of access points.

Q21: How many databases are in scope?

A21: There are no official AOC databases residing on any of the four (4) court networks, but it is likely that locally produced databases have been created. Initial interviews with each court should be structured to inquire as to the existence of local databases, and those that are revealed to the assessors shall be considered in scope.

Q22: How many firewalls are in scope?

A22: For the scope of this project, there are two (2) clustered firewall pairs in enterprise with none at court sites.

Q23: In Section 1.3, the RFQQ states that vendors do not get paid until after services and products are accepted. Could you clarify if payment is by each deliverable acceptance or at the close-out of the project?

A23: Payments to the selected Vendor will be based on the costs identified in RFQQ EXHIBIT F – Summary Key Deliverables Cost Sheet. For more information, see Section 15 of EXHIBIT C – *Draft Contract*.

Q24: Could you clarify if the three volumes referred to in Section 2.2 are to be bound as separate binders with section dividers or whether the three volumes can be bound as a single unit?

A24: Neither. Each volume copy must be bound separately by binder clip or in a three-ring binder.

Q25: In regards to Attachment A, Task 6, how many security policies, standards and procedures are included in the review and evaluation? Are there separate documents for each court location?

A25: Approximately 1000 pages of documentation will need to be reviewed as related to Attachment A, Task 6. No.

Q26: Does the AOC have an expected timeframe for completion of this project?

A26: See RFQQ Section 5.6 as modified under Amendment No. 1.

Q27: Section 1.17 states that Vendor interviews may be held at the AOC's discretion via video conference or onsite. In Section 7.39, the RFQQ states that all Vendor interviews will be held onsite without exception. Would you clarify these two conflicting statements?

A27: Section 7.39 is correct. See Amendment No. 1 for modifications to the RFQQ.

Q28: Please clarify if analyzing tests and assessments offsite is acceptable?

A28: Yes.

Q29: As the Washington courts are non-unified, does the AOC have the authority over all the courts networks, policies, standards and procedures in this request?

A29: AOC has authority over court network segments that are part of the AOC enterprise, and likewise part of this assessment. AOC also has authority over the policies referenced in section 5.11, as the requirement pertains only to AOC internal policies.

Q30: As AOC moves from JIS to COTS applications, what will be the role of the JISC moving forward? If this group is not responsible for setting policy goals going forward, will the AOC be assuming the responsibilities according to the rules set out in Chapter 2.68 RCW?

A30: This question is not applicable to the requirements set forth in the RFQQ.

Q31: Is the AOC bound by the State's OCIO security standards?

A31: No, but AOC evaluates OCIO standards and makes an effort to integrate the guidance where it aligns with our technology and business models.

Q32: We noted in the RFQQ Section 4.5.1 that the AOC requires the project manager to have the PMP certification. Is this a set requirement? Would extensive experience running similar engagements be acceptable in lieu of the PMP certification?

A32: Part 1: No, this is not a requirement. Part 2: Yes, similar experience may be considered.

Q33: Is PCI Approved Scanning Vendor (ASV) status required to perform this work?

A33: No.

Q34: Are penetration testing services required?

A34: Yes.

Q35: Total number of registered domain names maintained?

A35: Only one registered domain is maintained.

Q36: Total number of registered public (external) IP addresses to be tested?

A36: There are 1024 registered public (external) IP addresses to be tested.

Q37: Who is/are the Internet services provider(s) (ISP) used? Does the ISP monitor the network?

A37: Two Washington State agencies, Consolidated Technology Services and Department of Enterprise Services, act as the ISPs for AOC. Yes, the ISPs monitor the network.

Q38: Are managed security service providers (MSSP) used?

A38: No.

Q39: Are any websites, e-commerce, Internet banking, electronic mail or other public Internet services hosted by one or more third parties? If so, identify all the third parties. If services are hosted, does the organization have a SAS 70 audit or similar report for any of their hosted services and, if so, who has provided the organization with a SAS 70 report?

A39: No

Q40: Does the organization have an intrusion detection/prevention system (IDS/IPS) implemented?

A40: Yes, at both the enterprise and the Supreme Court location.

Q41: Number of devices (e.g., routers, firewalls, servers, etc.) available through the Internet that are located at the organization's facilities?

A41: None

Q42: Are load balancers used?

A42: Load balancers are not at the assessed locations.

Q43: Device inventory:

1. Make/model of router(s)
2. Make/model of switch(es)
3. Make/model of firewall(s)
4. Make/model of intrusion detection/prevention system(s) (IDS/IPS)
5. Make/model of server(s) and the operating system and version executed

A43: Device inventory information cannot be made available in this document, but will be provided to the awarded Vendor following contract execution.

Any modifications to the RFQQ required as a result to answers provided by AOC will be provided as an amendment to the RFQQ. Any such amendment will be published as a separate RFQQ document and will be available at [www.courts.wa.gov/procure/](http://www.courts.wa.gov/procure/).