**Washington State Consolidated Technology Services**

Solicitation Amendment

**Purchaser Name:** Consolidated Technology Services

**Solicitation Number:** 22-RFQQ-001

**Amendment Number:** 2

**Date Issued:** Cybersecurity Audit Assessment

**Purpose:**

This document is prepared by the Washington State Consolidated Technology Services (CTS) and shall serve as the sole official reply to Vendor Questions submitted in response to RFQQ 22-RFQQ-001.

Questions and responses are numbered for ease of reference only and are in no particular order or priority. Questions and comments have generally been stated as they were received except that some questions have been modified to maintain vendor confidentiality or to reduce redundancies. The answers may only explain or clarify what is already addressed in the RFQQ. Some of the answers may also supplement or change what was previously stated in the RFQQ or in an appendix. It is important that Vendors review all questions and answers. Vendors are advised to obtain and thoroughly review the complete, formal RFQQ located at: <http://watech.wa.gov/procurement-announcements>. In the revised RFQQ deleted text appears ~~struck through in black font~~, while added text appears underlined in red font.

**V****endor Questions and Official Answers**

|  |  |  |
| --- | --- | --- |
| **#** | **QUESTION** | **CTS RESPONSE** |
| 1 | We cannot find Exhibit A – Contractor Certification for Executive Order 18-03 – Workers’ Rights. Can you let us know where we can find the Exhibit A?  Executive Order 18-03 (Firms without Mandatory Individual Arbitration for Employees) - 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](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.governor.wa.gov%2Fsites%2Fdefault%2Ffiles%2Fexe_order%2F18-03%2520-%2520Workers%2520Rights%2520%2528tmp%2529.pdf%3F%3D32717&data=04%7C01%7Cmichael.callahan%40watech.wa.gov%7C7df80629cc6142d5022a08d979f72fe0%7C11d0e217264e400a8ba057dcc127d72d%7C0%7C0%7C637674924852991673%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=2W%2FyVCjOyS4TIdu4BRpVe0mxu9S5%2FfU7mxAh3MOlLro%3D&reserved=0) (dated June 12, 2018), Consolidated Technology Services – Office of Cyber Security will evaluate bids for best value and provide a bid preference in the amount of 100 points to any bidder who certifies, pursuant to the certification attached as Exhibit A – Contractor Certification for Executive Order 18-03 – Workers’ 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. | RFQQ 22-RFQQ-001 has been amended to reflect that bidder must include, in its response, a statement certifying whether the bidder meets this requirement.  The reference to Exhibit A has been removed. |
| 2 | Is it mandatory to have the following certifications: Industry certifications or similar qualifications appropriate to the services provided, at least two (2) of those listed below:* Certified Information Systems Auditor (CISA).
* Control Objectives for Information and Related Technologies (COBIT) 5 certifications (above Foundation).
* International Organization of Standards (ISO)
 | The expectations are that a consultant(s) possesses at least two of the following certifications - CISA, COBIT 5, or ISO. This requirement may be met with a single-consultant with two of the required certifications, or two-consultants that possess one of each certification, or multiple consultants possessing multiple certifications. |
| 3 | Has a security control framework been adopted? If yes, which one? | The State of Washington adheres to State technology policy OCIO 141.10 |
| 4 | Are there documented IT policies, procedures, standards, and guidelines in place?  If so, how many? | Yes, the IT Security Program audit was conducted to validate agency compliance with OCIO 141.10, the State of Washington’s cybersecurity policy and standards. There are approximately 264 controls in the OCIO 141.10 |
| 5 | How many state agency information technology security program audits were completed by Washington state agencies since July 1, 2015? | The expected range of IT Security Program Audits is expected to range between 70-85. |
| 6 | In Section 3, Project Description it states and “independent security assessments” have been performs, by “independent” does this mean an entity outside the State performed these assessments? Please clarify. | Audits were performed by organizations that are independent to the audited agency |
| 7 | Were the 70-85 agency security audits performed against any specific security framework or specific type of compliance such as PCI, etc.? If so, can you provided additional information to help provide additional detail and clarification? | The 70-85 IT Security Program Audits were conducted to determine an agency’s level of compliance to State of Washington’s OCIO 141.10. |
| 8 | In Section 3b, item 1, were the agency audits performed by the respective individual agencies, a centralized agency, external auditor(s) or some combination? | Audits were performed by organizations that are independent to the audited agency |
| 9 | In Section 3b, where any of these audits performed by SSA or IRS? If so, should the evaluation include a review of findings, standards, policies, and control effectiveness against IRS Pub 1075? | No |
| 10 | Were the security assessments performed against a specific baseline or framework or review of as-is-controls? | The IT Security Program Audits were performed to evaluate an agency’s level of compliance to OCIO 141.10  |
| 11 | Does the count of the approximately eighty (70-85) audits represent individual audit engagement covering approximately that many agencies, or multiple audit engagements of multiple agencies over several years? | Yes. The range of audits may include multiple audits from a single agency covering multiple years, audits from multiple agencies covering multiple years. |
| 12 | Might vendors have access to sanitized version(s) an audit(s) for the purpose of in assisting in assisting in more accurately sizing and scoping our response? | Not before being selected. The expected range of IT Security Program Audits is expected to range between 70-85. |
| 13 | Please clarify. In Section 3b, item 2, is it accurate in assuming that relative to industry standards at the time of the audit is that this requirement is requesting a vendor evaluation of the appropriateness of the finding given the current industry standards, not for the period of the original audit engagements (2015-2020)? | That is an incorrect assumption. Section 3b, element #2, clearly states, “Assess the content of audit findings and evaluate the findings relative to industry standards at the time of the audit” |
| 14 | In Section 3b, item 3, does this assume the successful vendor will have full access to all audit engagement documents, scoping, planning, intermediate and final findings and reports as well as all subsequent and documentation POAMs and mitigation or remediation activities irrespective of the final disposition (successfully implemented or not)? | The Office of Cyber Security will provide full access to the successful vendor of all existing audit documentation available from the previously conducted audits. |
| 15 | In Section 3b, item 4, is the scope of this evaluation CTS Information Security policies and standards, or is there a requirement that this be reviewed and reported at the individual agency level? | The IT Security Program Audits were performed to evaluate an agency’s level of compliance to OCIO 141.10, which is the State of Washington’s cybersecurity policy and standards. |
| 16 | Does this scope of work requirement assume that all current technology policies and standards will be made available for review? | The Office of Cyber Security will provide the successful vendor full access to all existing audit documentation available from the previously conducted audits. |
| 17 | Further, are policies centralized of the entire state IT program or do individual agencies write their policy? | The IT Security Program Audits were performed to evaluate an agency’s level of compliance to OCIO 141.10, which is the State of Washington’s cybersecurity policy and standards. |
| 18 | Section 3b, item 5, Is there a specific timeframe that the state has defined for “short term and long term”? Or is the vendor expected to define short- and long-term timeline recommendations? | OCS and the successful vendor will work together and collaborate on determining or defining “short term and long term” recommendations. |
| 19 | Were any of the audits combined? Or are the 70 to 85 audit reports need to be individually reviewed and assessed by the vendor? | No, the range of 70-85 audits will need to be individually evaluated and assessed by the successful vendor. |
| 20 | Section 3b, item e, would the state be able to provide additional explanation and information on “the state” of the existing agency audits to assist vendors to more accurately size and scope of work volume and effort? | The Office of Cyber Security will provide the successful vendor full access to all existing audit documentation available from the previously conducted audits. The range of audits is expected to range between 70-85 audits. |

The second purpose of this amendment is to disseminate the information to attend the Pre-Response Conference, per the Solicitation Schedule (as amended)*,* on September 23, 2021 from 1:30pm-2:00pm.

Vendors can attend the meeting in Microsoft Teams via the access information below:

Microsoft Teams meeting

**Join on your computer or mobile app**

[Click here to join the meeting](https://teams.microsoft.com/l/meetup-join/19%3Ameeting_MjRjMDY3YTAtMWY5Zi00Y2E2LTg5MDYtYzFkMmUxNmYxYjJl%40thread.v2/0?context=%7b%22Tid%22%3a%2211d0e217-264e-400a-8ba0-57dcc127d72d%22%2c%22Oid%22%3a%222cfbd888-6e0b-4b83-bb85-fab80e609269%22%7d)

**Or call in (audio only)**

+1 564-999-2000,,916724199#   United States, Olympia

Phone Conference ID: 916 724 199#

All other terms, conditions, and specifications remain unchanged.

**Bidder Acknowledgement:**

Bidder shall complete the following and return this Amendment with Proposal. Failures to provide the information requested below and submit this Amendment with Proposal will result in rejection of Proposal.

This Amendment need NOT be submitted with Bidder’s Proposal.