ITPS WORK REQUEST #24-02

NOVEMBER 20, 2023

2nd Tier Solicitation

Under Master Contract No. 08215

Category 10: Infrastructure Services

For WSIB - IT Security Audit

INTRODUCTION

The Washington State Investment Board (WSIB) is issuing this 2nd Tier solicitation under Master Contract, 08215. **Only Bidders awarded a Tier 1 Master Contract for Category 10: Infrastructure Services can bid on this opportunity.**

BACKGROUND

The WSIB is a public agency of the State of Washington established to administer the state's investment activity. The WSIB investment programs include both qualified (IRC § 401(a)) retirement programs and non-qualified programs. To learn more about the WSIB, please visit our website at https://sib.wa.gov/index.html.

Pursuant to Chapter 39.26 of the Revised Code of Washington (RCW), the WSIB is issuing this IT Professional Services (ITPS) Work Request to contract with a firm to evaluate the WSIB IT security policies for compliance with the Washington State Office of the Chief Information Officer's (OCIO) IT Security Policies (3-Year Compliance Audit); Conduct a comprehensive IT audit to evaluate existing WSIB IT security policies and practices in relation to current industry standards and best practices; Perform social engineering procedures and a review the implementation of and the effectiveness of the WSIB's IT security training program; and Perform penetration testing to ascertain whether the WSIB system could withstand attacks from a malicious hacker.

MAJOR DELIVERABLES AND TIMELINE

The contractor will work with appropriate staff at the WSIB and review systems and documentation. As needed, the contractor will work with staff from the Washington State OCIO or the State Auditor's Office (SAO) to accomplish the objectives outlined in the WA State OCIO 3-Year Compliance Audit Module (see Section 2.4 Performance Requirements for more information). The major deliverables and timeline are as follows:

A. Virtual attendance at two Audit Committee meetings:

a. March 12, 2024 – The recommended finalist(s) will be expected to provide a 20 – 30-minute virtual presentation to discuss the firm and overall audit approach. This presentation is part of the bid evaluation process and is not compensated.

b. September 3, 2024 – The Contractor will present the final audit and results.

B. Presentation of preliminary results, final presentation, detailed final report, and a separate executive summary:

a. Contractor will provide a presentation (virtual optional) of preliminary results to internal audit and information technology staff no later than June 30, 2024.

b. The final report and executive summary will be delivered to WSIB Internal Audit and Management by July 15, 2024.

c. A presentation on the final audit and results will be made to Audit Committee on September 3, 2024.

d. The report should include descriptions of any issues or observations including severity and recommendations to address the issues or observations.

C. As needed, follow-up activities to review correction action taken by WSIB to address issues or observations:

a. For items that are remediated by August, 28, 2024, contractor shall report to WSIB Internal Audit no later than August 30, 2024**.**

b. For items that are not remediated by August 28, 2024, Contractor shall be available to review corrective action and report to WSIB Internal Audit until October 31, 2024. Bidders should assume no more than twenty (20) additional hours for remediation after August 28, 2024.

This Solicitation is divided into six (6) sections:

- Section 1 provides a summary table of relevant deadlines for responding to the Solicitation and identifies contact information for the WSIB Procurement Coordinator.
- Section 2 provides important information about the procurement that is designed to help interested bidders evaluate the potential opportunity, including the purpose of the procurement, information about the resulting Contract, and the performance requirements.
- Section 3 identifies how the WSIB will evaluate the bids.
- Section 4 identifies how to prepare and submit a bid for this ITPS Work Request, including detailed instructions regarding what to submit and how to submit your bid.
- Section 5 details the applicable requirements to file a complaint, request a debrief conference, or file a protest regarding this ITPS Work Request.
- Section 6 provides information pertaining to doing business with the State of Washington, including the WSIB's efforts to enable Washington's small and diverse businesses to compete for and participate in state procurements.

In addition, this Solicitation includes the following Exhibits:

- *Exhibit A – Required Bidder Information*: These exhibits identify information that bidders must provide to constitute a responsive bid. Also see Section 4, below.
    - Exhibit A-1 – Bidder's Certification
    - Exhibit A-2 – Bidder's Profile and References
- *Exhibit B – Questionnaire*: This exhibit contains the questions bidders must respond to that will be evaluated by the WSIB.
- *Exhibit C – Fee Schedule*: This exhibit provides the pricing format bidders will complete as part of their bid.
- *Exhibit D – Work Order #24-02*: This exhibit is a draft of the Contract that any successful bidder will execute to include a required Data Sharing Agreement. If there are business concerns or other issues with the terms and conditions in this exhibit, provide proposed changes within the form. Note, however, that the WSIB reserves the right to approve or disapprove proposed changes and to take contract modifications under consideration during the evaluation process.

SECTION 1 – DEADLINES, QUESTIONS, PROCUREMENT COORDINATOR, AND MODIFICATION

This section identifies important deadlines for this ITPS Work Request, where to direct questions regarding the Competitive Solicitation, and the process for potential amendments or modifications.

1.1. **SOLICITATION SCHEDULE**. The following table identifies important dates for this ITPS Work Request:

ITPS WORK REQUEST SCHEDULE	
ITEM	**DATE**
Competitive Solicitation Posting Date	November 20, 2023
Bidder Questions Due to the WSIB	December 11, 2023
WSIB Answers to Questions Posted	December 29, 2023
Deadline for Submitting Bids	January 12, 2024
Interviews / References	January 29 – February 9, 2024
Finalist Notified	February 13, 2024
Contract Negotiation	February 13, 2024 – March 11, 2024
Final Draft Presentation Materials Due from Finalist	February 21, 2024
Finalist Presents to Audit Committee	March 12, 2024
Anticipated Announcement of Apparent Successful Bidder at Board Meeting	April 18, 2024
Anticipated Contract Start Date	April 18, 2024

1.2. **PROCUREMENT COORDINATOR.** During the ITPS Work Request process, all bidder communications must be directed to the Procurement Coordinator listed in the table below. Unauthorized bidder contact regarding this Solicitation with other state employees involved with this process may result in bidder disqualification.

PROCUREMENT COORDINATOR	
Name	Isaac Williamson
Telephone	(360) 956-4604
Email	contracts@sib.wa.gov
Subject Line	ITPS Work Request #24-02

1.3. **ITPS WORK REQUEST QUESTIONS**. Questions or concerns regarding this ITPS Work Request will be addressed consistent with the above schedule. The WSIB will provide written answers for questions received which will be posted to Washington's Electronic Business Solution (WEBS).

a. Bidders are encouraged to make any inquiries regarding this Solicitation as early in the process as possible. If a bidder does not notify the WSIB of an issue, exception, addition, or omission, the WSIB may consider the matter waived by the bidder for protest purposes.

b. If bidder inquiries result in changes to the Solicitation, written amendments, which may include the WSIB answers to bidder questions, will be issued and posted on WEBS. In no event will oral communications regarding the Solicitation be binding.

1.4. **SOLICITATION MODIFICATION**. The WSIB reserves the right to amend and modify this Solicitation. Notifications of amendments and other correspondence pertinent to this Solicitation will be posted to WEBS.

SECTION 2 – CONTRACT, PERIOD OF PERFORMANCE, PLACE OF PERFORMANCE, PERFORMANCE REQUIREMENTS

2.1. **CONTRACT**. The form of the Contract that will be awarded is attached as *Exhibit D – Work Order #24-02*.

2.2. **PERIOD OF PERFORMANCE**. The WSIB anticipates work will take place between April 18, 2024, and October 31, 2024. The period of performance for services may be extended for up to an additional one (1) year through mutual agreement of the parties.

2.3. **PLACE OF PERFORMANCE.** Performance will be a combination of onsite and virtual work. On-site work will be performed at the WSIB headquarters location in Olympia, WA.

2.4. **PERFORMANCE REQUIREMENTS**

a. The contractor will work with appropriate staff at the WSIB and review systems and documentation to accomplish the objectives outlined. An overview of the WSIB's IT environment and systems are provided as in Attachment A.

b. As needed, the contractor will work with staff from the Washington State Office of the Chief Information Officer (OCIO) or the State Auditor's Office to accomplish the objectives outlined in the WA State OCIO 3-Year Compliance Audit Module (see Section d. Work Requirements for more information).

c. The Scope of Services under the Contract will be presented at the March 12, 2024, Audit Committee meeting for review and at the April 18, 2024, Board meeting for approval. The finalist for this contract will be expected to provide a 20-30 minute virtual presentation at the March 12, 2024, Audit Committee meeting but will not be required to attend the April 18, 2024, Board meeting.

d. Work Requirements: The work will consist of 4 modules:

1. *WA State OCIO 3-Year Compliance Audit*

The Office of the Chief Information Officer's Information Technology Security Policy No. 141 requires state agencies to conduct an Information Technology Security Policy and Standards Compliance Audit every 3 years.

The contractor will evaluate existing WSIB IT security policies and procedures to determine compliance with state IT security standards (Attachment B) using the Office of the Washington State Auditor (SAO) agreed-upon audit procedures (Attachment C) Expected work will include inquiry of staff, review of

documentation, and testing to support the assessment of compliance. Any gaps will be identified and reported to management with recommendations for remediation.

2. *Information Technology Audit (Vulnerability Assessment & Risk Analysis)*

The contractor will perform a risk assessment, which will document reasonable and foreseeable threats to the WSIB, as well as controls in place to mitigate those threats. Controls will be tested through judgmental selection to determine their effectiveness.

The vulnerability assessment and risk analysis module should include an evaluation and assessment, as well as testing where applicable, of the following:

- Patch management
- Antivirus management – deploying and maintaining
- Monitoring and logging
  - Endpoint detection and response
  - Threat detection and response
- Incident management and response plan
- System and data backup
- Physical security controls around sensitive systems and/or data center(s)
- Firewall filtering rule configurations
- Separation of duties and dual control issues
- Encryption methodologies used
- Mobile device (phones and tablets) management
- Data storage device destruction procedures
- Administrative user provisioning account administration procedures and practices
- System access to sensitive network locations (policy and reviews)
- Disaster recovery
- Azure access configuration

For key third-party relationships, the contractor will assess (review and test, as applicable) the WSIB's practices for monitoring third-party vendors and the security, confidentiality, and accessibility of the WSIB data; compare with best practices; and make recommendations, as needed. This includes the processes and controls over, and practices of:

- Initial vendor review
- Data sharing agreements and contract requirements
- Ongoing monitoring, including but not limited to, review of and follow up on required reporting over IT security and cybersecurity (review of independent, external validation or System and Organization Control [SOC] reports, implementation of identified controls at the user entity), and discussion with vendors
- Proper classification, storage, and handling of WSIB data
- Removal of WSIB data at the conclusion of the contract

The contractor will perform and document a risk assessment of the WSIB's data, which should, at a minimum, include the WSIB's target profile, data sensitivity and categorization, and the contractor's assessment of the potential impact of a breach.

3. *Social Engineering and Training Program Assessment*

The contractor will perform social engineering procedures to assess the existence and effectiveness of the controls to prevent unauthorized physical and electronic access to the WSIB's IT systems. This will include a review of the implementation of and effectiveness of the WSIB's IT security training program and other activities, to include regular social engineer testing and staff training.

Contractor staff will conduct social engineering tests on WSIB staff. Some methods expected to be employed include spear phishing, impersonation, social site review, the use of physical devices, and any other common/most effective tactics used by perpetrators. Expected tests should be performed via email, text messaging to state-provided cellular devices, and state-provided direct dial numbers.

4. *Vulnerability and Network Penetration Test (External and Internal)*

The contractor will conduct a network analysis, security vulnerability review, and risk assessment of the WSIB's network infrastructure to assess the administrative and technical safeguards in place. This module will include testing of both external and internal WSIB networks.

For the external assessment, the contractor will perform non-volatile exploit procedures designed to assess the effectiveness of the WSIB's external security posture and the external network's ability to withstand up-to-date malicious exploits launched externally. The external assessment tests will be conducted with very little information provided by the WSIB. The contractor is expected to simulate a "hacker" in the wild with no inside information about the systems present or the technologies used. The contractor will perform an external scan and active penetration tests of the WSIB's network perimeter. Testing should include both application-layer and network-layer assessments, as well as remote access vectors. The external penetration testing should not include Denial of Service attacks.

For the internal assessment, the contractor will perform non-volatile exploit procedures designed to assess the effectiveness of the WSIB's internal security posture and other internal infrastructure. The internal assessment tests will also be conducted with little or no insider knowledge of the environment. The tests should simulate a purposeful attacker who has breached or otherwise circumvented perimeter security controls in order to gain access to internal systems. Testing should include both application-layer and network-layer assessments.

2.5. DELIVERABLES.

a. Virtual attendance at two Audit Committee Meetings:

1. March 12, 2024, meeting (final presentation materials due February 21, 2024)

2. September 3, 2024, meeting (final draft presentation materials due July 31, 2024)

b. No later than June 30, 2024, presentation of preliminary results (virtual optional) to Internal Audit and IT staff prior to finalizing results.

c. Detailed, final report including an executive summary, delivered to WSIB Internal Audit and WSIB management by July 15, 2024. Descriptions of any issues or observations (non-trivial), including an identification of their severity, as well as appropriate recommendations to address the issues or observations. The report and audit recommendations should be written in such a way that an informed, non-IT professional can readily understand the concerns raised.

d. Follow up report on remediation efforts for identified issues, if any, before the September 3, 2024, Audit Committee meeting. For items that are not remediated by August 28, 2024, contractor shall be available to review corrective action when noted complete and report to WSIB Internal Audit. Bidders should assume no more than twenty (20) additional hours for remediation after August 28, 2024.

2.6. **MINIMUM QUALIFICATIONS.**

- Five (5) years of experience.
- Substantial background and expertise in servicing governmental agencies in the State of Washington, clients like the WSIB, and/or in the financial services industry.
- Prior experience in evaluating IT environments similar to the WSIB.
- Information systems professional certifications such as CISA, CISSP, or other relevant certifications.

2.7. **COMPENSATION.**

Compensation will be based on deliverables received, not hours worked. Payment will be approved following WSIB's review of and verification that the contractor has performed the work detailed. Deliverables must show a direct correlation to the work listed in this solicitation and as will be set forth in *Exhibit D – Work Order #24-02*. Compensation for deliverables is anticipated to be made in separate payments as follows and is open to negotiation with the Apparent Successful Bidder:

Presentation of Preliminary Results (Modules detailed in Section 2.4) to Internal Audit and IT Staff	Payment 1
Reporting/Remediation Draft Report Final Report and Executive Summary Presentation Materials for Audit Committee Follow-up Report on Remediation Efforts Virtual Attendance/Presentation to Audit Committee	Payment 2
Up to 20 hours of remediation validation	Cost included above
Maximum Compensation for this Contract	Sum of Payment 1 and 2

- WSIB reserves the right to modify compensation process as set forth in this section to ensure compliance with state law or policy.

SECTION 3 – BID EVALUATION

This section identifies how the WSIB will evaluate bids for this Competitive Solicitation.

3.1. **OVERVIEW**. The WSIB will evaluate bids for this Solicitation as described below.

- Bidder responsiveness, performance requirements, price factors, and responsibility, will be evaluated based on the process described herein.
- Any bidder whose bid is determined to be non-responsive will be rejected and will be notified of the reasons for this rejection.

- The WSIB reserves the right to: (1) Request clarification regarding any bid; (2) Waive any informality; (3) Reject any or all bids, or portions thereof; (4) Accept any portion of the bid unless the bidder stipulates all or nothing in their bid; (5) Cancel the Solicitation and, if desired, re-solicit bids; and/or (6) Negotiate with the lowest responsive and responsible bidder(s) to determine if such bid can be improved.
- The WSIB will use the following process and evaluation criteria for an award of the Contract:

EVALUATION PROCESS	
Criteria	Available Points
Responsiveness	Pass/Fail
Response to Questionnaire	300
Cost	200
Evaluation Point Total	500
Bidder Responsibility Analysis	Pass/Fail
Interviews / References (optional)	See 3.5 and 3.6

- WSIB reserves the right to modify the evaluation process and points as set forth in this section to ensure compliance with state law or policy.

3.2. **BID RESPONSIVENESS (STEP 1)**. Proposals will be reviewed initially to determine, on a pass/fail basis, whether they meet all administrative requirements specified herein.

3.3. **RESPONSE TO EXHIBIT B QUESTIONNAIRE (STEP 2)**. An evaluation team will evaluate bidder's response to *Exhibit B – Questionnaire* and award points consistent with their best professional judgment.

3.4. **BID PRICING EVALUATION (STEP 3)**. The WSIB will evaluate bids by comparing the bidder's qualifications and the reasonableness of the submitted bid prices as provided in *Exhibit C – Fee Schedule*. Cost will be evaluated on the total not to exceed cost for all deliverables (not the hourly rate). Points awarded for Cost will be determined using the following:

Lowest overall bid = max points for cost

Lowest overall bid / bidder's total cost = % of available cost points awarded

Bidders % of available cost points awarded * 200 = cost points awarded

	Bidder A	Bidder B
Total cost for all deliverables	$10,000 (Low bid)	$12,000
% of available points awarded	100%	83%
Cost points (200 available)	200	166

3.5. **BIDDER RESPONSIBILITY ANALYSIS (STEP 4).** For responsive bids, the WSIB must determine whether the bidder is a 'responsible bidder.' Accordingly, the WSIB will make reasonable inquiry to determine bidder responsibility on a pass/fail basis. In determining bidder responsibility, the WSIB will consider the following statutory (See RCW 39.26.160) elements:

- The bidder's ability, capacity, and skill to perform the contract or provide the service required.
- The bidder's character, integrity, reputation, judgment, experience, and efficiency.
- Whether the bidder can perform the contract within the time specified.
- The bidder's performance quality pertaining to previous contracts or services.
- The bidder's compliance with laws relating to the contract or services.
- Such other information as may be secured having a bearing on the decision to award the Contract.

In addition, the WSIB may consider the following:

- Financial Information: The WSIB may request financial statements, credit ratings, references, record of past performance, clarification of bidder's offer, on-site inspection of bidder's or subcontractor's facilities, or other information as necessary to determine bidder's capacity to perform and the enforceability of bidder's contractual commitments. Failure to respond to these requests may result in a bid being rejected as non-responsive.
- References: The WSIB reserves the right to use references to confirm satisfactory customer service, performance, satisfaction with service/product, knowledge of products/service/industry and timeliness. Any negative or unsatisfactory reference can be reason for rejecting a bidder as non-responsible.

3.6. **INTERVIEWS / ORAL EVALUATIONS (STEP 5 - OPTIONAL).** The WSIB may choose to conduct virtual interviews for the final selection of the Apparently Successful Bidder(s). The virtual interviews will be evaluated to develop a consensus decision of the evaluation team.

3.7. **CONTRACT NEGOTIATIONS (STEP 6)**. The WSIB may negotiate with the highest scored responsive, responsible bidder to finalize the Contract and to determine if the bid may be improved. If, after a reasonable period of time, the WSIB, in its sole judgement, cannot reach agreement on acceptable Contract terms with such bidder, the WSIB may suspend negotiations and undertake negotiations with the next highest scored responsive, responsible bidder as determined by the evaluations.

3.8. **ANNOUNCEMENT OF APPARENT SUCCESSFUL BIDDER**. The WSIB will determine the Apparent Successful Bidder ("ASB"). The ASB will be the responsive and responsible bidder(s) that best meet(s) the Solicitation requirements and presents the best total value.

- Designation as an ASB does not imply that the WSIB will issue an award for a Contract to your firm. Rather, this designation allows the WSIB to perform further analysis and ask for additional documentation. The bidder must not construe this as an award, impending award, attempt to negotiate, etc. If a bidder acts or fails to act as a result of this notification, it does so at its own risk and expense.
- Upon announcement of the ASB(s), bidders may request a debrief conference as specified in Section 5.

3.9. **AWARD OF CONTRACT**. Subject to protests, if any, the WSIB and the ASB(s) will enter into a Contract as set forth in *Exhibit D – Work Order #24-02***.** The WSIB reserves the right to award on an all-or-nothing consolidated basis. Following the award of the Contract, all bidders registered in WEBS will receive a Notice of Award delivered to the bidder's email address provided in the bidder's profile in WEBS.

3.10. **BID INFORMATION AVAILABILITY**. Upon announcement of ASB(s), all bid submissions and all bid evaluations are subject to public disclosure pursuant to Washington's Public Records Act. *See* RCW 39.26.030(2).

SECTION 4 – HOW TO PREPARE AND SUBMIT A BID FOR THIS COMPETITIVE SOLICITATION

This section identifies how to prepare and submit your bid for this Competitive Solicitation. In addition, bidders will need to review and follow the Solicitation requirements including those set forth in the exhibits, which identifies the information that bidders must provide to constitute a responsive bid. By responding to this Solicitation and submitting a bid, bidders acknowledge having read and understood the entire Solicitation and accept all information contained within this Competitive Solicitation.

4.1. **BIDDER COMMUNICATIONS REGARDING THIS COMPETITIVE SOLICITATION**. During the Solicitation process, all bidder communications regarding this Solicitation must be directed to the Procurement Coordinator for this Competitive Solicitation. See Section 1.2 of this Competitive Solicitation. Bidders should rely only on this Solicitation and written amendments to the Solicitation issued by the Procurement Coordinator. In no event will oral communications regarding the Solicitation be binding.

- Bidders are encouraged to make any inquiry regarding the Solicitation as early in the process as possible to allow consideration and, if warranted, respond to the inquiry. If a bidder does not notify WSIB of an issue, exception, addition, or omission, WSIB may consider the matter waived by the bidder for protest purposes.
- If bidder inquiries result in changes to the Solicitation, written amendments will be issued and posted on WEBS.
- Unauthorized bidder contact regarding this Solicitation with other state employees involved with the Solicitation may result in bidder disqualification.

4.2. **PRICING**. Bid prices must include all cost components needed for the services as described in this Solicitation. In addition to hourly rates bidders should provide a blended hourly rate which includes all travel related costs where applicable.

- Inclusive Pricing: Bidders must identify and include all cost elements in their pricing. In the event that bidder is awarded a Contract, the total price for the services shall be bidder's price as submitted. Except as may be provided in the Contract, there shall be no additional costs of any kind.
- Credit Cards (P-Cards): In the event that bidder is awarded a Contract, the total price for the services shall be the same regardless of whether Purchasers make payment by cash, credit card, or electronic payment. Bidder shall bear, in full, any processing or surcharge fees associated with the use of credit cards or electronic payment.

4.3. **BID SUBMITTAL CHECKLIST – REQUIRED BID SUBMITTALS**. This section identifies the bid submittals that must be provided to constitute a responsive bid. The submittals must be delivered as set forth below. Bids that do not include the submittals identified below may be rejected as nonresponsive. In addition, a bidder's failure to complete any submittal as instructed may result in the bid being rejected. Bidders may not provide unsolicited materials. For any supplemental materials expressly required by the WSIB in writing, bidders must identify such supplemental materials with the bidder's name.

☐ **EXHIBIT A-1 – BIDDER'S CERTIFICATION**

This document is the Bidder's Certification. Complete the certification, attach it to the bid along with any exceptions or required explanations, and submit it to the WSIB.
Note: The Certification must be complete. Where there are choices, bidder must check a box. The certification must be signed and submitted by a duly authorized representative for the bidder.

☐ **EXHIBIT A-2 – BIDDER'S PROFILE AND REFERENCES**

This document is required bidder information for the WSIB contract administration purposes. Complete as instructed and submit with the bid to the WSIB.

☐ **EXHIBIT B – QUESTIONNAIRE**

Bidder will need to provide responses to the questions in *Exhibit B – Questionnaire*.

☐ **EXHIBIT C – FEE SCHEDULE**

Bidder will need to complete the price worksheet templates as instructed in *Exhibit C – Fee Schedule*.

☐ **EXHIBIT D – WORK ORDER #24-02 [PROPOSED CHANGES IF APPLICABLE]**

WSIB reserves the right to modify the terms and conditions to ensure compliance with state law or policy. If the bidder has business concerns or other issues with the terms and conditions in *Exhibit D - Work Order #24-02* the bidder must provide proposed changes within the form in MS Word format. If no changes are submitted the bidder therefore agrees to the contract as drafted. The WSIB will not thereafter consider substantive changes to *Exhibit D*.

4.4. **BID FORMAT**. Bids must be complete and must follow all instructions stated in the ITPS Work Request (including the exhibits). Unless otherwise specified in writing by the WSIB, documents included with an electronic bid must be prepared in MS Word, MS Excel, or Adobe PDF. Where required to do so, bidders may sign using either a physical or electronic signature.

4.5. **SUBMITTING BIDS**. Your electronic bid must be emailed to Contracts@sib.wa.gov. Email boxes can only accept emails that are less than 30MB in size. Bidders are cautioned to keep email sizes to less than 25MB to ease delivery. Zipped files will not be accepted.

SECTION 5 – COMPLAINT, DEBRIEF, & PROTEST REQUIREMENTS

This section details the applicable requirements for complaints, debriefs, and protests.

5.1. **COMPLAINTS**. This Solicitation offers a complaint period for bidders wishing to voice objections to this solicitation. The complaint period ends five (5) business days before the bid due date. The complaint period is an opportunity to voice objections, raise concerns, or suggest changes that were not addressed during the Question & Answer Period or, if applicable, at the Pre-Bid Conference. Failure by the bidder to raise a complaint at this stage may waive its right for later consideration. The WSIB will consider all complaints but is not required to modify or cancel the ITPS Work Request. If bidder complaints result in changes written amendment(s) will be issued and posted on WEBS.

a. **CRITERIA FOR COMPLAINT**. A formal complaint may be based only on one or more of the following grounds: (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.

b. **INITIATING A COMPLAINT**. A complaint must: (a) Be submitted to and received by the Procurement Coordinator no less than five (5) business days prior to the deadline for bid submittal; and (b) Be in writing (see Form and Substance, and Other below). A complaint should clearly articulate the basis of the complaint and include a proposed remedy.

c. **RESPONSE**. When a complaint is received, the Procurement Coordinator (or designee) will consider all the facts available and respond in writing prior to the deadline for bid submittals, unless more time is needed. The WSIB is required to promptly post the response to a complaint on WEBS.

d. **RESPONSE IS FINAL**. The Procurement Coordinator's response to the complaint is final and not subject to administrative appeal. Issues raised in a complaint may not be raised again during the protest period. Furthermore, any issue, exception, addition, or omission not brought to the attention of the Procurement Coordinator prior to bid submittal may be deemed waived for protest purposes.

5.2. **DEBRIEF CONFERENCES**. A Debrief Conference is an opportunity for a bidder and the WSIB through its Procurement Coordinator, to meet and discuss the bidder's bid (and, as further explained below, is a necessary prerequisite to filing a protest). Following the evaluation of the bids, the WSIB will issue an announcement of the ASB. That announcement may be made by any means, but the WSIB likely will use email to the bidder's email address provided in the Bidder's Profile. Bidders will have three (3) business days to request a Debrief

Conference. Once a Debrief Conference is requested, the WSIB will offer the requesting bidder one meeting opportunity and notify the bidder of the Debrief Conference place, date, and time. Please note, because the debrief process must occur before making an award, the WSIB likely will schedule the Debrief Conference shortly after the announcement of the ASB and the bidder's request for a Debrief Conference. The WSIB will not allow the debrief process to delay the award. Therefore, bidders should plan for contingencies and alternate representatives. **Bidders who wish to protest must first participate in a debrief conference. Bidders who are unwilling or unable to attend the Debrief Conference will lose the opportunity to protest. A debrief is a required prerequisite for a bidder wishing to file a protest**.

a. **TIMING**. A Debrief Conference may be requested by a bidder following announcement of the Apparent Successful Bidder (ASB).

b. **PURPOSE OF DEBRIEF CONFERENCE**. Any bidder who has submitted a timely bid response may request a Debrief Conference (see Form and Substance, and Other below). A Debrief Conference provides an opportunity for the bidder to meet with the WSIB to discuss bidder's bid and evaluation. It does not provide an opportunity to discuss other bids and evaluations.

c. **REQUESTING A DEBRIEF CONFERENCE**. The request for a Debrief Conference must be made in writing via email to the Procurement Coordinator and received within three (3) business days after the announcement of the Apparent Successful Bidder. Debrief conferences will be conducted virtually (e.g., by telephone or web-based virtual meeting such as Zoom, Skype, MS Teams), as determined by the WSIB, and may be limited by the WSIB to a specified period of time. The failure of a bidder to request a debrief within the specified time and attend a debrief conference constitutes a waiver of the right to submit a protest. Any issue, exception, addition, or omission not brought to the attention of the procurement coordinator before or during the debrief conference may be deemed waived for protest purposes.

5.3. **PROTESTS**. Following a Debrief Conference, a bidder may protest the award of a Contract.

a. **CRITERIA FOR A PROTEST**. A protest may be based only on one or more of the following: (a) Bias, discrimination, or conflict of interest on the part of an evaluator; (b) Error in computing evaluation scores; or (c) Non-compliance with any procedures described in the Competitive Solicitation.

b. **INITIATING A PROTEST**. Any bidder may protest an award to the ASB. A protest must: (a) Be submitted to and received by the Procurement Coordinator within five (5) business days after the protesting bidder's Debriefing Conference (see Form and Substance, and Other below); (b) Be in writing; (c) Include a specific and complete statement of facts forming the basis of the protest; and (d) Include a description of the relief or corrective action requested.

c. **PROTEST RESPONSE**. After reviewing the protest and available facts the WSIB will issue a written response within ten (10) business days from receipt of the protest, unless additional time is needed.

d. **DECISION IS FINAL**. The protest decision is final and not subject to administrative appeal. If the protesting bidder does not accept the protest response, the bidder may seek relief in Thurston County Superior Court.

5.4. **COMMUNICATION DURING COMPLAINTS, DEBRIEFS, AND PROTESTS**. All communications about this ITPS Work Order, including complaints, debriefs, and protests, must be addressed to the Procurement Coordinator unless otherwise directed.

a. **FORM, SUBSTANCE, & OTHER**. All complaints, requests for debrief, and protests must:

i. Be in writing.

ii. Be signed by the complaining or protesting bidder or an authorized agent, unless sent by email.

iii. Be delivered within the time frame(s) outlined herein.

iv. Identify the Solicitation number.

v. Conspicuously state "Complaint," "Debrief," or "Protest" in any subject line of any correspondence or email.

vi. Be sent to the address identified below.

b. **COMPLAINTS & PROTESTS**. All complaints and protests must (a) State all facts and arguments on which the complaining or protesting bidder is relying as the basis for its action; and (b) Include any relevant documentation or other supporting evidence.

5.5. **HOW TO CONTACT THE WSIB**.

a. **TO SUBMIT A COMPLAINT**. Send an email message to the Procurement Coordinator at the following email address: Contracts@sib.wa.gov. The email message must include "Complaint" in the subject line of the email message.

b. **TO REQUEST A DEBRIEF CONFERENCE**. Send an email message to the Procurement Coordinator at the following email address: Contracts@sib.wa.gov. The email message must include "Debrief" in the subject line of the email message.

c. **TO SUBMIT A PROTEST**. Send an email message to Procurement Coordinator at the following email address: Contracts@sib.wa.gov . The email message must include "Protest" in the subject line of the email message. Alternatively, mail the protest at the following address:

SECTION 6 – DOING BUSINESS WITH THE STATE OF WASHINGTON

This section provides additional information regarding Washington's Public Records Act and doing business with the State of Washington, including the WSIB's efforts to enable Washington's small, diverse, and veteran-owned businesses to compete for and participate in state procurements for services.

6.1. **WASHINGTON'S PUBLIC RECORDS ACT – PUBLIC RECORDS DISCLOSURE REQUESTS**.

- All documents (written and electronic) submitted as part of this procurement are public records. Unless statutorily exempt from disclosure, such records are subject to disclosure ***if*** requested. *See* RCW 42.56, Public Records Act. The WSIB strongly discourages bidders from unnecessarily submitting sensitive information (e.g., information that bidder might categorize as 'confidential,' 'proprietary,' 'sensitive,' 'trade secret,' etc.).
  - If, in bidder's judgment, Washington's Public Records Act provides an applicable statutory exemption from disclosure for certain portions of bidder's bid, please mark the precise portion(s) of the relevant page(s) of the bid that bidder believes are statutorily exempt from disclosure and identify the precise statutory basis for exemption from disclosure.
  - In addition, if, in bidder's judgment, certain portions of bidder's bid are not statutorily exempt from disclosure but are sensitive because these particular portions of bidder's bid (NOT including pricing) include highly confidential, proprietary, or trade secret information (or the equivalent) that bidder protects through the regular use of confidentiality or similar agreements and routine enforcements through court enforcement actions, please mark the precise portion(s) of the relevant page(s) of bidder's bid that include such sensitive information.
- In the event that the WSIB receives a public records disclosure request pertaining to information that bidder has submitted and marked either as (a) statutorily exempt from disclosure; or (b) sensitive, prior to disclosure, will do the following:
  - The WSIB's Public Records Officer will review any records marked by bidder as statutorily exempt from disclosure. In those situations, where the WSIB concludes the designation comports with the stated statutory exemption from disclosure, the WSIB will redact or withhold the document(s) as appropriate.
  - For documents marked 'sensitive' or for documents where the WSIB either determines that no statutory exemption to disclosure applies or is unable to determine whether the stated statutory exemption to disclosure properly applies, the WSIB will notify bidder, at the email address provided in the bid submittal, of the public records disclosure request and identify the date that the WSIB intends to release the document(s) (including documents marked 'sensitive' or exempt from disclosure) to the

requester unless the bidder, at bidder's sole expense, timely obtains a court order enjoining the WSIB from such disclosure. In the event bidder fails to timely file a motion for a court order enjoining such disclosure, the WSIB will release the requested document(s) on the date specified. Bidder's failure properly to identify exempted or sensitive information and timely respond after notice of request for public disclosure has been given shall be deemed a waiver by bidder of any claim that such materials are exempt or protected from disclosure.

6.2. **SMALL & DIVERSE BUSINESSES**. The WSIB, in accordance with Washington law, encourages small and diverse businesses to compete for and participate in state procurements as contractors and as subcontractors to awarded bidders. See, e.g., RCW 39.19 (OMWBE certified businesses); RCW 43.60A.200 (WDVA certified veteran-owned businesses); and RCW 39.26.005 (Washington small businesses).

- OMWBE CERTIFICATION. Bidders may contact the Washington State Office of Minority and Women's Business Enterprises (OMWBE) regarding information on Minority-Owned and Women-Owned certified firms, state and federal certification programs, or to become certified. OMWBE can be reached by telephone, 866-208-1064, or through their website at OMWBE. OMWBE-Certified firms may provide their certification information on *Exhibit A-2 – Bidder's Profile and References*.
- WDVA CERTIFICATION. Bidders may contact the Washington State Department of Veterans' Affairs (WDVA) for information regarding Certified Veteran-Owned businesses or to become a Certified Veteran-Owned Business. The WDVA can be reached by telephone, (360) 725-2169, or through their website at WDVA. WDVA Certified firms may provide their certification information in *Exhibit A-2 – Bidder's Profile and References*.
- WASHINGTON SMALL BUSINESSES. Bidders may contact the WSIB about small and diverse business inclusion and qualification as a Washington Small Business. If you qualify as a Washington Small Business, identify yourself as such in WEBS. Call WEBS Customer Service at 360-902-7400. The qualification requirements to self-certify as a Washington Small Business are set forth in *Exhibit A-1 – Bidder's Certification*.

6.3. **WEBS REGISTRATION**. Individuals and firms interested in state contracting opportunities with any state agency should register for Solicitation notices at the Washington Electronic Business Solution (WEBS) WEBS Registration. *Note*: There is no cost to register on WEBS.

ATTACHMENT A

HIGH-LEVEL INFORMATION TECHNOLOGY LANDSCAPE SUMMARY

11/17/2023

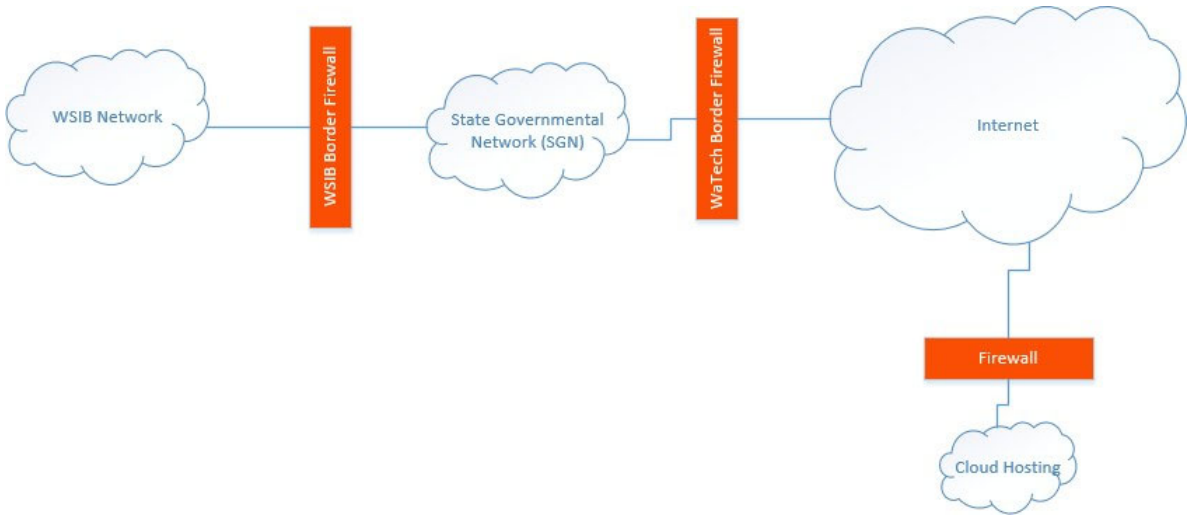
The WSIB has two physical offices, one in Olympia, WA and one in Seattle, WA. The WSIB employs approximately 115 people to include five in-house IT staff. The WSIB has approximately 12 information systems-specific policies, as well as approximately 6 other related policies that could be in the scope for this audit.

There are about 250 network end points across multiple local and cloud-based subnets. The majority of these endpoints are Microsoft Windows based. There is a data center is located at the Olympia, WA office, but we also have cloud presence with a leading cloud vendor. The bulk of our compute and storage is in the cloud environment.

The WSIB network is an element of the State Governmental Network (SGN) that is managed by the State's central IT group, Washington Technology Services (WaTech). WaTech also manages the state's border firewall and we jointly manage the WSIB's border firewall. WaTech is responsible for managing the VPN endpoint that WSIB staff utilize for accessing our network remotely and for the management of the Wi-Fi access points at the WSIB.

The WSIB has approximately fifteen primary applications that are used to support our business functions. Three of these applications are considered mission-critical and are SaaS products managed by outside parties. The remaining applications are hosted internally and are primary built and run on the Microsoft stack. The supporting databases for these applications are MSSQL, primarily running on a managed instance in the Azure cloud.

The WSIB only has one publicly exposed application, the WSIB's external facing website. It is hosted in our cloud environment.



ATTACHMENT B

Office of the Chief Information Officer (OCIO)	STANDARD NO. 141.10 **Securing Information Technology Assets**
Purpose: Set requirements for maintaining system and network security, data integrity, and confidentiality.	**Effective Date:** November 13, 2017 **See Also:** Policy No. 141 - Securing Information Technology Assets Policy No. 143 - IT Security Incident Communications Appendix C: IT Security Non-Compliance/Deviation Form Media Handling and Data Disposal Best Practices

PURPOSE

The state has a fiduciary responsibility to protect the IT systems, applications and data entrusted to it by its citizens. Therefore, it is necessary to take appropriate measures to ensure the security of these public IT assets.

INTRODUCTION

To enable the mission of state agencies and the state enterprise, reduce business risk and cost and protect the state's reputation, it is required that agencies adopt and implement common IT security standards. Common standards will help ensure that agencies have an effective means of protecting vital IT assets, and can securely store and share data between agencies and with citizens and business partners. Agencies may, and should, exceed these IT security standards based on their assessment of the risk and complexity of their IT environment or system implementation.

These IT security standards apply to all IT systems and applications, inside and outside the State Government Network (SGN), whether government-owned IT systems or contractor or vendor-owned systems that process state information, and define the processes, procedures, and practices necessary for implementing an agency-specific IT security program. They include specific steps that will be taken to ensure that a secure IT environment is maintained and all agency systems provide appropriate levels of privacy, confidentiality, integrity and availability.

Responsibly protecting public IT assets is made possible through an enterprise approach to security in state government that:

(1) Recognizes an interdependent relationship among agencies, such that strengthening security for one strengthens all and conversely, weakening one weakens all.
(2) Assumes mutual distrust until proven friendly, including relationships within government, with trading partners, and with anonymous users in a least-privilege approach to access control.
(3) Supports industry standards where applicable.

Agencies are responsible for adherence to these IT security standards to protect IT systems and applications, whether they are operated by or for an agency, and whether they operate internally on the SGN, or external to the SGN. Examples of environments external to the SGN include the Inter-Governmental Network (IGN), the Public Government Network (PGN), business partner hosted services and cloud services.

IT security planning is primarily a risk management issue. Therefore, the OCIO requires agencies to follow the IT Security policy and standards to mitigate security risks in a shared and trusted environment. Agencies will:

(1) Ensure secure interactions between and among governmental agencies take place within a shared and trusted environment.
(2) Ensure secure interactions between and among business partners, external parties, and that state agencies utilize a common authentication process, security architecture, and point of entry.
(3) Close unauthorized pathways into state networks and to the state's data.
(4) Prevent misuse of, damage to, or loss of IT hardware and software facilities.
(5) Ensure employee accountability for protection of IT assets.
(6) Ensure and oversee compliance with these IT security standards, including the annual verification of security compliance from the agency heads to OCIO.

This document contains the following IT Security Standards:

Section 1:	Agency IT Security Program Standard
Section 2 – 11:	Standards for IT security functional areas

Agencies must develop, document and implement policies and procedures for the IT security program in Section 1 and the functional areas in Sections 2 through 11. Agencies may, and should, exceed these IT security standards based on the risk and complexity of the IT environment.

SCOPE

(1) The IT security policy applies to state of Washington executive branch agencies, agencies headed by separately elected officials, and institutions of higher education.
(2) These IT security standards apply to state of Washington executive branch agencies and agencies headed by separately elected officials, referred to as "agencies" throughout this document.
(3) Institutions of higher education shall develop standards that are appropriate to their respective missions and that are consistent with the intended outcomes of the OCIO to secure data, systems and infrastructure. At a minimum, higher education institutions' security standards shall address:

a. Appropriate levels of security and integrity for data exchange and business transactions.
b. Effective authentication processes, security architectures(s), and trust fabric(s).
c. Staff training.
d. Compliance, testing, and audit provisions.

Academic and research applications and infrastructure at institutions of higher education are exempt.

STANDARDS

1. Agency IT Security Program

1.1. Documentation

The agency IT Security Program documentation must:

(1) Align with the agency's risk management strategy.
(2) Clearly identify the security objectives for agency systems.
(3) Contain policies, processes and procedures for all sections of OCIO IT security standards.
(4) Contain detail commensurate with the size, complexity, and potential business exposure based on the results of the agency's IT Risk Assessment process.
(5) Contain details of the security controls applied to agency systems.
(6) Contain details, justifications and approvals by OCIO for any deviation from the OCIO IT security standards.
(7) Contain results, logs, and records from risk and security assessments to demonstrate that the assessments performed met the intended security objectives of the agency.
(8) Identify mechanisms for receiving, documenting, and responding to reported security issues.

Agency Security Program documentation may contain information that is exempt from public disclosure as defined in RCW 42.56.420.

1.2. IT Risk Assessment

The agency must:

(1) Define and implement a formal IT Risk Assessment process to evaluate risks resulting from the use of information systems to agency operations, systems and personnel.
(2) Conduct an IT Risk Assessment when introducing new systems. When changes are made to an existing computing environment that impacts risk, conduct an IT Risk Assessment with a scope that is in proportion to the changes made.
(3) Identify assets that are within the scope of the agency IT Security Program and the entity that has responsibility for the production, development, maintenance, use, and security of the assets.

(4) Identify potential threats to assets identified as within scope.

(5) Identify the vulnerabilities that might be exploited by the threats.

(6) Identify the impacts that losses of confidentiality, integrity, and availability may have on assets identified as within scope.

(7) Assess the likelihood that security failures may occur based on prevailing threats and vulnerabilities.

(8) Conduct an IT Risk Assessment on Systems processing Category 3 data or higher once every three years. Please refer to Section 4 for data categories.

(9) Take into account business, legal, or regulatory requirements, and contractual security obligations.

1.2.1 Security Design Review and Risk Assessment

The agency must request a Security Design Review and Risk Assessment for maintenance and new development of systems and infrastructure projects when one or more of the following conditions exist:

(1) An agency is required to submit an investment plan to OCIO commensurate with the IT Investment Standards.

(2) An agency project or initiative requires OCIO or OCIO oversight as determined by OCIO policy and standards.

(3) An agency project or initiative impacts risk to state IT assets outside the agency.

(4) An agency project or initiative meets criteria for a Security Design Review and Risk Assessment as defined and documented by the agency IT security program.

Agencies are encouraged to consult with OCIO and CTS regarding any project to determine whether a Security Design Review and Risk Assessment is recommended.

The agency must provide the following to the state Chief Information Security Officer at CTS for the Security Design Review and Risk Assessment:

(1) The IT Security Checklist for the system. Please refer to Section 1.5.

(2) A system architecture diagram showing security controls and information flows.

(3) Security risk assessments identified for the system and IT infrastructure.

(4) The planned security controls and how they will be implemented.

The Chief Information Security Officer at CTS must:

(1) Review the results of the agency IT Security Checklist and other documents specific to the System.

(2) Determine whether the security design complies with OCIO IT security standards.

(3) Provide design recommendations as necessary for the agency to satisfy OCIO IT security standards.

Agencies may submit appeals regarding Security Design Review and Risk Assessment results to the OCIO.

1.3. IT Security Assessment

IT Security Assessments must be conducted periodically to review and assess the effectiveness of existing security controls. These assessments must include testing of security controls to make sure unauthorized access attempts can be identified or stopped. Examples of periodic testing include penetration tests, vulnerability assessments and system code analysis. The agency must:

(1) Establish an IT Security Assessment framework and schedule to identify a sampling of agency systems, applications, and IT infrastructure to test.

(2) Conduct IT Security Assessments against the sample in the framework to verify security controls and identify weaknesses at least once every three years.

(3) Conduct an assessment through testing scenarios relevant to changes made when the following conditions exist:
   a. A significant IT infrastructure upgrade or modification since the last IT Security Assessment was performed. Examples of a significant infrastructure upgrade or modification include but are not limited to: the addition of a new sub-network, DMZ or security perimeter device; upgrades to firewalls, switches or routers.
   b. Applications have been added or significantly modified.

(4) Correct weaknesses identified with appropriate controls.

1.4. Education and Awareness

The agency must:

(1) Ensure that personnel assigned responsibilities defined in the agency IT Security Program are competent to perform the required tasks.

(2) Document the knowledge, skills, and abilities required for personnel performing work affecting the agency IT Security Program.

(3) Require that all employees receive annual security awareness training that includes the risks of data compromise, their role in prevention, and how to respond in the event of an incident as relevant to the individual's job function.

(4) Ensure that personnel assigned responsibilities defined in the agency IT Security Program must, at a minimum, receive training that addresses the OCIO Security Policy and Standard and the agency's security policies and procedures.

1.5. Compliance

The agency must:

(1) Ensure compliant implementation of systems and IT infrastructure funded and approved after adoption of these IT security standards.

(2) Include estimates to implement these IT security standards and resulting security controls in schedules, budgets, and funding requests for maintenance and new development of applications, infrastructure, and operations.

(3) Complete the IT Security Checklist and include costs of required security controls in budgets and schedules of new development or maintenance when:

a. Significant changes are made to the application, IT infrastructure or operations.

b. An IT Investment Plan must be prepared.

c. It is required to complete a Security Design Review and Risk Assessment (Section 1.2.1)

d. The IT Security Checklist is required by the agency IT security program.

(4) Select and apply the appropriate security controls commensurate with the risk and complexity of the system after completing the agency IT Risk Assessment (Section 1.2), IT Security Assessment (Section 1.3), the IT Security Checklist, and the Security Design Review and Risk Assessment (when required) to comply with the requirements in the OCIO IT security standards.

(5) Require contractor's compliance with OCIO IT security standards relative to the services provided when:

a. The scope of work affects a state IT resource or asset.

b. The agency contracts for IT resources or services with an entity not subject to the OCIO IT security standards.

Contractor compliance may be demonstrated by mapping comparable contractor controls to these IT security standards, and by adding supplemental controls that close gaps between the two.

(6) Confirm in writing that the agency is in compliance with OCIO IT security standards. The head of each agency will provide annual verification to the OCIO by August 31 of each year or Office of Financial Management budget submittal date, whichever is later, that an agency IT Security Program has been developed and implemented according to the OCIO IT security standards. The annual security verification letter will be included in the agency IT portfolio and submitted to OCIO. The verification indicates review and acceptance of agency security policies, procedures, and practices as well as updates since the prior verification.

(7) Document instances of non-compliance with OCIO IT security standards beginning no later than August 2010 and during the funding and approval process for new initiatives referenced above in Section 1.5. For those components that do not comply, agencies complete the IT Security Non-Compliance/Deviation Form, Appendix C. Update the form and submit annually with the annual security verification letter. The form is submitted to the state CIO for approval through the state Chief Information Security Officer at CTS. For security reasons, please submit only hardcopy IT Security Non-Compliance/Deviation Forms. Do not submit these forms via email. Agencies may submit appeals to the OCIO.

1.6. Audit

The agency must:

(1) Ensure an independent audit is performed once every three years to assess compliance with OCIO IT security standards.
(2) Ensure the audit is performed by qualified parties independent of the agency's IT organization.
(3) Submit the results of the audit to the state chief information security officer at CTS.
(4) Maintain documentation showing the results of the audit according to applicable records retention requirements.
(5) Validate that security controls are implemented appropriately based on OCIO IT security standards, the agency security program, and applicable regulatory requirements.
(6) Identify nonconformities and related causes.
(7) Track progress to correct nonconformities.
(8) Implement the corrective action needed.

1.7. Maintenance

The agency must:

(1) Conduct an annual maintenance and review of the agency IT Security Program.
(2) Identify areas to improve the effectiveness of the agency IT Security Program.

2. Personnel Security

These Personnel Security controls are designed to reduce risks of human error, theft, fraud, or misuse of facilities. They help agencies ensure that users are aware of information security threats and are equipped to support the OCIO security policy in the course of their normal work.

Agencies must:

(1) Provide IT security orientation and supervision of employees and monitor contractors who have access to agency IT Assets.
(2) Ensure that appropriate staff conduct is achieved and maintained related to security matters.
(3) Conduct reference checks and background investigations as required by the agency IT security program and authorized by the agency.
(4) Require employees to receive appropriate awareness training and regular updates on agency and OCIO IT Security Policies and standards as described in Section 1.4.
(5) Provide opportunities for IT Security support staff to obtain technical training.
(6) Impose appropriate sanctions for security violations.
(7) Establish processes for the timely removal of system access for employees and contractors when duties change or when separating from service.
(8) Include appropriate language in vendor contracts to require compliance with OCIO and agency security policies, standards, and requirements.

(9) Require employees and contractors to comply with these IT security standards and agency IT policies and procedures. Each user should be made clearly aware of this responsibility.

(10) Identify, document, and implement rules for the acceptable use of IT assets consistent with rules provided by the Washington State Executive Ethics Board.

3. Physical and Environmental Protection

Agencies are responsible for ensuring that adequate physical security and environmental protections are implemented to maintain the confidentiality, integrity, and availability of the agency's computer systems. Agencies must prevent unauthorized access, damage, or compromise of IT assets. Investments in physical and environmental security must be commensurate with the risks, threats, and vulnerabilities unique to each physical site and location.

3.1. Facilities

Agencies must develop, document, and implement policies and procedures for the following:

(1) Location and layout of the facility.

(2) Physical security attributes for computer or telecommunications rooms.

(3) Design and enforcement of physical protection and guidelines for working in secure areas.

(4) Facility access control.

(5) Physical data storage and telecommunications controls.

(6) Off-site media storage.

(7) Physical security controls for mobile devices.

4. Data Security

Data security components outlined in this section are designed to reduce the risk associated with the unauthorized access, disclosure, or destruction of agency data.

4.1. Data Classification

Agencies must classify data into categories based on the sensitivity of the data. Agency data classifications must translate to or include the following classification categories:

(1) Category 1 – Public Information

Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.

(2) Category 2 – Sensitive Information

Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

(3) Category 3 – Confidential Information

Confidential information is information that is specifically protected from either release or disclosure by law. This includes, but is not limited to:

a. Personal information as defined in RCW 42.56.590 and RCW 19.255.10.
b. Information about public employees as defined in RCW 42.56.250.
c. Lists of individuals for commercial purposes as defined in RCW 42.56.070 (9).
d. Information about the infrastructure and security of computer and telecommunication networks as defined in RCW 42.56.420.

(4) Category 4 – Confidential Information Requiring Special Handling

Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

a. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements.
b. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

4.2. Data Sharing

Agencies must ensure that sharing data with the public at large complies with the OCIO Public Records Privacy Protection Policy and other applicable statutes or regulations.

When sharing Category 3 and above data outside the agency, an agreement must be in place unless otherwise prescribed by law. The agreement (such as a contract, a service level agreement, or a dedicated data sharing agreement) must address the following:

(1) The data that will be shared.
(2) The specific authority for sharing the data.
(3) The classification of the data shared. (4) Access methods for the shared data.
(5) Authorized users and operations permitted.
(6) Protection of the data in transport and at rest.
(7) Storage and disposal of data no longer required.
(8) Backup requirements for the data if applicable.
(9) Other applicable data handling requirements.

4.3. Secure Management and Encryption of Data

(1) Outside the SGN

The storage of Category 3 and Category 4 information outside the SGN requires agencies to ensure that encryption is selected and applied using industry standard algorithms validated by the National Institute of Standards and Technology (NIST) Cryptographic Algorithm Validation Program. Encryption must be applied in such a way that it renders data unusable to anyone but authorized

personnel, and the confidential process, encryption key or other means to decipher the information is protected from unauthorized access.

(2) New Systems and Applications Inside the SGN

Systems storing Category 3 and Category 4 information deployed within the SGN after [effective date of this revision] requires agencies to select and apply encryption using industry standard algorithms validated by the National Institute of Standards and Technology (NIST) Cryptographic Algorithm Validation Program. Encryption must be applied in such a way that it renders data unusable to anyone but authorized personnel, and the confidential process, encryption key or other means to decipher the information is protected from unauthorized access; unless, after completing an IT Risk Assessment, other compensating controls are identified and approved by the agency CIO and are fully implemented.

4.4. Secure Data Transfer

Agencies must appropriately protect information transmitted electronically. The transmission of Category 3 and above information outside of the SGN requires encryption such that:

(1) All manipulations or transmissions of data during the exchange are secure.
(2) If intercepted during transmission the data cannot be deciphered.
(3) When necessary, confirmation is received when the intended recipient receives the data.
(4) Agencies must use industry standard algorithms, or cryptographic modules validated by the National Institute of Standards and Technology (NIST).
(5) For agencies not on the SGN, this standard applies when transmitting Category 3 and above information outside of the agency's secure network.

5. Network Security

Agencies must ensure the secure operation of network assets through the use of appropriate layered protections commensurate with the risk and complexity of the environment.

5.1. Secure Segmentation

Agencies must:

(1) Define and implement logical boundaries to segment networks as determined by system risk and data classification.
(2) Enforce controls to protect segments and individual assets within each segment. The methods to achieve secure segmentation include but are not limited to those detailed in Sections 5.1.1- 5.1.3.

5.1.1 Network Devices

Agencies must:

(1) Securely segment Internet-available systems from internal networks.
(2) Disable unnecessary functionality such as scripts, drivers, features, subsystems, file systems and services.
(3) Harden devices based on industry best practice such as NIST, SANS, and vendor configuration standards.
(4) Change default or initial passwords upon installation.
(5) Display banner text conveying appropriate use at system entry points and at access points where initial user logon occurs.
(6) Disable remote communications where no business need exists.
(7) Standardize and document the device configurations deployed.
(8) Document deviations from device configuration standards along with the approval.
(9) Mask internal addresses from exposure on the Internet as necessitated by the risk and complexity of the system.
(10) Implement controls to prevent unauthorized computer connections and information flows through methods such as:
    a. Authentication of routing protocols.
    b. Ingress filtering at network edge locations.
    c. Internal route filtering.
    d. Routing protocols are enabled only on necessary interfaces.
    e. Restrict routing updates on access ports.
    f. Secure or disable physical network connections in public areas.

5.1.2 Firewalls

Agencies must:

(1) Securely segment DMZ interfaces, where utilized, from interfaces connected directly to the internal network.
(2) Configure network firewalls protecting production systems to:
    a. Allow system administration only through secure encrypted protocols.
    b. Prevent access by unauthorized source IP addresses or subnets.
    c. Block ingress of internal addresses from an external interface into the DMZ or internal interface.
    d. Block services, protocols, and ports not specifically allowed.
    e. Allow only necessary egress communications from the internal network to the DMZ, Internet, wireless networks and SGN.
    f. Allow only necessary ingress communications to the internal network from the DMZ, Internet, wireless networks and SGN.
    g. Maintain comprehensive audit trails.
    h. Fail in a closed state if failure occurs.
    i. Operate boundary/perimeter firewalls on a platform specifically dedicated to firewalls.

(3) Document services, ports and protocols allowed through firewalls, with supporting business purposes, in the agency IT security program.

(4) Review configurations annually.

5.1.3 Device Administration

Agencies must:

(1) Use authentication processes and mechanisms commensurate with the level of risk associated with the network segment or device.

(2) Encrypt non-console administrative access using technologies such as Secure Shell (SSH), Virtual Private Network (VPN), or Secure Sockets Layer (SSL)/Transport Security Layer Security (TLS) for Web-based management and other non-console administrative access.

5.2. Restricted Services

Agencies must implement controls to prohibit the use of the following service and application types listed in this section unless specifically authorized. The use of restricted services must be documented in the agency IT security program and approved by agency management. Restricted services include but are not limited to:

(1) Dial-in and dial-out workstation modems.

(2) Peer-to-peer sharing applications.

(3) Tunneling software designed to bypass firewalls and security controls.

(4) Auto-launching applications such as U3 that execute from a mobile device and do not require installation on a host system.

(5) Publicly managed e-mail, chat services, and video.

(6) Products that provide remote control of IT assets.

(7) Information systems audit tools.

5.3. External Connections

Agencies with devices connected to the SGN must:

(1) Prohibit direct public access between external networks and internal systems.

(2) Connect agency networks to the SGN through a CTS-managed security layer.

(3) Ensure connections between internal networks on the SGN and external networks are made through a CTS-managed security layer. The CTS-managed security layer includes, but is not limited to, firewalls, intrusion detection systems, proxy servers, security gateways, VPN and other security and monitoring systems as deemed necessary by CTS to protect the integrity of the SGN.

5.4. Wireless Connections

Agencies are responsible for the secure deployment of wireless networks. Agencies must ensure:

(1) The agency IT Security Program addresses the use of wireless technologies including but not limited to:

a. 802.11
b. Bluetooth

(2) Wireless devices that extend their Local Area Networks (LANs):
   a. Securely segment wireless access point connections from the agency network and the SGN.
   b. Use WPA or its successor for authentication and encryption. Use WPA2 Enterprise on all new equipment purchased and existing equipment that supports the protocol.
   c. Change wireless vendor defaults including but not limited to pre-shared keys and passwords.
   d. Disable Simple Network Management Protocol (SNMP) unless there is a clear business need. If enabled, change the vendor defaults.
   e. Follow wireless access security practices developed within the agency.
   f. Continuously monitor for rogue wireless devices.

(3) Wireless devices that do not extend the agency's local area network or connect to the SGN:
   a. Securely segment wireless access point connections from the Internet.
   b. Use authentication and encryption appropriate for the environment.
   c. Change wireless vendor defaults including but not limited to pre-shared keys and passwords.
   d. Disable Simple Network Management Protocol (SNMP) unless there is a clear business need. If enabled, change the vendor defaults.
   e. Follow wireless access security practices developed within the agency.
   f. Monitor for rouge wireless devices as defined in the agency security program.

(4) Open or public access wireless environments do not share assets or traverse infrastructure components that connect to the agency network or SGN unless wireless traffic is securely segmented, encapsulated or tunneled over shared infrastructure.

If wireless networks are prohibited, the agency IT Security Program documentation must define how this is periodically verified and enforced.

5.5. Security Patch Management

Agencies must develop and document in the agency IT Security Program a patch management process commensurate with the risk and complexity of the IT environment that at a minimum includes:

(1) Identification of the responsibilities required for patch management.
(2) Identification of the authorized software and information systems deployed in the production environment.
(3) Timely notification of patch availability.
(4) A method of categorizing the criticality of patches in route or on delivery.

(5) Testing procedures, when required, before deployment into production environments.

(6) Time-specific criteria for deploying patches as soon as reasonably possible after notification, including criteria for zero-day patches.

(7) Regular verification that available patches are managed according to the agency patch management process.

(8) A requirement for current patches on agency or non-agency remotely attached devices.

(9) A requirement for current patches on agency or non-agency devices attached to agency networks, whether on agency local area networks or wireless networks.

(10) Restrict access from devices that do not conform to the agency patch management policy.

5.6. System Vulnerabilities

Agencies must:

(1) Establish a process to identify newly discovered security vulnerabilities such as subscribing to alert services freely available on the Internet.

(2) Use processes that manage the installation and modification of system configuration settings.

(3) Harden systems before deployment using hardening standards that meet or exceed current best practices and manufacturer recommendations at the time of system deployment and throughout the lifecycle.

5.7. Protection from Malicious Software

Agencies must:

(1) Use anti-malware protection.

(2) Address malware prevention, detection, and removal.

(3) Keep malware protection current when connecting devices to the agency network or the SGN.

(4) Ensure that file transfers, e-mail, and Web browser-based traffic are examined for known viruses.

(5) Implement detection, prevention, and recovery controls to protect against malicious code.

(6) Integrate malicious software detection reporting with the Washington Computer Incident Response Center (WACIRC) incident reporting processes.

5.8. Mobile Computing

Examples of mobile devices include laptops, smart phones, Personal Digital Assistants (PDAs), accessible equipment, and portable data storage devices such as tape drives, zip drives, removable hard drives, and USB data storage devices.

Agencies must implement policies and procedures controlling the use of Category 3 and above data on mobile devices. At a minimum, agencies must:

(1) Approve and document the use of category 3 data or above on mobile devices.
(2) Encrypt Category 3 data or above on mobile devices using industry standard algorithms or cryptographic modules validated by the National Institute of Standards and Technology (NIST).
(3) Implement policies and procedures that address the use of portable data storage devices.

6. Access Security

6.1. Access Management

6.1.1 Policies

To ensure proper access controls that conform to the principle of least privilege agencies must:

(1) Implement policies and procedures that address access security controls for mainframe, client/server, wireless LANs, and stand-alone workstation-based systems that are consistent with the agency's classification of the data processed.
(2) Restrict access to data, application, and system functions by users and support personnel in accordance with the agency defined access control policy.
(3) Authentication and authorization controls must be appropriately robust for the risk of the application or systems to prevent unauthorized access to IT assets.
(4) Manage and group systems, data, and users into security domains and establish appropriate access requirements within and between each security domain.
(5) Implement appropriate technological controls to meet access requirements consistently.
(6) Restrict the use of programs or utilities capable of overriding system and application controls.
(7) Implement policies and procedures for identity proofing individuals.

6.1.2 Accounts

To ensure appropriate management of user accounts on system components agencies must:

(1) Establish a formal procedure for issuance, management and maintenance of UserIDs and passwords.
(2) Establish formal user registration and de-registration procedures for granting and revoking access to information systems and services.
(3) Identify users with a unique identifier, for their individual use only, before allowing them to access components, systems, networks, or data.
(4) Ensure that accounts are assigned access only to the services that they have been specifically authorized to use.

(5) Ensure the access rights of users to information and information processing facilities are removed upon suspected compromise, termination of their employment or contract, or are adjusted upon change in status.

(6) Control the addition, deletion, and modification of UserIDs, credentials, and other identifier objects.

(7) Implement mechanisms to restrict and control the use of privileges.

(8) Verify user identity before performing password resets.

(9) Set first-time passwords to a unique value per user that must be changed immediately after first use.

(10) Use time of day, and day of week restrictions as appropriate.

(11) Enable accounts used by vendors for remote maintenance only during the time needed.

(12) Prohibit the use of group, shared, or generic UserIDs/passwords.

(13) Establish a maximum of five incorrect login attempts and lock the account for a minimum of 15 minutes or until reset by an administrator.

6.1.3 Sessions

To ensure appropriate management of sessions on system components agencies must:

(1) Establish procedures to shut down or reauthorize inactive sessions after a defined and reasonable period of inactivity.

(2) Restrict user access to shared systems, especially those extending across the agency's boundaries, in accordance with the access control policy and requirements of the business applications.

(3) Ensure that access to operating systems is controlled by a secure log-on procedure.

6.1.4 Auditing

To ensure system controls are effectively enforcing access policies agencies must:

(1) Periodically review user access rights based on the risk to the data, application, or system using a formal process.

(2) Implement mechanisms to monitor the use of privileges.

6.2. Password Requirements

Agencies must ensure:

(1) Administration of password rules must be technically or procedurally enforced.

(2) UserID/password combinations are Category 3 data and must be protected.

(3) Individuals are prohibited from submitting a new password that is the same as any of the last four passwords used by the individual.

(4) Passwords used for External Authentication Types outlined under section 6.3.1 must:

a. Be a minimum of 10 characters long and contain at least three of the following character classes: uppercase letters, lowercase letters, numerals, special characters.
b. Not contain the user's name, UserID or any form of their full name.
c. Not consist of a single complete dictionary word, but can include a passphrase.
d. Be significantly different from the previous four passwords. Passwords that increment (Password1, Password2, Password3 ...) are not considered significantly different.

(5) Passwords used for Internal Authentication Types outlined under section 6.3.2 must:

a. Be a minimum of 8 characters long and contain at least three of the following character classes: uppercase letters, lowercase letters, numerals, special characters.
b. Not contain the user's name, UserID or any form of their full name.
c. Not consist of a single complete dictionary word, but can include a passphrase.
d. Be significantly different from the previous four passwords. Passwords that increment (Password1, Password2, Password3 ...) are not considered significantly different.

(6) PIN codes used in multi-factor authentication schemes must:

a. Be a minimum of five digits in length.
b. Not be comprised of all the same digit. PINs consisting of 11111, 22222 are not acceptable.
c. Not contain more than a three consecutive digit run. PINs consisting of 12347, 98761 are not acceptable.

(7) Pass codes used to secure mobile devices must:

a. Be a minimum of six alpha numeric characters.
b. Contain at least three unique character classes. Pass codes consisting of 11111a, aaaaa4, are not acceptable.
c. Not contain more than a three consecutive character run. Pass codes consisting of 12345a, abcde1 are not acceptable.
d. Render the device unusable after 10 failed login attempts.

6.3. Authentication

Authentication is used to validate the identity of users performing functions on systems. Selecting the appropriate authentication method is based on risks to data.

6.3.1 External Authentication

Six methods of authentication are defined for users accessing agency owned systems from resources outside the SGN.

6.3.1.1 Type 1 - External

Access to category 1 data, if authenticated, requires authentication via the SecureAccess® Washington infrastructure (OCIO Identity Management User Authentication Standards 7/10/2008) with the following controls:

(1) Requires UserID and hardened passwords as defined in Section 6.2.
(2) Password expiration period not to exceed 24 months.
(3) Successful authentication requires that the individual prove through a secure authentication protocol (in other words, encrypted) that the individual controls the password.
(4) Category 1 data may be accessed using type 2 or 3 authentication.

6.3.1.2 Type 2 - External

Access to category 2 data or a single category 3 record belonging to the individual requires authentication via the SecureAccess® Washington infrastructure (OCIO Identity Management User Authentication Standards 7/10/2008) with the following controls:

(1) Requires UserID and hardened passwords as defined in Section 6.2.
(2) Password expiration period not to exceed 24 months.
(3) Successful authentication requires that the individual prove through a secure authentication protocol (in other words, encrypted) that the individual controls the password.
(4) Category 2 data may be accessed using type 3 authentication.

6.3.1.3 Type 3 - External

Access to category 3 data or a single category 4 record belonging to the individual requires multi-factor authentication via the SecureAccess® Washington infrastructure (IOCIO Identity Management User Authentication Standards 7/10/2008) with the following controls:

(1) Requires multi-factor authentication supported by SecureAccess® Washington.
(2) Passwords must meet the criteria outlined in Section 6.2.
(3) Password expiration period not to exceed 13 months.
(4) Requires that the individual prove through a secure authentication protocol (in other words, encrypted) that the individual controls the password or token.
(5) Category 3 data may be accessed using type 4 authentication.

6.3.1.4 Type 4 - External

Access to category 4 information requires multi-factor authentication via the SecureAccess® Washington or Transact™ Washington infrastructure (OCIO Identity Management User Authentication Standards 7/10/2008) with the following controls:

(1) Requires multi-factor authentication using hardware or software tokens or digital certificates.

(2) Requires that the individual prove through a secure, encrypted authentication protocol that the individual controls the token by first unlocking the token with a password, PIN or biometric in a secure authentication protocol to establish two factors of authentication using a hardware or software token or digital certificate.

6.3.1.5 Type 5 - External

Employee and contractor access to agency resources or the SGN via common remote access methods outlined in Section 6.4 requires two-factor authentication with the following controls:

(1) Requires that the individual prove through a secure, encrypted authentication protocol that the individual controls a hardware or software token by first unlocking the token with a password, PIN or biometric in a secure authentication protocol to establish two factors of authentication.

6.3.1.6 Type 6 - External

Authenticated access that does not meet the criteria outlined in the OCIO Identity Management User Authentication Standards, 7/10/2008, requires, at a minimum, the use of the same controls specified in Authentication Types 1,2 and 3 above, as determined by the category of data.

6.3.2 Internal Authentication

Four methods of authentication are defined for users accessing agency owned systems from resources inside the agency network, SGN or already authenticated via common remote access methods outlined in Section 6.4.

6.3.2.1 Type 7 - Internal

Access to category 4 data and below requires authentication via the Enterprise Active Directory infrastructure (OCIO Identity Management User Authentication Standards, 7/10/2008) with the following controls:

(1) Requires UserID and hardened passwords as defined in Section 6.2.

(2) Password expiration period not to exceed 120 days.

6.3.2.2 Type 8 – Internal

Access to system administration functions requires the following controls:

(1) Requires a discrete account used only for interactive system administration functions.

(2) Where passwords are employed as an authentication factor:

a. Requires a hardened password as defined in Section 6.2 with an extended password length of 16 characters.

b. Password expiration period not to exceed 60 days.

6.3.2.3 Type 9 – Internal

Accounts used for system service, daemon or application execution (service accounts) require documentation in the agency security program and the following controls:

(1) Requires a discrete account used only for the defined privileged functions, and never used by an individual.

(2) Requires a hardened password as defined in Section 6.2 with an extended password length of 20 characters.

(3) Password expiration requirements must be documented in the agency security program.

(4) The principle of least privilege must be employed when determining access requirements for the account.

6.3.2.4 Type 10 – Internal

Authenticated access that does not meet the criteria outlined in the OCIO Identity Management User Authentication Standards, 7/10/2008, requires the following minimum controls:

(1) Requires a hardened password as defined in Section 6.2 or stronger authentication.

(2) Password expiration not to exceed 120 days.

(3) Additional controls documented in the agency IT Security Program.

6.4 Remote Access

Agencies must:

(1) Implement policies and procedures for remote access that mitigate the threat or risk posed by users or devices authorized to connect remotely to the agency network or the SGN including but not limited to:

a. Monitoring practices for remote access sessions.

b. Requirements for remote access devices.

c. Remote access session controls that conform to the principle of least privilege.

(2) Ensure mitigation is not susceptible to end-user modification.

(3) Prohibit the use of dial-up unless there is no other way to satisfy a business need. Dial-up access, if used, must be approved by management and documented in the Agency IT Security Program.

(4) Use industry standard protocols for remote access solutions.

(5) Use the state's common remote access services such as IPSec or SSL VPN when remotely accessing agency resources and services on the SGN.

(6) Ensure remote access solutions prompt for re-authentication or perform automated session termination after 30 minutes of inactivity.

(7) Ensure that agency operated remote access solutions, not connected to the agency network or the SGN, use equivalent technologies that require multi-factor authentication and include documentation of the configuration in the agency IT Security Program.

7. Application Security

7.1 Planning and Analysis

Agencies must specify security controls when developing business requirements for new or enhanced information systems including but not limited to:

(1) Ensure applications provide for data input validation to ensure the data is correct and appropriate and cannot be used to compromise security of the application, IT infrastructure, or data.

(2) Procedures are in place to manage the installation of software on operational systems including but not limited to servers and workstations.

(3) Access to program source code is restricted to only those individuals whose job requires such access.

(4) Include specific requirements in contracts for outsourced software development to protect the integrity and confidentiality of application source code.

(5) Implementation of changes will be managed by the use of formal change management procedures.

(6) Appropriate access and security controls; audit trails; and logs for data entry and data processing.

(7) Requirements for appropriate data protection.

7.2 Application Development

Agencies must develop software applications based on industry best practices and include information security throughout the software development life cycle, including the following:

(1) Separate development, test, and production environments.

(2) Implement separation of duties or other security controls between development, test and production environments. The controls must reduce the risk of unauthorized activity or changes to production systems or data including but not limited to the data accessible by a single individual.

(3) Production data used for development testing must not compromise privacy or confidentiality. Prohibit the use of Category 3 data or higher in development environments unless specifically authorized by the IT security program. Production data in any environment must meet or exceed the level of protection required by its data classification.

(4) Removal of test data and accounts before production systems become live.

(5) Removal of custom application accounts, usernames, and passwords from production environments before applications become active or are released to customers.

(6) Review of custom code prior to release to production or customers to identify potential coding vulnerabilities as described in Section 7.4 Vulnerability Prevention.

(7) Appropriate placement of data and applications in the IT infrastructure based on the risk and complexity of the system.

(8) Use of appropriate authentication levels.

7.3 Application Maintenance

Agencies must:

(1) Review and test system changes to ensure there are no adverse impacts on agency operations or security.

(2) Obtain timely information about technical vulnerabilities of information systems being used, evaluate the agency's exposure to such vulnerabilities, and take appropriate measures to address the associated risk.

7.4 Vulnerability Prevention

Agencies must prevent common coding vulnerabilities in software development processes. Agencies must:

(1) Develop software and applications based on secure coding guidelines. An example is the Open Web Application Security Project guidelines. See www.owasp.org – "The Ten Most Critical Web Application Security Vulnerabilities" which include:

a. Un-validated input.
b. Weak or broken access control such as malicious use of UserIDs.
c. Broken authentication/session management such as use of account credentials and session cookies.
d. Cross-site scripting (XSS) attacks.
e. Buffer overflows.
f. Injection flaws such as SQL injection.
g. Improper error handling that creates other conditions, divulges system architecture or configuration information.
h. Insecure storage.
i. Denial of service.
j. Insecure configuration management.

(2) Review code to detect and mitigate code vulnerabilities that may have security implications when significant changes have been made to the application.

7.5 Application Service Providers

Applications hosted by an Applications Service Provider or other third party outside of the shared, trusted environment must comply with:

(1) The OCIO IT Security Policy and Standard as described in Section 1.5.
(2) Agency security standards and procedures.

The operation of such applications must not jeopardize the enterprise security environment.

8. Operations Management

8.1 Change Management

Agencies must implement an effective change management process that:

(1) Ensures that duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the agency's IT assets.
(2) Ensures computing environments are segmented to reduce the risks of unauthorized access or changes to the operational system.
(3) Includes acceptance criteria for new information systems, upgrades, and new versions and ensure that suitable tests of the system(s) are carried out during development and prior to acceptance.

8.2 Asset Management

Agencies must:

(1) Clearly identify and maintain an inventory of major components in the IT environment.
(2) Ensure that information and assets associated with information processing be assigned to or 'owned' by designated parts of the agency. The term 'owner' identifies an individual or entity that has management responsibility for authorizing the collection, use, modification, protection and disposal of the information and asset(s).
(3) Maintain a current list of all systems containing Category 3 and Category 4 information they are responsible for, both inside and outside the SGN, whether government owned IT systems or contactor or vendor-owned systems, and include this information in their Agency IT Security Program.

8.3 Media Handling and Disposal

Agencies must:

(1) Ensure that storage media that is owned, leased or otherwise under the physical control of the agency is sanitized securely and safely when no longer required, using formal, documented procedures. At a minimum, agencies must:

a. Sanitize equipment containing storage media prior to disposal, consistent with NIST SP 800-88 Guidelines for Media Sanitation.

b. Destroy, securely overwrite, or make unavailable all data and software consistent with the software licensing agreement.

c. Verify the media is fully sanitized.

d. Verify the sanitization tools are tested and maintained per a documented schedule.

e. Maintain records that provide the date and methods used to sanitize and/or dispose of the storage media, and include attestation of the process by at least one individual.

f. Physically destroy media when it cannot be sanitized through the use of software tools. Agencies may choose to physically destroy media even when the software sanitization tools are effective. Physical destruction may be accomplished by shredding, pulverization or other means that ensure the media can never be re-used. Disposal of physically destroyed media should be conducted in accordance with the Responsible Recycling (R2) standard, the e-Stewards Standard, or some other environmentally responsible way.

(2) Ensure staff responsible for data disposal are trained to perform and attest to media sanitization functions.

(3) Ensure that media sanitization and disposal documentation is protected against unauthorized access.

(4) Ensure media containing information is protected against unauthorized access, misuse, or corruption from the time it is removed from operational status to the time it is sanitized or disposed, whether within the agency or outside the agency's physical boundaries.

8.4 Data and Program Backup

Agencies must:

(1) Satisfy data archival and rotational requirements for backup media based on the results of an IT Security Risk Assessment.

(2) Implement procedures for periodic tests to restore agency data from backup media.

(3) Test recovery procedures for critical systems at the frequency documented in the agency IT Security Program.

(4) Establish methods to secure their backup media.

(5) Store media back-ups in a secure location such as a designated temporary staging area, an off-site facility, or a commercial storage facility.

9. Electronic Commerce

Agencies must address the effect of using the Internet to conduct transactions for state business with other public entities, citizens, and businesses.

Agencies must:

(1) Prepare and incorporate plans for Internet-based transactional applications, including but not limited to e-commerce, into the agency's portfolio.

(2) Protect information involved in electronic commerce passing over public networks from fraudulent activity, contract dispute, and unauthorized disclosure and modifications required by these IT security standards.

(3) Protect information involved in on-line transactions in order to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication, or replay.

(4) Protect IT infrastructure supporting electronic commerce services from unauthorized access and use according to these IT security standards.

10. Security Monitoring and Logging

Audit logs recording user activities, exceptions, and information security events are necessary to detect and audit unauthorized information processing activities.

10.1 Logging Policies

Agencies must develop and document a logging strategy that addresses each system based on the risk and complexity of the system. At a minimum the logging strategy must address the following:

(1) The log records including events, exceptions and user activities necessary to reconstruct unauthorized activities defined by the strategy.

(2) Procedures for periodic review and analysis of recorded logs as set forth in the agency IT Security Program.

(3) Retention periods for logs.

10.2 Logging Systems

At a minimum, logging systems must satisfy the logging strategy identified by the agency and:

(1) Protect the logging facilities and log information against tampering and unauthorized access.

(2) Synchronize with an agency approved accurate time source.

(3) Provide automated recording to allow for reconstruction of the following events:

a. Actions taken by individuals with root or administrative privileges.

b. Invalid logical access attempts.

c. Initialization of the logging process.

d. Creation and deletion of system objects.

10.3 Intrusion Detection and Prevention

CTS will monitor state networks with Intrusion Detection and Prevention systems at critical junctures. Agencies that deploy Intrusion Detection and Prevention systems must ensure the systems are configured to log information continuously and the logs are reviewed periodically as set forth in the agency IT Security Program.

11. Incident Response

Agencies must:

(1) Ensure timely and effective handling of IT security incidents.

(2) Establish, document, and distribute an incident response plan to be used in the event of system compromise. At a minimum, the plan must address specific incident response procedures, recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies in addition to the following:

a. Escalation procedures.
b. Designate specific personnel to respond to alerts.
c. Be prepared to implement the incident response plan and to respond immediately to a system breach.
d. Provide appropriate training to staff with security breach response responsibilities.
e. Have a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.
f. Incorporate the incident response plan in the agency IT Security Program.

(3) Test the incident response plan at least annually.

(4) Leverage the statewide incident response capabilities such as the WACIRC and the CTS Computer Security Incident Response Team to satisfy these response standards. Agencies are also encouraged to participate in appropriate security alert response organizations at the state and regional levels.

(5) Develop and maintain a managed process for system availability throughout the agency that addresses the information security requirements needed for the agency's business operations.

Agencies must comply with the WACIRC incident reporting process(es). In the event of an incident involving the release of Category 3 data and above, agencies must comply, as appropriate, with the state breach notification statute, RCW 42.56.590 Personal Information.

RESPONSIBILITIES

Chief Information Officer (or designee)

(1) Interpret the policy and standards.

(2) Ensure policy and standards content is kept current.

(3) Recommend updates to the policy and related standards in response to changes in technology, service delivery, or other challenges to the security environment.
(4) Review agency projects for compliance with the security policy and standards.
(5) Develop an escalation process if an agency is not in agreement or compliance.
(6) Help agencies understand how to comply with the policy and standards.
(7) Monitor annual compliance by agencies.
(8) Approve deviations from the standard.

Technology Services Board

(1) Review and approve major policy changes.

CTS

(1) Maintain security of all CTS-managed networks such as the SGN, Intergovernmental Network (IGN), and Public Government Network (PGN).
(2) Design, establish, and maintain the shared IT infrastructure necessary to support applications and data within a trusted, state-wide environment.
(3) Review agency projects for compliance with the security policy and standards.
(4) Help agencies understand how to comply with the policy and standards.

State Auditor

(1) Develop, publish, and maintain audit standards for IT security audits.
(2) Conduct audits of state agencies according to its audit schedule.

Agency Heads

(1) Oversee the agency's information technology security program and ensure compliance with the security policy and these IT security standards.
(2) Assign responsibility for IT security to an individual or group with the appropriate training and background to administer those functions and ensure that the individual or group has proper authority to install, monitor, and enforce IT security standards and procedures.
(3) Ensure agency security policies, procedures, and other documents necessary for the security program are developed, implemented, maintained, and tested.
(4) Ensure all agency users of IT resources are trained to follow security policies, standards, and procedures.
(5) Submit an annual, signed security verification letter.

DEFINITIONS

When used in these IT security standards, the following terms are defined terms and will be proscribed the following meanings:

Access. The ability to use, modify, or affect an IT system or to gain entry to a physical area or location.

Application. A computer program or set of programs that meet a defined set of business needs. See also Application System.

Application System. An interconnected set of IT resources under the same direct management control that meets a defined set of business needs.

Attack. An attempt to bypass security controls on an IT system in order to compromise the data.

Authentication. The process of ensuring the identity of a connected user or participants exchanging electronic data.

Contractor. The firm, its employees and affiliated agents. Contractor also includes any firm, provider, organization, individual, or other entity performing the business activities of the agency. It will also include any subcontractor retained by Contractor as permitted under the terms of the Contract. Contractor and third-party are synonymous as defined within the Definitions section of this standard.

Environmental Security. Physical protection against damage from fire, flood, wind, earthquake, explosion, civil unrest and other forms of natural and man-made risk.

Extranet/VPN Connection. Network-level access originating from outside the network. Examples include SSL, IPSec, “terminal service” or Citrix-like connections.

Firewall. A combination of hardware and software designed to control the types of network connections allowed to a system or combination of systems or that enforces a boundary between 2 or more networks.

Information Technology (IT). Telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services.

Information Technology (IT) Assets. The processes, procedures, systems, IT infrastructure, data, and communication capabilities that allow each agency to manage, store, and share information in pursuit of its business mission, including but not limited to:

- Applications**.**
- All data typically associated with IT systems regardless of source (agency, partner, customer, citizen, etc.).
- All data typically associated with IT systems regardless of the medium on which it resides (disc, tape, flash drive, cell phone, personal digital assistant, etc.).
- End-user authentication systems.
- Hardware (voice, video, radio transmitters and receivers, mainframes, servers, workstations, personal computers, laptops, and all end point equipment).
- Software (operating systems, application software, middleware, microcode).
- IT infrastructure (networks, connections, pathways, servers, wireless endpoints).

- Services (data processing, telecommunications, office automation, and computerized information systems).
- Telecommunications hardware, software, and networks.
- Radio frequencies.
- Data computing and telecommunications facilities.
- Intelligent control systems such as video surveillance, HVAC, and physical security.

Information Technology (IT) Infrastructure. IT infrastructure consists of the equipment, systems, software, and services used in common across an organization, regardless of mission/program/project. IT Infrastructure also serves as the foundation upon which mission/program/project-specific systems and capabilities are built. Approaches to provisioning of IT infrastructure vary across organizations, but commonly include capabilities such as Domain Name Server (DNS), Wide Area Network (WAN), and employee locator systems. Additional common capabilities examples include IT security systems, servers, routers, workstations, networked Supervisory Control and Data Acquisition (SCADA) systems, and networked printers (multifunction devices).

Information Technology (IT) Risk Assessment. Reference 1.2. Risk assessment is a process by which to determine what IT Assets exist that require protection, and to understand and document potential risks from IT security failures that may cause loss of information confidentiality, integrity, or availability. The purpose of a risk assessment is to help management create appropriate strategies and controls for stewardship of information assets. (Source: Information Resources and Communications (IR&C) at the University of California Office of the President)

Internal System or Network. An IT system or network designed and intended for use only by state of Washington employees, contractors, and business partners.

Intrusion Detection Systems (IDS). Software and/or hardware designed to detect an attack on a network or computer system. A Network IDS (NIDS) is designed to support multiple hosts, whereas a Host IDS (HIDS) is set up to detect illegal actions within the host. Most IDS programs typically use signatures of known cracker attempts to signal an alert. Others look for deviations of the normal routine as indications of an attack.

Intrusion Prevention Systems (IPS). Software and/or hardware designed to prevent an attack on a network or computer system. An IPS is a significant step beyond an IDS because it stops the attack from damaging or retrieving data. Whereas an IDS passively monitors traffic by sniffing packets off of a switch port, an IPS resides inline like a firewall, intercepting and forwarding packets. It can thus block attacks in real time.

Malicious Code. Software (such as a Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.

Malware. A general term coined for all forms malicious software including but limited to computer viruses, worms, trojan horses, most rootkits, spyware, dishonest adware, crimeware and other malicious and unwanted software.

Mobile Device. A small-sized computing device that may have a display screen, touch input or a keyboard, and/or data storage capability. Examples include laptops, Personal Digital Assistants (PDAs), smart phones, tablet PCs, accessible equipment, and portable data storage devices such as tape drives, zip drives, removable hard drives and USB data storage devices.

Multi-factor Authentication (MFA). A security system or mechanism in which more than one form of authentication is implemented to verify the legitimacy of a transaction. In contrast, single factor authentication involves only a UserID/password.

In 2-factor authentication, the user provides dual means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code.

Additional authentication methods that can be used in MFA include biometric verification such as keyboard cadence, finger scanning, iris recognition, facial recognition and voice ID. In addition to these methods, device identification software, smart cards, and other electronic devices can be used along with the traditional UserID and password.

Network. A term that describes an approach to link together computers and their peripherals in order to communicate among them and with outside parties.

Network Device. A device available to other computers on a network. Examples include servers, firewalls, routers, switches, workstations, networked Supervisory Control and Data Acquisition (SCADA) systems, and networked printers (multifunction devices).

Password. A unique string of characters that, in conjunction with a logon ID, authenticates a user's identity.

Penetration Test. A deliberate probe of a network or system to discover security weaknesses. The test attempts to leverage identified weaknesses to penetrate into the organization. The test exploits the vulnerabilities uncovered during a vulnerability assessment to avoid false positives often reported by automated assessment tools.

Physical Security. Physical security describes measures that prevent or deter attackers from accessing a facility, resource, or information stored on physical media in an IT facility.

Record Units of related data fields such as groups of data fields that can be accessed by a program and that contains information on a specific item or an individual.

Risk. The potential that an event may cause a material negative impact to an asset.

Risk Assessment. The process of identifying and evaluating risks to assess potential impact.

Risk Management. Identification and implementation of IT security controls to reduce risks to an acceptable level.

Secure Segmentation. Secure segmentation is defined as implementing methods that allow for secure communication between various levels of segmented environments. These environments typically involve 4 basic segment groups:

1. Outside (Trust no one)
2. Services (Trust limited to defined segmentation lines)
3. Internal (Trust limited to defined group)
4. External users (Trust limited to defined group)

The methods for securing these segments may include but are not limited to firewall and switch/router configurations and router/switch ACLs.

Security. The protection afforded to IT systems and data in order to preserve their availability, integrity, and confidentiality. The ability to protect:

- The integrity, availability, and confidentiality of information held by an agency.

- Information technology assets from unauthorized use or modification and from accidental or intentional damage or destruction.
- Information technology facilities and off-site data storage.
- Computing, telecommunications, and applications related services.
- Internet-related applications and connectivity.

Security Controls. The security requirements and methods applied by agencies to manage IT security risk including but not limited those defined in the OCIO IT security standards.

Security Domain. An environment or context that is defined by security policy, a security model, or security architecture to include a set of system resources and the set of system entities that have the right to access the resources.

State Government Network. The shared, internal enterprise network bounded by a CTS-managed security layer. The CTS-managed security layer is defined as firewalls, proxy servers, security appliances, secure gateways and other centrally-managed security services.

System. Any collection of people, processes, and technology needed to deliver a service, capability, or functionality.

Tablet PC. A portable general-purpose computer contained within a single small form factor LCD display sized to approximately match that of a traditional writing paper tablet. A tablet PC utilizes a touch screen as the primary input source. Typically either wireless (802.11) or mobile (4G) networks are used for connectivity with limited physical port options.

Examples of Tablet PC's include: iPad, Motorola Xoom, HP Elitebook, Samsung Galaxy, Sony Tablet S, Toshiba Thrive, Acer Iconia, Kindle Fire, Nook tablet, etc.

Threat. Any circumstance or event (human, physical, or environmental) with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data, and/or denial of service by exploiting vulnerability.

Token. A security token may be either a dedicated hardware device or software-based installation on an electronic device which is used for identity proofing in multi-factor authentication.

Trusted Agency, System or Network. An IT system or network that is recognized automatically as reliable, truthful, and accurate without continual validation or testing.

Untrusted. Characterized by absence of trusted status. Assumed to be unreliable, untruthful, and inaccurate unless proven otherwise.

Vulnerability. Relates to risk of attack. In IT terms, vulnerability describes points of risk to penetration of security barriers. Awareness of potential vulnerability is very important to designing ever more effective defenses against attack by unauthorized parties.

Vulnerability Assessment. A comprehensive analysis that attempts to define, identify, and classify the security holes (vulnerabilities) in a system, network, or communications infrastructure within the assessment scope.

REVISION HISTORY

Date	Action taken
December 2017	On 12/11/2017, the Technology Services Board approved the adopted standard with no changes.
November 2017	Creation of new Purpose section. New wording added to Introduction to emphasize that Standards apply to any system storing, processing or transmitting state data, regardless of location. Enhancements and clarification to classification of Category 3 data. Creates new encryption requirements for systems outside the SGN or any new system implemented on the SGN in Section 4.3. Major revision to Media Handling and Disposal section. Definition for SGN added. Recommended for approval by the TSB Policy and Portfolio Subcommittee on 11/09/2017. Adopted by the State CIO on 11/13/2017 pending approval of the full Technology Services Board. This policy is in effect with adoption.
August 19, 2013	Wording change to section 1.4(3) and addition of new section, 1.4(4). The purpose is to remove the requirement that all employees be required to be trained on OCIO Security Policy and Standard and the agency's security policies and procedures, but stipulates such requirement for personnel assigned responsibilities defined in the agency's IT Security Program.
April 10, 2012	Technical correction to clear up confusion about the meaning of 6.2.7 (b). Added the term "classes" to modify the phrase "Contain at least three unique characters." The purpose is to clarify that the pass code must contain some combination of at least three of the following: uppercase letters, lowercase letters, numerals, and special characters.
March 28, 2012	The standards are changed to add an additional subsection (7) following Section 6.2 (6). A new definition is added for the term "Tablet PC"; and "tablet PCs" are added to the examples listed in the definition of Mobile Device.
October 2011	Standards reformatted for migration to Office of Chief Information Officer. Reflected changes in responsibilities from DIS to CTS. Highlighted sections currently under review.

August 13, 2009	The revision was designed to close the gap between the existing Standards and current industry security best practices to mitigate the breadth and sophistication of IT security threats. Many of the security controls and the organization of the updated standards are based on IT security best practice frameworks from the recognized IT standards bodies.
January 10, 2008	Added statement #9 requiring comparable security policies for entities wishing to connect to state systems.
November 2006	Revised format; revised Applies To section content; added requirement to submit audit results to the ISB in statement #7; revised annual compliance filing date to match agency's budget submittal date in statement #8; removed language redundant with Information Technology Security Standards, Policy No. 401-S3; simplified and clarified language throughout.
April 2002	Revised format; added language to policy statement #5 on Internet applications; added language to policy statement #8 on agencies providing annual certification to the ISB.
October 6, 2000	Initial effective date.
July 14, 2000	Policy adopted.

CONTACT INFORMATION

For questions about this policy, please contact your OCIO Information Technology Consultant. For technical security questions or to request a Design Review and Risk Assessement, please contact the state Chief Information Security Officer at Consolidated Technology Services.

APPROVING AUTHORITY

Rob St. John, Acting Chief Information Officer

ATTACHMENT C

OFFICE OF THE CHIEF INFORMATION OFFICER'S STANDARD NO. 141.10 SECURING INFORMATION TECHNOLOGY ASSETS

PROCEDURE RESULTS

The agreed-upon procedures and associated results are as follows:

1. **Agency IT Security Program – Documentation**
   a. Confirm the organization has developed a written IT Security Program. (OCIO Standard 141.10, §1.1)

      Results: [Describe results]

2. **Agency IT Security Program – IT Risk Assessment**
   a. Confirm a formal, written, IT Risk Assessment process has been developed. (OCIO Standard 141.10, §1.2(1))

      Results: [Describe results]

   b. Obtain a list of systems that use Category 3 or 4 data. Select up to five systems and inspect documentation to confirm the organization has conducted an IT Risk Assessment for each system in the past three years. (OCIO Standard 141.10, §1.2(2) and 1.2(8))

      Results: [Describe results]

   c. Select one IT Risk Assessment from the previous procedure and confirm it addresses all elements of OCIO Standard 141.10, §1.2(3)-(7) and (9).

      Results: [Describe results]

   d. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §1.2.1, first section (1)-(4).

      Results: [Describe results]

   e. Select a system that uses Category 3 or 4 data, or an infrastructure project that met one or more of the conditions of OCIO Standard 141.10, §1.2.1, first section (1) through (4), and inspect the Security Design Review and Risk Assessment completed by CTS (WATech).

      Results: [Describe results]

   f. If there were recommendations from the Security Design Review or Risk Assessment, inquire whether the organization's IT management has responded to the recommendations or has submitted an appeal. (OCIO Standard 141.10, §1.2.1, third section (3))

      Results: [Describe results]

3. **Agency IT Security Program – IT Security Assessment**
   a. Confirm the organization has established a schedule to test its systems, applications, and IT infrastructure assets. (OCIO Standard 141.10, §1.3 (1))

      Results: [Describe results]

   b. Inspect documentation to confirm the organization has reviewed a sample of systems and applications that use Category 3 or 4 data at least once in the last three years. (OCIO Standard 141.10, §1.3(2))

      Results: [Describe results]

   c. Select up to five systems that use Category 3 or 4 data or infrastructure projects that have been added or significantly modified in the last three years and inspect documentation to confirm the organization completed an IT Security Assessment for each of them. (OCIO Standard 141.10, §1.3(3))

Results: [Describe results]

d. Inquire with the organization's IT management about whether control weaknesses identified in the IT Security Assessments from the previous agreed-upon procedure have been addressed. (OCIO Standard 141.10, §1.3(4))

Results: [Describe results]

e. Inquire with the organization's IT management about whether any organization applications, network devices or significant infrastructure were upgraded or modified without an updated IT Security Assessment being completed. (OCIO Standard 141.10, §1.3(3))

Results: [Describe results]

4. Agency IT Security Program – Education and Awareness

a. Inspect the organization's IT Security Program and confirm it requires annual security training. (OCIO Standard 141.10, §1.4(3))

Results: [Describe results]

b. Select one person with security responsibilities and inspect documentation to confirm the person completed the annual security awareness training. (OCIO Standard 141.10, §1.4(3))

Results: [Describe results]

5. Agency IT Security Program – Compliance

a. Select the most recently implemented system or IT infrastructure and inspect documentation that confirms the organization satisfied the requirements of OCIO Standard 141.10, §1.5(2)-(3).

Results: [Describe results]

b. Obtain the IT Risk Assessment over the previously selected system or infrastructure. Select one risk and inquire with IT management as to the controls used to mitigate that risk. (OCIO Standard 141.10, §1.5(4))

Results: [Describe results]

c. Inspect the most recent contract with a non-State agency IT vendor and confirm OCIO compliance expectations are included in the contract terms. (OCIO Standard 141.10, §1.5(5)

Results: [Describe results]

d. Inspect documentation of the last written statement of compliance with ITS Security Standards, or Nationwide Cybersecurity Review (NCSR), submitted to OCIO. (OCIO Standard 141.10, §1.5(6))

Results: [Describe results]

e. Inspect the organization's completed IT Security Non-compliance/Deviation Forms and confirm they were approved by the state CIO. (OCIO Standard 141.10, §1.5(7))

Results: [Describe results]

6. Agency IT Security Program – Audit

a. Inspect documentation to confirm the most recent OCIO engagement was completed within the last three years and was performed by an independent party. (OCIO Standard 141.10, §1.6(1))

Results: [Describe results]

b. Select one nonconformity from the results of the most recent OCIO engagement and inspect documentation to confirm corrective action has been planned and is being tracked. (OCIO Standard 141.10, §1.6(7)-(8))

Results: [Describe results]

7. Agency IT Security Program – Maintenance

a. Inspect documentation to confirm the organization performed annual maintenance and review of the organization's IT Security Program. (OCIO Standard 141.10, §1.7(1))

Results: [Describe results]

8. Personnel Security

a. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §2(7)-(10).

Results: [Describe results]

b. Inspect the most recently executed IT contract and confirm it requires compliance with OCIO and the organization's own security policies, standards and requirements. (OCIO Standard 141.10, §2(8))

Results: [Describe results]

c. Inquire with the organization's IT management regarding whether inappropriate staff or contractor conduct or lack of security awareness was the root cause for any security incidents. If it was, inquire whether sanctions were issued at the time of the security violation. (OCIO Standard 141.10, §2(6))

Results: [Describe results]

9. Physical and Environmental Protection

a. Inspect the organization's IT Security Program and confirm it covers all facilities with IT assets and addresses all elements of OCIO Standard 141.10, §3.1.

Results: [Describe results]

10. Data Security – Data Classification

a. Inspect the organization's IT Security Program regarding data classification, and confirm the defined classification of information is consistent with the categories outlined in OCIO Standard 141.10, §4.1(1)-(4).

Results: [Describe results]

11. Data Security – Data Sharing

a. Inspect the data sharing agreement template and the most recent activated data sharing agreement for Category 3 or 4 data and confirm each addresses all elements of OCIO Standard 141.10, §4.2(1-7).

Results: [Describe results]

12. Data Security – Secure Management and Encryption of Data

a. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §4.3.

Results: [Describe results]

b. Obtain and confirm the organization has a list of applications using or storing Category 3 or 4 data.

Results: [Describe results]

c. Select one application, implemented after November 13, 2017, that uses or stores Category 3 or 4 data. Through observation or inspection, confirm data is encrypted using industry standard algorithms validated by the National Institute of Standards and Technology (NIST) Cryptographic Algorithm Validation Program. (OCIO Standard 141.10, §4.3)

Results: [Describe results]

13. Data Security – Secure Data Transfer

a. Inquire with the organization's IT management whether Category 3 or 4 data is transmitted outside of the State Government Network (SGN). If it is, select an application and confirm the data is encrypted during transmission using a method that complies with OCIO Standard §4.4(4).

Results: [Describe results]

14. Network Security – Secure Segmentation

a. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §5.1.1(1)-(9).

Results: [Describe results]

b. Inspect the organization's IT Security Program and confirm it addresses OCIO Standard 141.10, §5.1.2(1) and (3).

Results: [Describe results]

c. Inspect documentation confirming that the firewall configurations have been reviewed within the last year. (OCIO Standard 141.10, §5.1.2(4))

Results: [Describe results]

d. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §5.1.3.

Results: [Describe results]

e. Inquire with the organization's IT management whether non-console administrative access is encrypted. (OCIO Standard 141.10, §5.1.3(2))

Results: [Describe results]

15. Network Security – Restricted Services

a. Inspect the organization's IT Security Program and confirm it addresses the restricted services listed in OCIO Standard 141.10, §5.2.

Results: [Describe results]

b. Obtain a list of all allowed restricted services. Inspect documentation to confirm each was approved by management. (OCIO Standard 141.10, §5.2)

Results: [Describe results]

16. Network Security – External Connections

a. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §5.3(1)-(2).

Results: [Describe results]

b. Inquire with IT management regarding whether there are any connections between internal networks and external networks that are exempt from connecting through a CTS (WaTech)-managed security layer. (OCIO Standard 141.10, §5.3(3))

Results: [Describe results]

17. Network Security – Wireless Connections

a. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §5.4(2)-(3).

Results: [Describe results]

b. Inquire with the organization's IT management about whether monitoring for wireless devices is performed as defined by OCIO Standard 141.10, §5.4(2)f and (3)f.

Results: [Describe results]

18. Network Security – Security Patch Management

a. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard §5.5.

Results: [Describe results]

b. Select one device from an inventory of devices attached to the organization's local area and rouge wireless networks Confirm the most current patch was installed. (OCIO Standard 141.10, §5.5(6) and (9))

Results: [Describe results]

c. Inquire with organization's network management regarding:

- How timely notification of the last patch deployment was received. (OCIO Standard 141.10, §5.5(3))

  Results: [Describe results]
- How criticality of the last patch was assessed. (OCIO Standard 141.10, §5.5(4))

  Results: [Describe results]
- How the last patch was tested before deployment. (OCIO Standard 141.10, §5.5(5))

  Results: [Describe results]
- How the devices were regularly verified to be following the patch management process. (OCIO Standard 141.10, §5.5(7))

  Results: [Describe results]

19. Network Security – System Vulnerabilities

a. Inquire with IT Management whether they subscribe to alert services to identify newly discovered security vulnerabilities (OCIO Standard 141.10, §5.6(1))

Results: [Describe results]

b. Inspect the organization's IT Security Program and confirm it addresses OCIO Standard 141.10, §5.6(2)-(3).

Results: [Describe results]

20. Network Security – Protection from Malicious Software

a. Inspect the organization's IT Security Program and confirm it addresses OCIO Standard 141.10, §5.7(1), (2) and (4).

Results: [Describe results]

b. Inquire with the organization's IT management to identify which anti-malware the organization is currently using and the date of the last update. (OCIO Standard 141.10, §5.7(1) and (3))

Results: [Describe results]

21. Network Security – Mobile Computing

a. Inspect the organization's IT Security Program related to use of mobile data storage devices and confirm it addresses all elements of OCIO Standard 141.10, §5.8(2)-(3).

Results: [Describe results]

b. Select two mobile devices from an inventory list of mobile devices that access or process Category 3 or 4 information and confirm they are encrypted using industry standard algorithms or cryptographic modules validated by the National Institute of Standards and Technology (NIST). (OCIO Standard 141.10, §5.8(2))

Results: [Describe results]

22. Access Security – Access Management

a. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §6.1.1(1)-(4) and (6).

Results: [Describe results]

b. Through observation or inspection, confirm that access controls to mainframe or key systems are based on least privilege concepts. (OCIO Standard 141.10, §6.1.1)

Results: [Describe results]

c. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §6.1.2(1)–(5) and (8).

Results: [Describe results]

d. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §6.1.3.

Results: [Describe results]

e. Inspect the Group Policy configuration settings that detect an inactive Windows session, and confirm the settings address disabling or reauthorizing inactive sessions after a defined period of inactivity. (OCIO Standard 141.10, §6.1.3(1))

Results: [Describe results]

f. Obtain a list of all non-Windows applications that use Category 3 or 4 data and require end-user log-on. Select one application from the list, inspect the system's configuration settings, and confirm they address disabling or reauthorizing inactive sessions after a defined period of inactivity. (OCIO Standard 141.10, §6.1.3(1))

Results: [Describe results]

g. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §6.1.4.

Results: [Describe results]

h. Select one system that uses Category 3 or 4 data and inquire with the organization's IT management:

- How often the system's user access rights are reviewed. (OCIO Standard 141.10, §6.1.4(1))

  Results: [Describe results]

- How often privileged activities, such as granting of escalated rights, are monitored. (OCIO Standard 141.10, §6.1.4(2))

  Results: [Describe results]

23. Access Security – Password Requirements

a. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §6.2.

Results: [Describe results]

b. Through observation or inspection, confirm password rules are configured in accordance with OCIO Standard 141.10, §6.2(5)a-c.

Results: [Describe results]

24. Access Security - Authentication

a. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §6.3.1 for Types 3(1)-(4) and Types 4 and 5.

Results: [Describe results]

b. Obtain a list of all systems using Category 3 or 4 data that can be accessed by external parties (non-state employees) from resources outside of the SGN. Select one system from the list and determine which type of authentication method is defined for the system. (OCIO Standard 141.10, §6.3.1 Type 6(1)-(2))

Results: [Describe results]

c. c. Inspect the organization's IT Security Program and confirm it addresses all applicable elements of OCIO Standard 141.10, §6.3.2.

Results: [Describe results]

25. 25. Access Security – Remote Access

a. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §6.4.

Results: [Describe results]

b. Through observation or inspection, confirm that remote access controls are in place in accordance with the organization's IT Security Program. (OCIO Standard 141.10, §6.4(1)a).

Results: [Describe results]

c. Inquire with IT management whether the organization uses any means other than the State's common remote access services such as IPsec or SSL VPN when remotely accessing resources and services on the SGN. (OCIO Standard 141.10, §6.4(5)).

Results: [Describe results]

26. Application Security – Planning and Analysis

a. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §7.1.

Results: [Describe results]

b. Through observation or inspection, confirm controls are in place to manage the installation of software on operational systems, including, but not limited to, servers and workstations. (OCIO Standard 141.10, §7.1(2))

Results: [Describe results]

c. Inquire with the organization's IT management whether access to program source code is restricted to only those individuals whose job responsibilities require such access. (OCIO Standard 141.10, §7.1(3))

Results: [Describe results]

d. Inspect the most recent contract to outsource software development and confirm it contains specific requirements for outsourced software development that protect the integrity and confidentiality of the source code. (OCIO Standard 141.10, §7.1(4) and (7))

Results: [Describe results]

27. Application Security – Application Development

a. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §7.2.

Results: [Describe results]

b. Select one system that uses Category 3 or 4 data. Confirm different individuals are assigned to the development, test and production environments and observe whether separate development, test and production environments are utilized. (OCIO Standard 141.10, §7.2(2))

Results: [Describe results]

28. Application Security – Application Maintenance

a. Select the most recent change to an application that uses, processes or stores Category 3 or 4 data and inspect documentation to confirm the organization reviewed the change to reduce adverse impacts. (OCIO Standard 141.10, §7.3(1))

Results: [Describe results]

29. Application Security – Vulnerability Prevention

a. Inspect the organization's IT Security Program and confirm it addresses OCIO Standard 141.10, §7.4(1).

Results: [Describe results]

30. Application Security – Application Service Providers

a. Inquire with the organization's IT management whether the outsourced third-party vendor or organization selected in the Agency IT Security Program – Compliance section follows all elements of OCIO Standard 141.10, §1.5. (OCIO Standard 141.10, §7.5.)

Results: [Describe results]

31. Operations Management – Change Management

a. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §8.1.

Results: [Describe results]

b. Select the last change to an IT asset and confirm the change was approved and accepted prior to deployment. (OCIO Standard 141.10, §8.1(3))

Results: [Describe results]

32. Operations Management – Asset Management

a. Inspect the organization's current inventory list of major components in the production IT environment and confirm all listed information-processing assets are assigned an owner and whether the components are inside, or outside of, the SGN. (OCIO Standard 141.10, §8.2(1)-(2))

Results: [Describe results]

33. Operations Management – Media Handling and Disposal

a. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §8.3(1).

Results: [Describe results]

b. Inspect the most recent disposal record for storage media containing Category 3 or 4 data and confirm the supporting documentation addresses the elements specified in OCIO Standard 141.10, §8.3(1).

Results: [Describe results]

34. Operations Management – Data and Program Backup

a. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §8.4.

Results: [Describe results]

b. Obtain a list of media backup locations and confirm offsite locations are used. (OCIO Standard 141.10, §8.4(5))

Results: [Describe results]

35. Electronic Commerce

a. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §9.

Results: [Describe results]

36. Security Monitoring and Logging – Logging Policies

a. Inspect the organization's IT Security Program and confirm it addresses all elements of OCIO Standard 141.10, §10.1.

Results: [Describe results]

b. Inquire with the organization's IT management whether audit logs are periodically analyzed for all applications in accordance with the organization's strategy. (OCIO Standard 141.10, §10.1(2))

Results: [Describe results]

37. Security Monitoring and Logging – Logging Systems

a. Obtain a list of systems that access or process Category 3 or 4 data. Select one system and, through observation or inspection, confirm that logging is enabled and that it is recording for the events listed in OCIO Standard 141.10, §10.2(3).

Results: [Describe results]

38. Security Monitoring and Logging – Intrusion Detection and Prevention

a. Inspect the organization's IT Security Program and identify how the organization ensures that Intrusion Detection and Prevention systems are configured to log information continuously. (OCIO Standard 141.10, §10.3)

Results: [Describe results]

39. Incident Response

a. Inspect the organization's Incident Response plan and confirm it addresses all elements of OCIO Standard 141.10, §11(2).

Results: [Describe results]

b. Inspect documentation of the organization's most recent test of its Incident Response plan and confirm it was completed within the last year. (OCIO Standard 141.10, §11(3))

Results: [Describe results]

c. Inquire with IT management whether the most recent incident involved the unauthorized release of Category 3 or 4 data. If applicable, inspect documentation to confirm the organization complied with notifications as required by the state breach notification statute, RCW 42.56.590 Personal Information. (OCIO Standard 141.10, §11)

Results: [Describe results]