Washington State Auditor's Office
Troy Kelley
Independence • Respect • Integrity

Performance Audit

Opportunities to Improve State IT Security

December 15, 2014

Washington has taken significant measures to protect the state from cyber threats, but opportunities exist to strengthen the state's information technology (IT) security posture to reduce security risk. We found that the state's IT security standards align closely with leading practices, including its statewide approach to IT security management. We also found that agencies are not in full compliance with these standards. Through our compliance and application security testing, we found numerous issues at five selected agencies. We also found significant discrepancies between agency-reported compliance with state standards and our own results. This indicates the monitoring and reporting process currently used to develop a statewide picture of Washington's IT security risks is not functioning as intended.

Audit Number: 1012957

Table of Contents

The mission of the Washington State Auditor's Office

The State Auditor's Office holds state and local governments accountable for the use of public resources.

The results of our work are widely distributed through a variety of reports, which are available on our website and through our free, electronic **subscription service**.

We take our role as partners in accountability seriously. We provide training and technical assistance to governments and have an extensive quality assurance program.

For more information about the State Auditor's Office, visit **www.sao.wa.gov**.

Americans with Disabilities

In accordance with the Americans with Disabilities Act, this document will be made available in alternative formats. Please email Communications@sao.wa.gov for more information.

State Auditor's Office contacts

State Auditor Troy Kelley
360-902-0360, Auditor@sao.wa.gov

Chuck Pfeil, CPA :: Director of State & Performance Audit
360-902-0366, Chuck.Pfeil@sao.wa.gov

Lou Adams, CPA :: Deputy Director of Performance Audit
360-725-5577, Louella.Adams@sao.wa.gov

Erin Laska, MPA, CIA :: Senior Performance Auditor
360-725-5555, Erin.Laska@sao.wa.gov

Thomas Shapley :: Deputy Director of Communications
360-902-0367, Thomas.Shapley@sao.wa.gov

To request public records

Public Records Officer
360-725-5617, PublicRecords@sao.wa.gov

Executive Summary

Opportunities exist for Washington to further protect the confidential information entrusted to the state by improving IT security

While Washington has taken significant measures to protect the state from cyber threats, opportunities exist to strengthen the state's information technology (IT) security posture and reduce security risk. We found that the state's IT security standards align closely with leading practices, including its statewide approach to IT security management. We also found that agencies are not in full compliance with these standards. Through our compliance and application security testing, we found numerous issues at five selected agencies. We also found significant discrepancies between agency-reported compliance with state standards and our own results. This indicates the monitoring and reporting process currently used to develop a statewide picture of Washington's IT security risks is not functioning as intended.

Responsibility for securing the state's IT environment is shared

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

Testing identified non-compliance issues and security weaknesses

While we found the state has established strong IT security standards, our audit also found state agencies are not fully complying with these standards. We tested five of the 11 state IT security standards at five selected agencies, and found close to 350 instances – out of 1,035 security standard components tested – in which these agencies are not in full compliance.

Around three-quarters of the issues found were due to a lack of documentation, which typically represents less of a security risk than a lack of implementation. The areas where we found the most noncompliance issues were:

- Application security, where we found issues such as a lack of documentation for application changes
- Data security, where we found issues such as inadequate use of encryption
- Operations management, where we found issues such as a failure to send backup data to an offsite location.

Our audit focused on OCIO IT security standards 4 through 8, which are most critical for protecting the state from cyber threats

We conducted application security tests to assess whether applications and their underlying infrastructure were vulnerable to an attack. We found a total of 46 issues at the five selected state agencies; seven were rated critical (extreme impact to entire entity and almost certain to be exploited), and 12 were rated high (major impact to entire entity or individual program and can be exploited by attacker with minimal skills). All five agencies worked quickly to start fixing the issues we identified and some agencies reported using the information to improve other applications not included in testing.

The state's IT security standards align closely with leading practices, but improvements could be made

We found no significant gaps between the state's IT security standards and leading practices. We did find a few areas where the OCIO could improve the standards by adding more details from leading practices, or clarifying language to ensure greater consistency in agency compliance. Examples of improvements include:

- Clarifying expectations for agency data-sharing agreements to ensure the safeguarding of confidential data
- Clarifying agency requirements for ensuring that external service providers meet state IT security standards
- Adding environmental protection requirements for agency data centers, such as emergency power, lighting, temperature and humidity controls.

The state's process to monitor agency IT security compliance could be improved

The state has an appropriate IT security framework that includes good statewide IT security standards, as well as a process to monitor and oversee compliance with those standards. However, the significant difference between what agencies reported to the OCIO and what we found during our audit points to the need for improvements to monitoring and oversight of agency compliance. This is particularly important because without complete and accurate information from state agencies, those responsible for IT security do not have the information needed to support those agencies, or effectively monitor IT security for the state.

Recommendations

To help ensure the state maintains the integrity of its IT networks and systems, and to better protect the confidential information entrusted to the state, we make the following recommendations:

To the five selected state agencies:

- Continue remediating gaps identified where agency practices or documented policies are not in full compliance with the state's IT security standards, and weaknesses identified through our application security testing.
- Provide accurate and complete information on agency compliance with, and any deviations from, the state's IT security standards in the agency's annual verification letter to the Office of the Chief Information Officer.

Reporting detailed results

IT security information is exempt from public disclosure in accordance with RCW 42.56.420 (4).

To protect the IT security of our state, this report does not include the names of the five selected agencies, nor any detailed descriptions of our findings. Disclosure of such details could potentially be used by a malicious attacker against the state.

Detailed findings and recommendations were provided to each agency we reviewed, and to the OCIO and CTS.

To the state's Chief Information Officer:

- Revise the state's IT security standards to more closely align with leading practices, and clarify those where our review found multiple agencies did not comply.
- Evaluate and revise the current process used for agencies to annually report the status of their compliance with, and deviations from, the state's IT security standards to ensure the process provides meaningful and accurate information. While doing so, evaluate what is needed to help agencies understand how to technically comply with the standards and to monitor annual agency compliance.
- Continue to collaborate with the state's Chief Information Security Officer to develop methods to help state agencies better understand the importance of complying with the state's IT security standards, and how best to do so.

To the state's Chief Information Security Officer:

- Continue to collaborate with the state's Office of the Chief Information Officer to develop methods to help state agencies better understand the importance of complying with the state's IT security standards, and how best to do so.

Introduction

Information technology security continues to receive increased attention as threats to IT systems become more numerous and sophisticated. The National Association of State Chief Information Officers reported IT security is the number one priority in 2014 for their members. The breadth and scope of state government activities, from education and law enforcement to regulatory oversight and health services, means that the state is entrusted with vast amounts of confidential information. Virtually all of this data – including Social Security numbers, license numbers and credit card details – is stored in state databases, making state IT systems a tempting target for hacking and cyber crime. As a result, states and their citizens are at increased risk from cyber threats.

According to the Washington State Chief Information Security Officer, the state is experiencing increasing volumes of sophisticated attacks against its networks. These attacks are often targeted and persistent, and designed to disrupt important government processes or obtain valuable information. With the increasing availability of government services online and the interconnectedness of agency systems, an effective statewide IT security approach, with strong IT security programs at each agency, is vital to helping ensure the entire state network is secure. If the state fails to maintain the integrity of its IT systems and protect data resources, consequences can include financial losses, problems delivering vital government services, and erosion of public confidence.

Media reports of significant security breaches demonstrate the potential costs to states. A 2014 study, by the Ponemon Institute, estimated the average cost for each government record lost is $172, and suggested that governments have a one-in-four chance of experiencing a material data breach (more than 10,000 records) in the next two years. Locally, a 2013 breach of the Washington Administrative Office of the Courts may have compromised about 160,000 Social Security numbers and 1 million drivers' license numbers.

In light of these risks, we wanted to determine whether there were opportunities to improve Washington's IT security posture and further protect the state's confidential information by asking the following questions:

- Do the state's IT security standards align with leading practices?
- Are selected state agencies in compliance with the state's IT security standards?
- Are those agencies adequately protecting confidential information from cyber threats?

Background

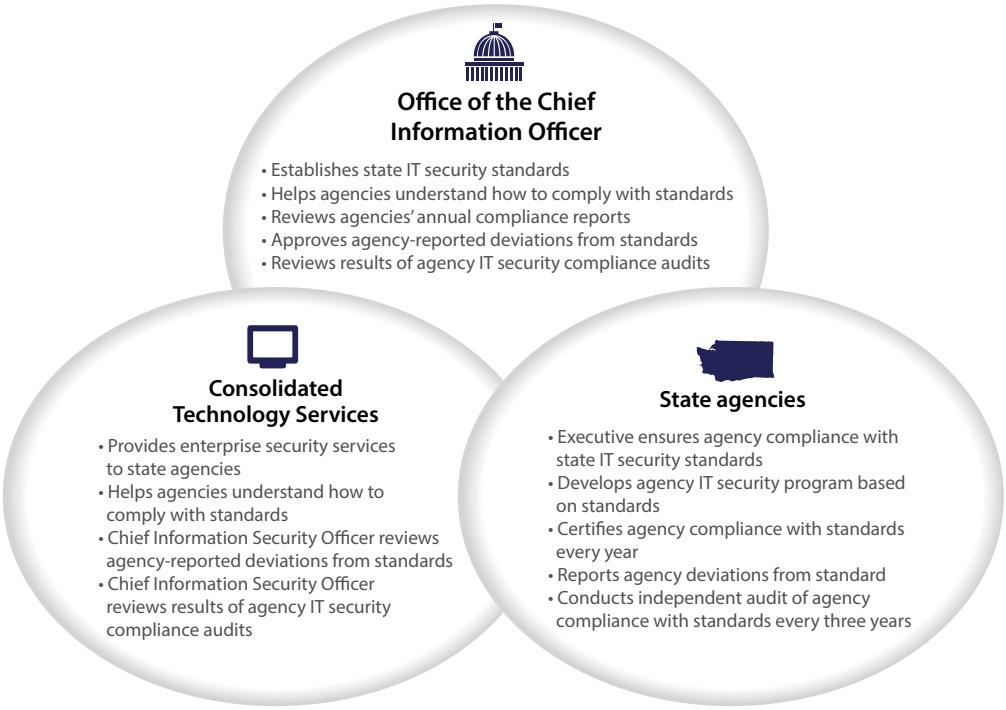
The National Association of State Chief Information Officers consistently promotes a statewide enterprise approach to IT security oversight. Under this approach, state agencies work cooperatively within a decentralized state government framework. To be effective, an enterprise approach starts with IT security policies and standards all agencies must follow and use as a basis for their own agency-specific IT security programs. In a computing environment such as state government, where agencies are connected, following common IT security standards helps ensure a secure IT environment for all agencies. An enterprise approach should also include a process to monitor and test agency compliance with state IT security policies and standards.

Responsibility for securing the state's IT environment is shared

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

To help ensure agencies are in compliance with the state's IT security standards, agency executives are required to annually certify to the Office of the Chief Information Officer that they are following the state's security standards and, if not, report any deviations from the standard. Every three years, agencies are required to conduct an independent audit of their IT security programs. **Exhibit 1** provides additional details on controls in place to help ensure agencies comply with the state's IT security standards.

Exhibit 1 - Key management controls for ensuring state agency IT security compliance



The Office of the Chief Information Officer established minimum requirements for state agency IT security programs in Standard 141.10, "Securing Information Technology Assets." As **Exhibit 2** illustrates, it addresses 11 broad IT security standards. These 11 standards include just over 300 individual components agencies must comply with as they develop their own IT security program tailored to their unique operating environments. **Appendix B** contains the full text of the OCIO's Standard 141.10.

Washington consolidated IT security services under CTS to reduce redundancies and offer state agencies valuable security services and expertise to which they might not otherwise have access. CTS has a leadership role in identifying and assisting agencies in mitigating security risks within the state network. It is also responsible for the security infrastructure, which protects the state's computer network from cyber threats such as hackers and viruses. For example, CTS recently offered an internet proxy service that provides increased security for state employees searching the Internet by preventing access to high-risk Internet sites known for viruses or malicious activities. CTS also offers a vulnerability assessment tool that helps agencies identify system and application vulnerabilities. Additionally, the CTS Security Operations Center alerts agency IT security personnel about potential security incidents and provides incident response services.

Exhibit 2 - The OCIO's IT Security Standards are organized into11 broad areas

Scope and Methodology

To determine whether there were opportunities to improve the IT security posture and further protect the state's confidential information, we asked the following questions:

- Do the state's IT security standards align with leading practices?
- Are selected state agencies in compliance with the state's IT security standards?
- Are those agencies adequately protecting confidential information from cyber threats?

To help conduct the audit, we hired subject matter experts with expertise in assessing IT security standards and controls, penetration testing, and conducting IT security audits.

Comparing the state's IT security standards to leading practices

To determine whether the state's IT security standards align with leading practices, we conducted a gap analysis to identify areas where the state standards could benefit from revision to make them stronger. Appendix B contains a copy of the state's IT security standards. To conduct our gap analysis, we primarily relied on the IT security standards developed and used by the U.S. Government. These standards are written and maintained by the National Institute of Standards and Technology (NIST). We used Special Publication 800-53, Revision 4 "Security and Privacy Controls for Federal Information Systems and Organizations" for our comparisons.

We also compared the state's IT security standards to those developed by the International Organization for Standardization (ISO), specifically ISO 27001. Both NIST and ISO IT security standards are viewed as leading practices by the IT security industry, and are used as the basis for developing more detailed standards or policies and procedures for both government entities and private industry. **Appendix C** shows our comparison of the state's IT security standards to leading practices. **Appendix D** includes the results of our gap analysis.

Selecting state agencies for testing

To determine whether state agencies were in compliance with the state's IT security standards, and if they are adequately protecting the state's confidential information, we judgmentally selected five agencies for detailed compliance and application security testing. The factors we used to select these agencies were developed in consultation with the state's Office of the Chief Information Officer and Chief Information Security Officer. Those factors included:

- **Agency size** – As size affects an agency's IT resources and structure, and its ability to respond to an attack, we selected two large, two medium and one small agency based on the number of employees.
- **Data type** – Agency security programs should be driven by the type of confidential information they must protect. The agencies we selected represent a cross-section of confidential data such as financial and personally identifiable information.

Reporting detailed results

IT security information is exempt from public disclosure in accordance with RCW 42.56.420 (4).

To protect the IT security of our state, this report does not include the names of the five selected agencies, nor any detailed descriptions of our findings. Disclosure of such details could potentially be used by a malicious attacker against the state.

Detailed findings and recommendations were provided to each agency we reviewed, and to the OCIO and CTS.

- **Appeal** – Some agencies are more likely to be targeted for malicious attacks than others. In our selection, we considered whether certain agencies had received a disproportionate number of outside attacks.
- **Other reviews** – We excluded agencies that had recently completed or were in the process of having a similar independent review.

Compliance testing

To determine compliance with IT security standards at the five selected state agencies, we focused our work on five standards that are critical for protecting the state from cyber threats. After consulting with the state's Office of the Chief Information Officer and Chief Information Security Officer, we selected data security, network security, access security, application security, and operations management for our review. Within those five security standards, we tested 207 different components at each of the five agencies. Those components are detailed in the state's IT security standards in **Appendix B**. Between two and five critical high risk applications were selected for compliance testing at each agency. Our compliance testing included: review of the agencies' applicable policies, procedures and practices; review of the accompanying documentation; observation of IT security controls; and interviews with agency staff.

We compared the results of our compliance testing across the agencies to identify common problems that could indicate a need for greater clarity in the state's IT security standards. We also compared our compliance results with the annual verification letters sent to the Office of the Chief Information Officer, to determine if agencies reported all their deviations as required.

To help understand why state agencies did not fully comply with the five state IT security standards we selected, we interviewed officials at the selected agencies as well as at the Office of the Chief Information Officer, and the state's Chief Information Security Officer.

Application security testing

To determine whether the five selected state agencies were adequately protecting their confidential information from external threats, we conducted security tests on agency applications and their underlying infrastructure, including identifying and assessing vulnerabilities and determining if vulnerabilities could be exploited. To help ensure a real-world response to application security testing, only agency executives and a few key staff knew about the testing beforehand. At three agencies our testing included social engineering tests.

We selected a mission-critical application at each of the agencies for application testing; at four, we tested a web-facing application, because the number of web-facing applications is increasing as the state offers more services to its citizens through the Internet. The subject matter experts who conducted the testing ranked the level of risk associated with ease and probability of the identified weakness being exploited based on their professional experience.

We gave the agencies the results of the tests as they were completed, then conducted follow-up testing to ensure agencies successfully mitigated the identified weaknesses the agencies told us they had remedied. We also compared the results of the application security testing for each agency to their compliance testing results to see if there was a connection between noncompliance with a state IT security standard and a known system weakness.

An **IT application** is a software program, or group of programs designed to accomplish a task for an end user. A word processor such as Microsoft Word is an example of an application.

Web-facing applications are programs connected to the internet to provide the public with information or services, such as a banking application that allows you to check your bank account balance from home. These web-facing applications are more susceptible to attack than internal agency applications used to conduct agency business and not accessible through the internet.

Audit performed to standards

We conducted this performance audit under the authority of state law (RCW 43.09.470), approved as Initiative 900 by Washington voters in 2005, and in accordance with Generally Accepted Government Auditing standards (December 2011 revision) issued by the U.S. Government Accountability Office. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. See **Appendix A**, which addresses the I-900 areas covered in the audit.

Next steps

Our performance audits of state programs and services are reviewed by the Joint Legislative Audit and Review Committee (JLARC) and/or by other legislative committees whose members wish to consider findings and recommendations on specific topics. Representatives of the State Auditor's Office will review this audit with JLARC's Initiative 900 Subcommittee in Olympia. The public will have the opportunity to comment at this hearing. Please check the JLARC website for the exact date, time, and location (**www.leg.wa.gov/JLARC**). The State Auditor's Office conducts periodic follow-up evaluations to assess the status of recommendations and may conduct follow-up audits at its discretion.

Audit Results

Opportunities exist for Washington to further protect the confidential information entrusted to the state by improving IT security

While Washington has taken significant measures to protect the state from cyber threats, we found many opportunities to strengthen the state's IT security posture and reduce IT security risks. Although the state's IT security standards align closely with leading practices, including its statewide approach to IT security management, we found that agencies do not fully comply with those standards, nor fully communicate their security weaknesses to the Office of the Chief Information Officer. Through compliance and application security testing, we found numerous noncompliance issues at all the audited entities. We also found a significant discrepancy between agency-reported compliance with state standards and the results of our tests, which indicates the monitoring and reporting process currently used to develop a statewide picture of Washington's IT security risks is not functioning as intended.

All audited agencies were given detailed results of our tests, and are already taking steps to address the issues we raised. We also shared our detailed results with the Office of the Chief Information Officer and Consolidated Technology Services.

While the state's IT security standards align closely with leading practices, improvements could be made

We found the state's IT security standards closely align with leading practices, with no significant gaps. We also concluded the Office of the Chief Information Officer could strengthen some standards by adding details from leading practices. For example, the state's physical and environmental protection standard does not include environmental protection requirements, such as emergency power, lighting, temperature and humidity controls, for agency data centers. The full result of our comparison of the state's IT security standards to leading practices is available as a link to our website in **Appendix C**.

When we examined the results of our compliance testing for patterns of noncompliance, we found several areas where further clarification could help ensure consistent compliance with standards. For example, agencies need to improve data-sharing agreements to help ensure the entities they share confidential data with apply appropriate safeguards. We also found the audited agencies that rely on contractors to provide IT services did not fully understand the related standard that required them to ensure these contractors protected the state's data.

Our detailed recommendations to improve the state's IT security standards are set out in **Appendix D**. We have already provided these recommendations to the Office of the Chief Information Officer which is working to address them and plans to release an update to the standards reflecting these changes within a year.

Assessing IT security at the State Auditor's Office

While the State Auditor's Office conducted this performance audit, we also engaged an independent IT audit firm to conduct a thorough assessment of our own IT security program. The Office underwent application security testing and a compliance review against all 11 components in the OCIO's state IT security standard 141.10.

This assessment identified areas for improvement. In response, our Office hired an agency Chief Information Security Officer and developed a plan to remediate all identified issues.

Selected agencies are not in full compliance with state IT security standards

While the state established strong IT security standards, our audit found state agencies are not fully complying with these standards. The highlighted bars in **Exhibit 3** show the five standards we reviewed, which are regarded by the Chief Information Officer and the state's Chief Information Security Officer as most critical for protecting the state from IT security attacks.

We tested the 207 components incuded in the five selected IT security standards at each of the five audited agencies for a total of 1,035 components.

As shown in **Exhibit 4**, below, we identified close to 350 instances where agencies were not in full compliance with a specific component under these five IT security standards. Given the interdependency of standards across the five areas we tested, an IT security issue identified at an agency could result in multiple noncompliance instances within the 207 components tested.

Exhibit 3 - Our audit focused on OCIO IT security standards 4 through 8, which are most critical for protecting the state from cyber threats

Exhibit 4 – Agencies are not in full compliance with five selected IT security standards

207 components of the five IT security standards were tested at each of five agencies

Standard type	Total components within standards tested	Total noncompliance issues found	Not documented	Not implemented
Data security	90	61	56	8
Network security	340	80	49	43
Access security	415	74	20	56
Application security	110	91	91	5
Operations management	80	41	35	13
Total	**1,035**	**347**	**251***	**125***

** If an agency had both **Not documented** and **Not implemented** a component of an IT security standard, we counted it as only one noncompliance issue. For this reason, these columns do not add up to the number in the **Total noncompliance issues found** column.*

Around three-quarters of the noncompliance issues we found were due to a lack of documentation, which typically represents a lower security risk than a lack of implementation. However, in some instances where documentation was lacking, we could not tell whether the agency had implemented a process to address the security standard component.

The areas where we found the most noncompliance issues were under the standards for application security, data security and operations management.

Application security – These standards help ensure the development and maintenance of agency applications do not create security risks through inadequate controls over access to source code, or the use of insecure coding in application development. We found almost all of the application security issues were due to a lack of documentation. However, without adequate documentation, we could not always determine whether agencies had implemented appropriate processes. For example, all five agencies did not consistently document all application development changes so we could not confirm the changes included appropriate security controls such as restricting access to program source code to only those who require access.

Data security – These standards, such as requirements for encryption, help prevent the disclosure of confidential information through data breaches, and unauthorized changes to data. A majority of the issues we found for data security were related to lack of documentation. Examples of issues we found were inadequate encryption procedures for email communication and mobile devices.

Operations management – These standards help ensure continuous operation of critical IT applications and processes. Most of the operations management control issues were due to a lack of documentation. Examples of the operations management issues we found include:

- One agency failed to send its backup data to an offsite location, which could compromise its ability to recover data in the event of a local disaster.
- Three agencies had not developed or implemented formal procedures to test restoration of critical systems.

Application security testing identified security issues

We tested the security of applications and their underlying infrastructure at five state agencies to identify actual weaknesses in the state's current IT system. We found security weaknesses at all five agencies. **Exhibit 5** shows the results of our testing by the level of risk associated with the likelihood and probability of the identified weakness being exploited.

Exhibit 5 – Results of application security testing at five selected agencies

Risk category	Risk rating description	Issues identified
Critical	Extreme impact to entire entity and almost certain to be exploited.	7
High	Major impact to entire entity or individual program and can be exploited by attacker with minimal skills.	12
Medium	Noticeable impact to individual program and knowledgeable insider or expert attacker could exploit with minimal difficulty.	11
Low	Minor damage to entity and requires considerable expertise and resources to exploit. Could also be used with other vulnerabilities to perform a more serious attack.	6
Informational	Likely not an immediate risk on its own, but risk increases if other vulnerabilities exist.	10
Total		**46**

All five agencies worked quickly to start fixing the issues we identified, and two agencies reported using the results to improve other applications not included in testing. The Auditor's Office is conducting additional testing to confirm that these issues have been addressed.

We also compared each agency's application security test results to its compliance test results. We found agencies might have avoided some security issues identified had they been in compliance with the related IT security standard. For example, we identified data security issues at multiple agencies and found that they were also out of compliance with the related IT security standard.

Use of social engineering tactics

We used social engineering tactics to test how state agency staff would respond to our attempts to obtain information that a hacker could exploit. Hackers use these tactics to trick individuals into providing passwords or financial information, or to gain access to their computers by secretly installing malicious software. Our social engineering tests were largely successful in that they were unsuccessful in obtaining exploitable information from state agency staff.

We left USB drives disguised as lost keys, lanyards or other lost items (illustrated in the photograph at right) at three state agencies to see if staff would pick them up and plug them into their agency computers. USB drives can be used to install malicious programs on computers or the networks they are connected to in an effort to interrupt operations or

collect confidential information. Our USB drives contained files that, if opened, would send us a notification. We received no such notifications from state agency computers. Many state agency staff followed appropriate protocols and reported the suspicious USB drives to security personnel. Responding to these reports, a notification was sent to all agencies in the surrounding area where the suspicious USBs were found.

User information can also be gained through "spear phishing," by sending emails posed as requests from familiar individuals or businesses to try and trick individuals into clicking on email attachments or embedded links to provide user IDs and passwords. We sent a malicious spear phishing email, masked as a LinkedIn invitation, to nine state agency employees to see if they would disclose their state user ID and password. Four people clicked the invitation link, but no one provided a state user ID and password. However, clicking a link in an email is a concern because it could lead to malicious websites, or install malicious software on a state agency computer and potentially compromise agency information or IT networks.

Agencies reported several barriers to fully complying with state IT security standards

Agency staff told us their agencies faced barriers that prevented them from fully complying with the state's IT security standards. Four of the five agencies said resource constraints prevent them from fully implementing the standards, including financial constraints and a lack of staff to properly segregate duties and document how the agency complies with the standards. Four agencies also noted some of the standards are unclear or open to interpretation. Additional issues reported by agencies included technical incompatibilities, inconsistent guidance on how to implement the state's IT security standards, and a lack of cooperation from agency computer users. Two agencies suggested that training would help them better comply with the standards.

The state's process to monitor agency IT security compliance could be improved

The state has an appropriate IT security framework that includes good statewide IT security standards, as well as a process to monitor and oversee compliance with those standards. However, we found the Office of the Chief Information Officer could improve the process it uses to monitor and oversee agency compliance because the agencies we reviewed are not providing complete or accurate IT security compliance information as required by state law.

Agencies are required to annually verify their compliance with IT security standards and report areas of noncompliance, so the Office of the Chief Information Officer and the state's Chief Information Security Officer can form a complete understanding of statewide IT security risks. We compared the latest annual reports made by the five agencies we reviewed to our audit results, and found the information they reported was neither complete nor accurate.

For example, three agencies reported they were in full compliance with the state's IT security standards, yet we found numerous instances where they were not. This may be due in part to agency staff not having all the information needed to fully understand whether or not they were in compliance with the standards.

OCIO staff told us that they do not have the resources to monitor agencies individually, or to confirm the information they receive is complete and accurate.

Without complete and accurate information from state agencies, the OCIO cannot readily monitor IT security at an enterprise level. This issue is important because many state agencies share common services such as email, or work together to provide government services to citizens. As a result, all agencies are connected with each other to some degree and one agency with inadequate IT security can unknowingly expose other agencies to risk.

Conclusions

While those responsible for Washington's IT security have already taken significant measures to protect the state, more could be done to improve the state's IT security posture. This includes:

- Strengthening and clarifying a few areas of the state's security standards to more closely align with leading practices
- Working to improve compliance with the state's IT security standards
- Improving the current process used to monitor and oversee agency compliance with the state's IT security standards.

Improving the monitoring process will help those responsible for state IT security oversight to have the information they need to better support agencies and help ensure they have the complete picture needed to properly monitor the state's IT security risks.

Recommendations

To help ensure the state maintains the integrity of its IT networks and systems, and to better protect the confidential information entrusted to the state, we make the following recommendations:

To the five selected state agencies:

- Continue remediating gaps identified where agency practices or documented policies are not in full compliance with the state's IT security standards, and weaknesses identified through our application security testing.
- Provide accurate and complete information on agency compliance with, and deviations from, the state's IT security standards in the agency's annual verification letter to the Office of Chief Information Officer.

To the state's Chief Information Officer:

- Revise the state's IT security standards to more closely align with leading practices, and clarify those where our review found multiple agencies did not comply.
- Evaluate and revise the current process used for agencies to annually report the status of their compliance with, and deviations from, the state's IT security standards to ensure the process provides meaningful and accurate information. While doing so, evaluate what is needed to help agencies understand how to technically comply with the standards and to monitor annual agency compliance.
- Continue to collaborate with the state's Chief Information Security Officer to develop methods to help state agencies better understand the importance of complying with the state's IT security standards, and how best to do so.

To the state's Chief Information Security Officer:

- Continue to collaborate with the state's Office of the Chief Information Officer to develop methods to help state agencies better understand the importance of complying with the state's IT security standards, and how best to do so.

Agency Response

JAY INSLEE
Governor

STATE OF WASHINGTON
OFFICE OF THE CHIEF INFORMATION OFFICER
PO Box 43113 • Olympia, Washington 98504-3113 • (360) 902-0407

December 12, 2014

The Honorable Troy Kelley
Washington State Auditor
P.O. Box 40021
Olympia, WA 98504-0021

Dear Auditor Kelley:

On behalf of the audited agencies and Consolidated Technology Services (CTS), thank you for the opportunity to review and respond to the State Auditor's Office (SAO) performance audit report *"Opportunities to Improve State IT Security."*

We appreciate the efforts of your staff with my office, CTS and the agencies selected, to look for improvements to the state's information technology (IT) security. The collaborative and responsible approach taken by your office ultimately strengthens the state's IT security posture.

Thank you for acknowledging in the report the significant measures Washington has already taken to prevent cyber threats and recognizing the state has established strong IT security standards with no significant gaps between our standards and leading practices. Washington is committed to continuously improving how we protect confidential data and preventing and eliminating security vulnerabilities. We have begun and remain committed to continuous improvement addressing the opportunities your office identified for improvement.

We also appreciate the precautionary steps your office took to protect the IT security of our state throughout this performance audit. We believe these steps are paramount to future performance audits on this topic.

Sincerely,

/s/
Michael Cockrill
Chief Information Officer
Office of the Chief Information Officer

Enclosure

cc: Joby Shimomura, Chief of Staff, Office of the Governor
Kelly Wicker, Deputy Chief of Staff, Office of the Governor
Miguel Pérez-Gibson, Executive Director of Legislative Affairs, Office of the Governor
Matt Steuerwalt, Executive Director of Policy, Office of the Governor
David Schumacher, Director, Office of Financial Management
Tracy Guerin, Deputy Director, Office of Financial Management
Rob St. John, Director, Consolidated Technology Services
Wendy Korthuis-Smith, Director, Results Washington, Office of the Governor
Tammy Firkins, Performance Audit Liaison, Results Washington, Office of the Governor

OFFICIAL STATE AGENCY RESPONSE TO THE PERFORMANCE AUDIT ON OPPORTUNITIES TO IMPROVE STATE IT SECURITY DEC. 12, 2014

This management response to the State Auditor's Office (SAO) performance audit report received Dec. 1, 2014, is provided by the Office of the Chief Information Officer (OCIO) on behalf of Consolidated Technology Services (CTS) and the audited agencies.

SAO PERFORMANCE AUDIT OBJECTIVES:

The SAO sought to answer these questions:

1. Do the state's IT security standards align with leading practices?
2. Are selected state agencies in compliance with the state's IT security standards?
3. Are those agencies adequately protecting confidential information?

SAO Issue 1: Opportunities exist for Washington to further protect the confidential information entrusted to the state by improving IT security.

SAO Issue 2: While the state's IT security standards align closely with leading practices, improvements could be made.

SAO Issue 3: Selected agencies are not in full compliance with state IT security standards.

SAO Issue 4: Application security testing identified security issues.

SAO Issue 5: Agencies reported several barriers to fully complying with state IT security standards.

SAO Issue 6: The state's process to monitor agency IT security compliance could be improved.

SAO Recommendation 1: The five audited agencies should continue remediating gaps identified where agency practices or documented policies are not in full compliance with the state's IT security standards, and weaknesses identified through our application security testing.

STATE RESPONSE:
We agree with the opportunities for improvement identified by the SAO.

Action Steps and Time Frame

- Agencies will continue to work diligently to remediate gaps and improve both practices and documentation. Ongoing. .

SAO Recommendation 2: The five audited agencies provide accurate and complete information on agency compliance with, and deviations from, the state's IT security standards in the agency's annual verification letter to the Office of the Chief Information Officer.

STATE RESPONSE:

The selected agencies concur with the SAO recommendation to provide the OCIO complete and accurate information in their annual verification letters.

Action Steps and Time Frame

- Agencies will provide complete and accurate IT security compliance information to the OCIO in their annual verification letters by the next annual reporting date, which is August 31, 2015.

SAO Recommendation 3: The state's Chief Information Officer revise the state's IT security standards to more closely align with leading practices, and clarify those where our review found multiple agencies did not comply.

STATE RESPONSE:
While we recognize that the report found no significant gaps in the state's IT standards, the OCIO is committed to continually updating these standards to ensure they are consistent with national standards and address emerging cyber threats. The standards have been updated several times in the past two years to provide relevance and clarity, and we agree that further updates are necessary to more completely align the standards with national best practices and clarify the intent and purpose for agencies.

Action Steps and Time Frame

- The OCIO will incorporate the additional national best practices identified in the report into the OCIO standards and clarify those sections of the standards where it was found that multiple agencies did not comply by June 30, 2015.

SAO Recommendation 4: The state's Chief Information Officer evaluate and revise the current process used for agencies to annually report the status of their compliance with, and deviations from, the state's IT security standards to ensure the process provides meaningful and accurate information. While doing so, evaluate what is needed to help agencies understand how to technically comply with the standards and to monitor annual agency compliance.

STATE RESPONSE:
The OCIO agrees with the opportunities for improvement identified by the SAO

Action Steps and Time Frame

- Beginning in January 2015, the OCIO will work with agencies to better understand how the reporting process can be improved to solicit more accurate, meaningful information, and how they might better monitor compliance to the standards. Also, realizing that agencies often rely on the results of required 3-year independent audits to determine their compliance status, the OCIO will review the audit standard currently used by agencies to determine if these should be enhanced to provide more in-depth, operational information that can be used by agencies to enhance their security posture and provide more accurate compliance information to the OCIO.

SAO Recommendation 5: The state's Chief Information Officer continue to collaborate with the state's Chief Information Security Officer to develop methods to help state agencies better understand the importance of complying with the state's IT security standards, and how best to do so.

STATE RESPONSE:
The state's Chief Information Officer (CIO) agrees that continued input from, and collaboration with, the state's Chief Information Security Officer (CISO) is critical in making sure OCIO security policies and standards address real-world, operational security concerns. The importance of this relationship is well understood and must continually be strengthened in order to effectively combat the continually increasing number and complexity of cyber threats.

Action Steps and Time Frame

- The state's CISO, though a member of Consolidated Technology Services, currently reports to the CIO through a dotted-line relationship. The CIO and CISO meet on a regularly scheduled basis, and the CISO is in contact with OCIO staff on a near-daily basis. Also, as mentioned in the auditor's report, legislation is being drafted to merge the OCIO, CTS and parts of DES. This will strengthen the reporting relationship between the CIO and CISO, and bring greater cohesion between the policy and operational aspects of IT security.

SAO Recommendation 6: The state's Chief Information Security Officer continue to collaborate with the Office of the Chief Information Officer to develop methods to help state agencies better understand the importance of complying with the state's IT security standards, and how best to do so.

STATE RESPONSE:
The state's Chief Information Security Officer (CISO) agrees that close collaboration with the state's Chief Information Officer (CIO) is critical to ensuring OCIO security policies and standards address real-world, operational security risks. This relationship is critical to providing consistent implementation strategies across agencies as the threat landscape changes.

Action Steps and Time Frame

- The CISO and CIO meet on a regularly scheduled basis, and the CISO is in contact with OCIO staff on a near-daily basis. As the OCIO incorporates the additional national best practices identified in the report into the OCIO IT standards, the CISO with work with the CIO to provide guidance on how agencies can consistently implement the security controls identified in the updated security standards by December 2015.

Appendix A: Initiative 900

Initiative 900, approved by Washington voters in 2005 and enacted into state law in 2006, authorized the State Auditor's Office to conduct independent, comprehensive performance audits of state and local governments.

Specifically, the law directs the Auditor's Office to "review and analyze the economy, efficiency, and effectiveness of the policies, management, fiscal affairs, and operations of state and local governments, agencies, programs, and accounts." Performance audits are to be conducted according to U.S. General Accountability Office government auditing standards.

In addition, the law identifies nine elements that are to be considered within the scope of each performance audit. The State Auditor's Office evaluates the relevance of all nine elements to each audit. The table below indicates which elements are addressed in the audit. Specific issues are discussed in the Audit Results and Recommendations section of this report.

I-900 element	Addressed in the audit
1. Identification of cost savings	**No.** The audit did not identify cost savings.
2. Identification of services that can be reduced or eliminated	**No.** The audit did not address services that could be reduced or eliminated.
3. Identification of programs or services that can be transferred to the private sector	**No.** The audit did not identify programs or services that can be transferred to the private sector.
4. Analysis of gaps or overlaps in programs or services and recommendations to correct gaps or overlaps	**Yes.** We identified gaps in select state agencies' IT security programs and made recommendations to decrease IT security risk. We also discovered a gap in the information the Office of the Chief Information Officer (OCIO) collects related to state agencies' level of compliance with state IT security standards. We recommend OCIO evaluate its process and resources for gathering this information and recommend agencies provide accurate information to OCIO.
5. Feasibility of pooling information technology systems within the department	**No.** The audit did not consider pooling information technology systems; it focused on assessing the IT security posture at select state agencies.
6. Analysis of the roles and functions of the department, and recommendations to change or eliminate departmental roles or functions	**Yes.** We recommend OCIO continue collaborating with Consolidated Technology Services (CTS) to develop methods to help state agencies better understand the importance of complying with the state's IT security standards, and how to comply with the state's IT security standards.
7. Recommendations for statutory or regulatory changes that may be necessary for the department to properly carry out its functions	**No.** We did not identify a need for statutory or regulatory change.
8. Analysis of departmental performance, data performance measures, and self-assessment systems	**No.** The audit did not address the agencies' performance measures and self-assessment systems.
9. Identification of best practices	**Yes.** The audit identified certain OCIO IT security standards that can be strengthened to more closely align with leading practices.

Appendix B: OCIO Standard No. 141.10

Content for Appendix B follows this page.

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:** August 19, 2013 **See Also:** Appendix A: IT Security Checklist Appendix B: IT Security Risk Threatscape Appendix C: IT Security Non-Compliance/Deviation Form Securing Information Technology Assets Policy (141) Securing Information Technology Guidelines Auditor's Procedures Engagement Media Handling and Data Disposal Best Practices

INTRODUCTION

To implement the Information Technology (IT) Security Policy, to protect IT resources, and to enable security audits of those resources, it is required that agencies adhere to common IT security standards. Common standards will help ensure that agencies have an effective and secure environment for IT processing.

Security standards define the processes, procedures, and practices necessary for implementing an agency-specific IT security program. These IT security standards apply to all IT activities, whether they are operated by or for an agency. They include specific steps that will be taken to ensure that a secure IT environment is maintained and all agency systems provide for privacy and security of confidential information.

Such an environment 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.
(4) Implements security with a customer-centric focus.

Agencies that operate some or all of their information systems outside of this environment will still adhere to the IT security standards.

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 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 Design Review

The agency must request a security design review 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 Design Review 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 design review is recommended.

The agency must provide the following to the state Chief Information Security Officer at CTS for the design review:

(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) The Security risks 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 Design Review 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 results 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. The IT Security Checklist is required by the agency IT security program.
(4) Include in the agency investment plan the signed off copy of the IT Security Checklist from the Design Review itemizing the security controls and associated budget, schedule and resource estimates. If the agency investment plan is submitted to OCIO, the IT Security Checklist will be returned to the agency when processing is complete and securely filed in the agency.
(5) Attain full compliance with these IT security standards by August 2012.
(6) 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 Design Review (when required) to comply with the requirements in the OCIO IT security standards.
(7) 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.

(8) 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.

(9) 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

(2) 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.

(3) Category 2 – Sensitive Information

(4) 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.

(5) Category 3 – Confidential Information

(6) Confidential information is information that is specifically protected from disclosure by law. It may include but is not limited to:

a. Personal information about individuals, regardless of how that information is obtained.

b. Information concerning employee personnel records.

c. Information regarding IT infrastructure and security of computer and telecommunications systems.

(7) 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) The storage of Category 3 and above information requires agencies to select and apply encryption, at the discretion of the agency, after completing an agency IT Security Risk Assessment. Agencies must use industry standard algorithms or cryptographic modules validated by the National Institute of Standards and Technology (NIST).

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 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) Connect internal networks to external networks through a CTS-managed or CTS-approved security layer. The CTS-managed security layer is defined as firewalls, proxy servers and security gateways.

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 user IDs, 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 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

6.3.2 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).

8.3 Media Handling and Disposal

Agencies must:

(1) Ensure that media be disposed of securely and safely when no longer required, using formal documented procedures.

(2) Sanitize equipment containing storage media prior to disposal (reference best practices such as NIST SP 800-88 Guidelines for Media Sanitation or equipment disposal procedures documented in the IT security program) and:
   a. Destroy, securely overwrite, or make unavailable agency identifiable data.
   b. Destroy, securely overwrite, or make unavailable software consistent with the software licensing agreement.

(3) Ensure the safe and secure disposal of sensitive media.

(4) Ensure that system documentation is protected against unauthorized access.

(5) Ensure Media containing information is protected against unauthorized access, misuse, or corruption during transportation beyond an 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, 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 user ID 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.

RecordUnits 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.

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
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, please contact the state Chief Information Security Officer at Consolidated Technology Services.

APPROVING AUTHORITY

Chief Information Officer Date
Chair, Technology Services Board

Appendix C: Comparing the State OCIO's IT Security Standards to Leading Practices

This appendix provides a comparison of the entire state IT Security Standards to leading practices in

- National Institute of Standards and Technology (NIST), Special Publication 800-53, Revision 4 "Security and Privacy Controls for Federal Information Systems and Organizations"
- International Organization for Standardization (ISO, IT Security Standards ISO 27001

Due to the length of this appendix, it is only provided online at the State Auditor's Office website at:
www.sao.wa.gov/state/Documents/PA_State_IT_Security_AppC.pdf

Appendix D: OCIO Standards, Leading Practices and Recommendations

Leading practices used for comparison were:

- National Institute of Standards and Technology (NIST), Special Publication 800-53, Revision 4 "Security and Privacy Controls for Federal Information Systems and Organizations"
- International Organization for Standardization (ISO, IT Security Standards ISO 27001)

Observed in practice refers to clarifications we are recommending based on results of our findings at the agencies.

A complete copy of the OCIO's IT Security Standards can be found in **Appendix B**.

OCIO Standard, Control Source & Gap Description

1.1 - Agency IT Security Program - Documentation

Observed in practice

Clarify when documentation is required, including showing implementation of specific standards and providing evidence that specific testing standards were followed (for example, annual configuration reviews).

1.1 (6) - Agency IT Security Program - Documentation

Observed in practice

Clarify what is required for annual reporting and the importance of reporting accurate and complete information.

1.6 (1) - Agency IT Security Program – Audit

Observed in practice

Specify what standards these audits should follow, the specific outcomes desired of the audit, and whether a risk assessment should guide audit scope.

3 - Physical & Environmental Protection

ISO 11.1.3, Physical & Environmental Security: Securing offices, rooms and facilities

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically, related IT security policies should include guidelines for all offices and buildings; not just computer/telecommunications rooms.

ISO 11.1.4, Physical & Environmental Security: Protecting against external and environmental threats

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically include guidelines for protection against natural disasters, malicious attacks or accidents.

ISO 11.1.6, Physical & Environmental Security: Delivery and loading areas

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically include guidelines for delivery and loading areas.

3 - Physical & Environmental Protection, continued

ISO 11.2.2, Physical & Environmental Security: Supporting utilities

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically include guidelines for supporting utilities (such as electricity, telecommunications, water supply, gas, sewage, HVAC). These services should be protected from power failures and other outages that may occur.

NIST PE-2, Physical & Environmental Protection: Physical Access Authorization

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically include guidelines for physical access authorization.

NIST PE-5, Physical & Environmental Protection: Access Control for Output Devices

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically include guidelines for access control for output devices.

NIST PE-6, Physical & Environmental Protection: Monitoring Physical Access

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically include guidelines for monitoring physical access.

NIST PE-8, Physical & Environmental Protection: Visitor Access Records

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically include guidelines for visitor access records.

NIST PE-9, Physical & Environmental Protection: Power Equipment and Cabling

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically include guidelines for power equipment and cabling, particularly for state agency data centers and network closets.

NIST PE-10, Physical & Environmental Protection: Emergency Shutoff

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically include guidelines regarding emergency shutoff procedures.

NIST PE-11, Physical & Environmental Protection: Emergency Power

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically include guidelines for regarding emergency power.

NIST PE-12, Physical & Environmental Protection: Emergency Lighting

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically include guidelines regarding emergency lighting.

3 - Physical & Environmental Protection, continued

NIST PE-13, Physical & Environmental Protection: Fire Protection

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically include guidelines regarding fire protection.

NIST PE-14, Physical & Environmental Protection: Temperature and Humidity Controls

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically include guidelines regarding temperature and humidity controls.

NIST PE-15, Physical & Environmental Protection: Water Damage Protection

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically include guidelines regarding water damage protection.

NIST PE-16, Physical & Environmental Protection: Delivery and Removal

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically include guidelines regarding delivery and removal.

NIST PE-17, Physical & Environmental Protection: Alternate Work Site

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically include guidelines for alternative work sites.

NIST PE-18, Physical & Environmental Protection: Location of Information System Components

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically include guidelines regarding location of information system components.

NIST PE-20, Physical & Environmental Protection: Asset Monitoring and Tracking

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically include guidelines for asset monitoring and tracking.

NIST SC-42, System and Communications Protection: Sensor Capability and Data

Establish environmental protection standards for agencies with their own data center. For agencies using the State Data Center, establish environmental protection standards for agency networking closets. Specifically include guidelines for sensor capability and data.

4.2 (1-9) - Data Security - Data Sharing

Observed in practice

Strengthen standard to specify when agencies must establish data sharing agreements.

4.3 - Data Security - Secure Management & Encryption of Data

Observed in practice

Clarify encryption standards to help ensure secure key management practices and continuous encryption of applicable data.

4.3 (1) - Data Security - Secure Management & Encryption of Data

ISO 10.1.2, Cryptographic controls: Key Management

Establish standards specifically for public and private key management. Processes should address generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys. Generated keys should be stored in a secure location not accessible to unauthorized personnel. Distribution of public keys needs to be limited to those requiring them. Standards should include how long keys are good for, what constitutes a change in keys, and details on how to dispose of keys.

5.1.1 (5) - Network Security - Secure Segmentation - Network Devices

NIST AC-8, Access Control: System Use Notification

Strengthen standard by including requirements to consider data confidentiality when determining whether to use a system banner, or whether to retain these notification messages on the screen until users access the applicable system.

5.1.2 (2)(g) - Network Security - Secure Segmentation - Firewalls

NIST AU-2, Audit Events: Audit Events

Clarify standard by defining what is required for comprehensive audit trails including what specific audit events must be captured.

NIST AU-3, Content of Audit Records: Content of Audit Records

Clarify standard by defining what is required for comprehensive audit trails including what details audit records must include.

NIST AU-8, Audit & Accountability: Time Stamps

Clarify standard by defining what is required for comprehensive audit trails including the use of time stamps.

NIST AU-11, Audit Record Retention: Audit Record Retention

Clarify standard by defining what is required for comprehensive audit trails including firewall audit record retention.

NIST AU-14, Session Audit: Session Audit

Clarify standard by defining what is required for comprehensive audit trails including whether session audits must be retained.

Observed in Practice

Clarify standard by stating specifically what elements are required in a "comprehensive audit trail."

5.5 - Network Security - Security Patch Management

ISO 12.6.1, Operations Security: Management of technical vulnerabilities

Clarify standard by requiring audit logs for all procedures applicable to addressing a vulnerability or patch.

NIST CM-1, Configuration Management: Configuration Management Policy and Procedures

Strengthen standard by requiring agencies to follow their configuration management policies and procedures.

NIST CM-3, Configuration Management: Configuration Change Control

Strengthen standard by requiring agencies to follow their change control policies and procedures.

5.6 (3) - Network Security - System Vulnerabilities

NIST CM-2, Configuration Management: Baseline Configuration

Strengthen standard by requiring agencies to develop, document and maintain baseline configurations of systems and system components.

NIST CM-6, Configuration Management: Configuration Settings

Strengthen standard by fully addressing requirements for configuration settings.

Observed in practice

Clarify standard by specifically defining how agencies must harden systems for the life of the product.

5.8 - Network Security - Mobile Computing

ISO 6.2.1, Organization of Information Security: Mobile device policy

Strengthen standard by including requirements for registration of mobile devices; physical protection; restriction of software installation; software versions; patch management; restriction of connections to information services; access control; malware protection; remote disabling, erasure or lockout; backups; and usage of web services and applications.

NIST AC-19, Access Control: Access Control for Mobile Devices

Strengthen standard by including specific requirements related to access control for non-Category 3 mobile computing.

Observed in practice

Clarify what is required in agency mobile device policies, including mobile device lock-out procedures.

5.8 - Network Security - Mobile Computing

ISO 6.2.2, Organization of Information Security: Teleworking

Establish standards requiring agency policies and supporting security measures related to protection of information accessed, processed, or stored at teleworking sites.

6.1.1 - Access Security - Access Management - Policies

NIST AC-14, Access Control: Permitted Actions without Identification or Authentication

Strengthen standard by addressing what data can be accessed without any authentication, such as public information provided on a webpage; and specifically require agencies to inventory data based on whether or not identification or authentication is required.

6.1.2 - Access Security - Access Management - Accounts

NIST AC-9, Access Control: Previous Logon Notification

Strengthen standard by requiring agencies to use previous logon notifications when technically feasible.

NIST IA-6, Identification and Authentication: Authenticator Feedback

Strengthen standard by fully addressing use of previous logon notifications and other authenticator feedback methods. Controls could be added to the account management section to address misuse of information on stale accounts.

6.1.3 - Access Security - Access Management - Sessions

NIST AC-10, Access Control: Concurrent Session Control

Strengthen standard by addressing requirements for concurrent session control when technically feasible.

6.1.4 - Access Security - Access Management - Auditing

NIST AU-2, Audit Events
Strengthen standard by addressing audit events.

NIST AU-3, Audit & Accountability: Content of Audit Records
Strengthen standard by addressing the content of audit records.

NIST AU-4, Audit & Accountability: Audit Storage Capacity
Strengthen standard by addressing audit of storage capacity.

NIST AU-6, Audit & Accountability: Audit Review, Analysis, and Reporting
Strengthen standard by addressing audit review, analysis, and reporting.

NIST AU-7, Audit & Accountability: Audit Reduction and Report Generation
Strengthen standard by addressing audit reduction and report generation.

NIST AU-8, Audit & Accountability: Time Stamps
Strengthen standard by addressing time stamps.

NIST AU-9, Audit & Accountability: Protection of Audit Information
Strengthen standard by addressing protection of audit information.

NIST AU-10, Non-repudiation
Strengthen standard by addressing including non-repudiation.

NIST AU-11, Audit Record Retention
Strengthen standard by addressing audit record retention.

NIST AU-12, Audit Generation
Strengthen standard by addressing audit generation.

Observed in practice
Strengthen standard by defining what is meant by a "formal process."

6.3 - Access Security - Authentication

NIST IA-1, Identification and Authentication: Identification and Authentication Policy and Procedures
Strengthen standard by specifically requiring formal Identification and Authentication Policy and Procedures.

6.4 - Access Security - Remote Access

NIST IA-4, Identification and Authentication: Identifier Management
Strengthen standard by specifically addressing identifying and documenting remote accounts in accordance with account management, or remote access identifier management. For account management, this includes such things as managing accounts by establishing conditions for group members; identifying authorized users; specifying access privileges; requiring approvals of requests to establish accounts; and establishing, activating, modifying, disabling and removing temporary and guest accounts. For remote access accounts, this includes such things as user identification and authorization, and disabling access after an agreed upon amount of time.

7.1 - Application Security - Planning & Analysis

NIST PL-2, Planning: System Security Plan

Strengthen standard by specifically addressing creating and approving a system security plan.

NIST PL-8, Planning: Information Security Architecture

Strengthen standard by requiring agencies to create an Information Security Architecture for information systems.

7.2 - Application Security - Application Development

NIST SA-5, System and Services Acquisition: Information System Documentation

Strengthen standard by specifically requiring documentation of information systems.

NIST SA-8, System and Services Acquisition: Security Engineering Principles

Strengthen standard by specifically requiring agencies to use security engineering principles during design and implementation of information systems.

NIST SA-17, System and Services Acquisition: Developer Security Architecture and Design

Strengthen standard by specifically requiring design specification and security architecture during the development of the information system.

7.2 (3), (4), (5) - Application Security - Application Development

ISO 14.3.1, System acquisition, development and maintenance: Protection of test data

Strengthen standard by requiring separate authorization each time operational information is copied to a test environment, operational information be erased from a test environment immediately after testing is complete, logging of the copying and use of operational information to provide an audit trail, and that operational information references production data.

7.2 (6) - Application Security - Application Development

NIST SA-11, Developer Security Testing and Evaluation: Developer Security Testing and Evaluation

Strengthen standard to adequately reflect system development life cycle procedures.

7.5 - Application Security - Application Service Providers

NIST SA-4, System and Services Acquisition: Acquisition Process

Strengthen standard by requiring security requirements in contracts be based on a risk assessment.

NIST SA-9, System and Services Acquisition: External Information System Services

Strengthen standard by requiring agencies to monitor third-party compliance with security controls.

Observed in practice

Clarify standard so it is clear that IT vendor contracts for outsourced applications must include a requirement for the vendor to be compliant with OCIO standards; Also clarify agencies' vendor monitoring responsibilities, including how the vendor is to verify they are compliant with OCIO IT security standards.

8.1 - Operations Management - Change Management

ISO 12.1.2, Operations Security: Change management

Strengthen standard by requiring fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.

NIST CA-5, Certification, Accreditation, and Security Assessments: Plan of Action and Milestones

Strengthen standard by requiring an agency-specific formal documented change management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for plans of action and milestones for certifications, accreditations, and security assessments.

NIST CM-1, Configuration Management: Configuration Management Policy and Procedures

Strengthen standard by requiring an agency-specific formal documented change management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for configuration management policy and procedures.

NIST CM-2, Configuration Management: Baseline Configuration

Strengthen standard by requiring an agency-specific formal documented change management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for baseline configuration.

NIST CM-9, Configuration Management: Configuration Management Plan

Strengthen standard by requiring an agency-specific formal documented change management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for configuration management.

NIST MA-1, Maintenance: System Maintenance Policy and Procedures

Strengthen standard by requiring an agency-specific formal documented change management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for system maintenance.

NIST MA-3, Maintenance: Maintenance Tools

Strengthen standard by requiring an agency-specific formal documented change management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for maintenance tools.

NIST MA-5, Maintenance: Maintenance Personnel

Strengthen standard by requiring an agency-specific formal documented change management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for maintenance personnel.

8.1 - Operations Management - Change Management, continued

NIST MA-6, Maintenance: Timely Maintenance

Strengthen standard by requiring an agency-specific formal documented change management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for timely maintenance.

Observed in Practice

Clarify standards on what procedures should be followed and what needs to be documented when making system or application changes. Change management (SDLC) procedures should specify what changes are approved, tested, approved for implementation into production, etc., including changes to firewalls or updating application code.

8.1 (3) - Operations Management - Change Management

NIST CM-3, Configuration Management: Configuration Change Control

Strengthen standard by requiring agencies to retain and review configuration changes, to audit changes made, and to maintain a formal control oversight process for all changes.

NIST SI-2, System and Information Integrity: Flaw Remediation

Establish standard to address flaw remediation.

8.2 - Operations Management - Asset Management

ISO 8.1.1, Asset management: Inventory of assets

Clarify standard by specifically defining what a major IT component is, including what is considered a major IT component for the purposes of the inventory, and clarify standard so all assets the organization owns such as hardware, software, data and network devices are considered.

Observed in practice

Clarify standard by specifically defining what a major IT component is, and how to properly identify data asset owners for significant applications in the agency (such as data is not "owned" by IT, IT only maintains the data).

8.3 (1) - Operations Management - Media Handling & Disposal

ISO 11.2.7, Physical & Environmental Security: Secure disposal or re-use of equipment

Strengthen standard by requiring logging of the disposal of sensitive items to maintain an audit trail, and the verification of sanitized equipment before disposal or re-use. The standard should incorporate the language included in the OCIO's *Media Handling and Data Disposal Best Practices* document.

ISO 8.3.2, Asset management: Disposal of media

Strengthen standard by requiring logging of the disposal of sensitive items to maintain an audit trail, and the verification of sanitized equipment before disposal or re-use. The standard should incorporate the language included in the OCIO's *Media Handling and Data Disposal Best Practices* document.

8.3 (2) - Operations Management - Media Handling & Disposal

NIST MP-6, Media Protection: Media Sanitization

Establish standard to require periodic tests on sanitation equipment and procedures to ensure correct performance.

8.4 - Operations Management - Data & Program Backup

ISO 12.3.1, Operations Security: Information backup

Strengthen standard by specifying that back-up information be given appropriate levels of physical and environmental protection and that back-ups of confidential information be encrypted where appropriate.

Observed in Practice

Clarify standard to be more specific on when backups are required and where backups must be stored.