Office of the Washington State Auditor
Pat McCarthy

Performance Audit

Continuing Opportunities to Improve State Information Technology Security – 2017

March 29, 2018

We assessed the security at three state agencies in 2017. The state agencies included in this performance audit have taken significant measures to protect their information technology systems. In addition, our security review identified opportunities to further strengthen the agencies' security.

Report Number: 1021044

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 Pat McCarthy
360-902-0360, Pat.McCarthy@sao.wa.gov

Scott Frank – Director of Performance Audit
360-902-0376, Scott.Frank@sao.wa.gov

Erin Laska, CIA – Principal Performance Auditor
360-725-5555, Erin.Laska@sao.wa.gov

Joseph Clark – Performance Auditor
360-725-5572, Joseph.Clark@sao.wa.gov

Ryan Thedy, CISA – Performance Auditor
360-725-5414, Ryan.Thedy@sao.wa.gov

Kathleen Cooper – Deputy Director for Communications
360-902-0470, Kathleen.Cooper@sao.wa.gov

To request public records

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

Introduction

Washington's state government and the critical functions it provides – such as public safety, tax collection, social services and transportation systems – depend on computerized information systems to carry out operations and to process, maintain and report essential information. These state IT systems include vast amounts of public and confidential information. Examples of confidential information include Social Security numbers, health care information, arrest records and federal tax information.

An attack against a state IT system could lead to unauthorized access of confidential information and disruption of state critical services. In some cases, malicious hackers target state government IT systems because they want to steal confidential information and sell it for financial gain, while in other cases the goal is disruption of vital government services. The security of state IT systems and related data are paramount to public confidence, the stability of government operations, and the safety and well-being of the state and its residents.

Residents could suffer directly from a data breach including financial harm and identity theft. Governments also face considerable tangible costs for data breaches. A 2017 study by the Ponemon Institute found that a data breach costs government an average of $110 per record lost. These costs can include:

- Engaging forensic experts to determine the cause and breadth of the incident
- Hotline support for affected victims
- Notifying affected victims
- Providing free credit monitoring subscriptions (potentially $8 to $15 per person per month)
- Paying fines. For example, the U.S. Department of Health and Human Services' Office for Civil Rights may impose fines when protected health information is breached.

As state governments face unprecedented risk from cyber-attacks and high costs from data breaches, the focus on protecting sensitive and personally identifiable information continues to be a top priority for state Chief Information Officers nationwide. To help Washington protect its mission-critical IT systems and secure the data it needs to carry on state business, we conducted a performance audit designed to assess whether there are opportunities to improve IT security at three participating state agencies.

In recent years public entities have suffered several breaches here in Washington. In 2016 and 2017 over half a dozen Washington state public entities, including at least four state agencies, submitted breach notifications to the Washington State Office of the Attorney General.

State law (RCWs 19.255.010 and 42.56.590) requires any business, individual or public agency to notify the Washington State Office of the Attorney General when more than 500 Washington residents have their data stolen as a result of a single security breach.

Scope and methodology

To determine whether there were opportunities to strengthen IT security controls at three state agencies, we asked the following questions:

- Are selected state agencies adequately protecting their confidential information from external and internal threats?
- Are selected state agencies' IT security practices aligned with select Critical Security Controls and compliant with related state IT security standards?

To help conduct the audit, we hired subject matter specialists with expertise in conducting security testing of organizational IT infrastructure and applications.

Selecting state agencies for testing

We selected three medium to large state agencies that rely on confidential information to serve the people of Washington. One of the agencies asked to be included in this audit following the publication of our second cybersecurity performance audit in 2016. After we selected the agencies, we consulted with the state's Chief Information Security Officer at the Washington Technology Solutions (WaTech) Office of Cyber Security to ensure a coordinated approach and to reduce the impact of our testing on agency operations.

External and internal security testing

To determine whether the three selected state agencies were adequately protecting their confidential information from threats, we conducted external and internal security testing of each agency's applications, systems and their underlying networks, including identifying and assessing issues and determining if they could be exploited. To help ensure a real-world response to the external security testing, only agency executives and a few key staff knew about the testing in advance.

With the involvement of each agency's key IT security staff, we selected several mission-critical applications for external and internal security testing. Because the state offers many of its services through the internet, the testing included applications available to the public online as well as applications available only to agency employees on their internal network.

Comparing state agencies' security programs to leading practices and state standards

Leading practices

We reviewed select IT security controls at the agencies, including a review of agency policies, procedures, and technical implementation of the controls, to determine if they align with internationally-recognized leading practices. Specifically, we used select Critical Security Controls from the Center for Internet Security (CIS) as our criteria to assess the effectiveness of agencies' IT security controls and to identify areas that could be made stronger.

The CIS is a nonprofit organization focused on safeguarding public and private organizations against cyber threats. The Controls are a prioritized set of leading practices for cyber defense created to stop the most pervasive and dangerous attacks, and are developed and vetted across a broad community of government and industry practitioners including, for example, the U.S. Department of Defense National Security Agency, the U.S. Department of Energy nuclear energy labs, law enforcement organizations, Verizon, HP, and Symantec.

As the CIS Controls are prioritized, we reviewed the top five because according to CIS, aligning with the top five Controls can provide an effective defense against the most common cyber attacks. We also reviewed Control 11 because it is closely related to Control 3. Specifically we reviewed the following CIS Controls:

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges

11. Secure Configurations for Network Devices

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 three selected agencies, nor any detailed descriptions of our findings. Disclosure of such detail could potentially be used by a malicious attacker against the state.

Detailed findings and recommendations were provided to each agency we reviewed and the Office of Cyber Security at Washington Technology Solutions.

State standards

We also determined agencies' compliance with the state's required IT security standards that are related to the six CIS Controls reviewed. The state's security standards are published by the Office of the Chief Information Officer under the authority of WaTech's Office of Cyber Security as Securing Information Technology Assets Standards (141.10).

We determined which state standards were related to the six CIS Controls, and if assessing a CIS Control could also address a state standard. We reviewed 92 of the 270 required state IT security controls at each of the three state agencies. This allowed us to provide the agencies with an assessment of how their security practices and policies align with the six CIS Controls, which are optional leading practices, and the related state standards (OCIO 141.10), which are required.

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 as published in 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

The three state agencies included in this audit have taken significant measures to protect their information technology systems, but opportunities exist to strengthen IT security.

Our external and internal security testing found strengths in agencies' security, but also uncovered issues that should be addressed. The security controls in policies, procedures and technical implementation we tested partially or fully align with several leading practices and required state standards, but there are areas where agencies can make improvements. For example, our examination of agencies' compliance with the subset of state standards found all three state agencies need to better document their IT security programs. Specifically, while all three agencies' policies included requirements to comply with state standards, the agencies' policies and procedures lacked specifics about what controls must be implemented to comply with the standards.

State IT security standards require agencies' policies and procedures to contain details of the security controls applied to agency systems. Furthermore, without specific controls detailed in agencies' policies and procedures, there is a higher risk that security will not be implemented as intended. Detailed policies and procedures provide a clear roadmap for compliance; more general policies and procedures are open to interpretation. When policies and procedures are open to interpretation, different personnel may implement the same control differently. Additionally, security and IT operations personnel from all three agencies said detailed policies and procedures are helpful to them because, in addition to clearly outlining security expectations, they give security personnel authority to implement and enforce robust security.

Where agency practices are not fully aligned with leading practices and required state standards, agency personnel reported resource constraints, including lack of IT security personnel and high turnover as causes. One agency reported supplemental guidance would help agencies build security programs because the state standards are vague in some areas. At one agency we noted further centralization of the agency's IT security function would improve security and compliance with state IT security standards. The three state agencies have already begun addressing many of the significant issues we identified and are continuing to improve their security programs.

We gave each of the three state agencies the detailed results of their individual agency's tests as we completed them, as well as detailed recommendations. We also gave all detailed results and recommendations to WaTech's Office of Cyber Security. As noted previously, this report does not include the agencies' names or the detailed descriptions of our results in order to protect the state's IT systems, and the confidential and sensitive information contained in those systems. These detailed results are exempt from public disclosure in accordance with RCW 42.56.420(4).

Recommendations

To help strengthen the agencies' IT security controls, protect the confidential information within the state's networks and systems, and improve the agencies' security posture, we make the following recommendations.

To the three selected state agencies:

1. Continue remediating issues identified during the security testing.
2. Continue remediating gaps identified between agency practices or documented policies and procedures and the state's IT security standards and industry leading practices.
3. Continue periodically assessing the agency's IT security needs and resources, including personnel and technology, to mature and maintain sufficient security.

To the Office of Cyber Security, WaTech:

4. Continue to conduct outreach to state agencies to determine how additional clarity or guidance could help agencies identify detailed controls to incorporate into their policies and procedures, and help them align agency practices with the state IT security standards.
5. Continue to develop and provide that additional clarity or guidance to state agencies.

Agency response

JAY INSLEE
Governor

Rob St. John
Acting Director & State Chief
Information Officer

STATE OF WASHINGTON

WASHINGTON TECHNOLOGY SOLUTIONS

1500 Jefferson Street SE • Olympia, Washington 98504-1501 • (360) 407-8700

March 15, 2018

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

Dear Auditor McCarthy:

On behalf of the audited agencies, thank you for the opportunity to review and respond to the State Auditor's Office (SAO) performance audit report Continuing Opportunities to Improve State Information Technology Security – 2017.

We appreciate the report's recognition of the significant measures agencies have taken to protect their information technology systems from risk. We agree that opportunities exist to continue to strengthen our security and will continue to do so.

We also appreciate the collaborative approach your staff exercised throughout this performance audit to protect the IT security of our state. Please extend our thanks to them.

Sincerely,

Rob St. John
Acting Director and State Chief Information Officer

cc: David Postman, Chief of Staff, Office of the Governor
Kelly Wicker, Deputy Chief of Staff, Office of the Governor
Keith Phillips, Director of Policy, Office of the Governor
David Schumacher, Director, Office of Financial Management
Inger Brinck, Director, Results Washington, Office of the Governor
Tammy Firkins, Performance Audit Liaison, Results Washington, Office of the Governor

OFFICIAL STATE CABINET AGENCY RESPONSE TO THE PERFORMANCE AUDIT ON CONTINUING OPPORTUNITIES TO IMPROVE STATE IT SECURITY – 2017 MAR. 15, 2018

This management response to the State Auditor's Office (SAO) performance audit report received Feb. 22, 2018, is provided by the acting Director of Washington Technology Solutions and State Chief Information Officer on behalf of the audited agencies.

SAO PERFORMANCE AUDIT OBJECTIVES:

The SAO sought to determine if there were opportunities to strengthen IT security controls at three state agencies through these questions:

1. Are selected state agencies adequately protecting their confidential information from external and internal threats?
2. Are their security practices aligned with select critical security controls and compliant with related state IT security standards?

SAO Issue 1: Opportunities exist to strengthen IT security.

SAO Recommendations 1-3: The three audited agencies should:

- Continue remediating issues identified during the security testing.
- Continue remediating gaps identified between agency practices or documented policies and procedures and the state's IT security standards and industry leading practices.
- Continue periodically assessing the agency's IT security needs and resources, including personnel and technology, to mature and maintain sufficient security.

STATE RESPONSE:
We agree with the opportunities for improvement identified to strengthen IT security by the SAO. The audited agencies will continue to work diligently to remediate the issues identified during testing and the gaps identified between agency practices or documented policies and procedures and the state's IT security standards. Agencies are committed to ongoing assessment of IT security needs.

Action Steps and Time Frame

- Each audited agency will establish a plan to address the gaps and improvements identified. These plans will be monitored over time by the SAO and the audited agency security staff. *By May 31, 2018*.

SAO Recommendation 4: To the state's Office of Cyber Security (OCS): Continue to conduct outreach to state agencies to determine how additional clarity or guidance could help agencies

identify detailed controls to incorporate into their policies and procedures, and help them align agency practices with the state IT security standards.

STATE RESPONSE:
The state Office of Cyber Security will continue to encourage agencies to participate in OCS provided monthly technical and policy training sessions and weekly open office hours to address security questions and/or issues.

Action Steps and Time Frame

- OCS will send monthly training notifications to a broader audience. *By May, 31 2018*.

SAO Recommendation 5: To the state's Office of Cyber Security: Continue to develop and provide that additional clarity or guidance to state agencies.

STATE RESPONSE:
The state Office of Cyber Security will continue to encourage agencies to participate in OCS provided monthly technical and policy training sessions and weekly open office hours to address security questions and/or issues.

Action Steps and Time Frame

- OCS will send monthly training notifications to a broader audience. *By May 31, 2018*.

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. Government 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 section of this report.

I-900 element		Addressed in the audit
1.	Identify cost savings	**No**. The audit did not identify measurable cost savings. However, strengthening IT security could help agencies avoid or mitigate costs associated with a data breach.
2.	Identify services that can be reduced or eliminated	**No**. The audit did not address services that could be reduced or eliminated.
3.	Identify programs or services that can be transferred to the private sector	**No**. State law and IT security policy require state agencies to take steps to ensure a secure IT environment is maintained and all systems provide for the security of confidential information.
4.	Analyze gaps or overlaps in programs or services and provide recommendations to correct them	**Yes**. The audit compares agencies' IT security controls against required state standards and leading practices, and makes recommendations to align them.
5.	Assess feasibility of pooling information technology systems within the department	**No**. The audit did not assess the feasibility of pooling information systems; it focused on select agencies' IT security postures.
6.	Analyze departmental roles and functions, and provide recommendations to change or eliminate them	**Yes**. The audit evaluates the roles and functions of certain IT security areas at the agencies, and makes recommendations to better align them with required state standards and leading practices.
7.	Provide recommendations for statutory or regulatory changes that may be necessary for the department to properly carry out its functions	**No**. The audit does not recommend statutory or regulatory changes. However, it does recommend WaTech continue to provide additional clarity or guidance to agencies to help them better align their IT security programs with state IT security standards.
8.	Analyze departmental performance data, performance measures and self-assessment systems	**Yes**. Our audit examined and made recommendations to improve certain IT security controls at selected agencies.
9.	Identify relevant best practices	**Yes**. Our audit identified and used leading practices maintained by the Center for Internet Security to assess select agencies' IT security controls.