Washington State Auditor's Office

Government that works for citizens

Performance Audit

Continuing Opportunities to Improve State Information Technology Security – 2016

November 7, 2016

Report Number: 1017915

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
360-902-0370, Auditor@sao.wa.gov

Jan M. Jutte, CPA, CGFM – Deputy State Auditor
360-902-0360, Jan.Jutte@sao.wa.gov

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

Thomas Furgeson, Deputy Director of Performance Audit
360-725-5629, Thomas.Furgeson@sao.wa.gov

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

To request public records

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

Introduction

State government is entrusted with vast amounts of confidential information, making its information technology (IT) systems a tempting target for hacking and cybercrime. Examples of the confidential information state government collects include Social Security numbers, health care information, arrest records and federal tax information. Indeed, research published in the Verizon 2016 Data Breach Investigations Report states the public sector experienced the most cybersecurity incidents, and the fourth-most confirmed data breach incidents, of any industry in 2015.

Whether coordinating a statewide emergency response or processing a tax payment, state government necessarily relies on complex computer systems to provide essential public services. If the state does not protect its IT systems and networks effectively, it may fail to deliver those services and put the private information of its people at risk of loss, modification, or destruction. Costs associated with remedying the effects of cyberattack are high. Recently, the U.S. Office of Personnel Management paid $133 million for credit monitoring services for the people affected by a breach of federal employee data. A 2016 study by the Ponemon Institute found it costs government an average of $86 per record lost in a data breach.

To help Washington protect its 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. Three state agencies participated in this audit.

Scope and Methodology

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

- Are these state agencies adequately protecting their confidential information from external and internal threats?
- Are their security programs aligned with select IT security leading practices?

To help conduct the audit, we hired subject matter specialists with expertise in conducting security assessments 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 first cybersecurity performance audit in 2014. 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 assessment testing

To determine whether the three selected state agencies were adequately protecting their confidential information from threats, we conducted external and internal security assessments 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 assessment, 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 assessment testing. Because the state offers many of its services to its citizens 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

We reviewed select IT security controls, including a review of policies, procedures, and technical implementation of the controls, to determine if they align with nationally-recognized leading practices. Specifically, we used the U.S. Government's National Institute of Standards and Technology (NIST) Special Publication 800-53 and 800-53A, Revision 4, to develop our criteria for assessing the effectiveness of certain information technology security controls and identifying areas that could benefit from revision to make them stronger.

We also considered the state's IT security standards in our assessment of agency information technology security controls. The state's security standards were published by the Office of the Chief Information Officer and are now under the authority of WaTech's Office of Cyber Security as Securing Information Technology Assets Standards (141.10). We decided to use the federal NIST leading practices instead of the state standards because NIST included specific details and metrics we needed to make our assessments.

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

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

Our external and internal security assessment testing found strengths in agencies' security but also uncovered issues that should be addressed. We also found the security controls (in their policies, procedures and technical implementation) we tested partially or fully align with the majority of leading practices, but there are areas where improvements can be made.

Where agency practices are not fully aligned with leading practices, agency personnel reported resource constraints and unclear state standards as the primary causes. They also said improved communication with WaTech, the state's enterprise IT service provider, would help them optimize statewide enterprise service offerings. 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. To protect the state's IT systems, and the confidential and sensitive information contained in those systems, this report does not include the agencies' names or the detailed descriptions of our results. These detailed results are exempt from public disclosure in accordance with RCW 42.56.420 (4).

Recommendations

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

To the three selected state agencies

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

To WaTech

To help ensure agencies can effectively plan and budget to make full use of WaTech's services:

- Solicit input from state agencies when procuring new services
- Provide details about new services to state agencies as early as possible. Service specifications should be set out in a "terms of service" or similar document; key specifications to consider covering include limitations, roles and responsibilities, performance measures, and security of the service.

To the Office of Cyber Security, WaTech

- Conduct outreach to state agencies to determine how additional clarity or guidance could help align practices with the state IT security standards and leading practices
- Develop and provide that additional clarity or guidance to state agencies

Agency response

JAY INSLEE
Governor

MICHAEL COCKRILL
Director & State Chief
Information Officer

STATE OF WASHINGTON

"the consolidated technology services agency" RCW 43.105.006

WASHINGTON TECHNOLOGY SOLUTIONS

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

November 1, 2016

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

Dear Auditor Kelley:

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 – 2016.

One of Washington's greatest commitments and challenges is to continuously improve how we protect confidential data, as well as prevent and eliminate security vulnerabilities. These performance audits provide great value in helping that effort.

Thank you for acknowledging the significant efforts already undertaken to protect the state's information technology (IT) systems. We agree that opportunities exist to strengthen our security and we will continue to do so.

We appreciate the careful and collaborative approach of your staff with my office and the agencies selected. We also appreciate the caution your office exercised throughout this performance audit to protect the IT security of our state.

Sincerely,

Michael Cockrill
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
Matt Steuerwalt, Executive Director of Policy
David Schumacher, Director, Office of Financial Management
Rich Roesler, Acting 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 – 2016 Nov. 1, 2016

This management response to the State Auditor's Office (SAO) performance audit report received Oct. 11, 2016, is provided by the state's Chief Information Officer on behalf of Washington Technology Solutions (WaTech) and 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 these state agencies adequately protecting their confidential information from external and internal threats?
2. Are their security programs aligned with select IT security leading practices?

SAO Issue 1: Opportunities exist to strengthen IT security.

SAO Recommendation 1: The audited agencies should continue remediating issues identified during security assessment testing and gaps identified between agency practices or documented policies and procedures and the leading practices. They should continue to assess agency's IT security needs and resources periodically, including personnel and technology, to mature and maintain sufficient security.

STATE RESPONSE:
We agree with the opportunities for improvement identified by the SAO. Agencies will continue to work diligently to remediate the issues identified between agency practices or documented policies and procedures and the leading practices. Agencies have an ongoing commitment to assess IT security needs.

Action Steps and Time Frame

- Each agency will establish a plan for the gaps and improvements identified by the end of the year. These plans will be monitored by the SAO and WaTech. *By Dec. 31, 2016.*

SAO Recommendation 2: To WaTech, to help ensure agencies can effectively plan and budget to make full use of WaTech's services:

- Solicit input from state agencies when procuring new services
- Provide details about new services to state agencies as early as possible. Service specifications should be set out in "terms of service" or similar document; key specifications to consider covering include limitations roles and responsibilities, performance measures, and security of the service.

STATE RESPONSE:
The State's Chief Information Officer (CIO) agrees that agencies should be aware of and involved in the exploration and needs of WaTech services that can be leveraged by agencies to fulfill their missions in government. A full understanding of WaTech's services can inform agencies in the development of their technology strategic plans and budgets. Terms of Service or service level agreements should provide clarity in roles and responsibilities, performance measures, security, and limitations when known.

WaTech will review and update Terms of Service to include more clarity in roles and responsibilities, performance, security and known limitations. This effort is already underway and will be ongoing as new Terms of Service and Service Level Agreements are entered.

WaTech implemented the *Service Catalog Process* to maintain the WaTech service catalog, or list of current services, effective December 2015. The planning for new WaTech services includes review with customers seeking input on those services. WaTech seeks input from customers through multiple methods including the WaTech Advisory Council, the CIO Forum, Quarterly Customer meetings and through interactions with customers on an individual basis. WaTech publishes updates to the Service Catalog on the WaTech website and on the WaTech Strategic Roadmap.

Action Steps and Time Frame

- Update the Terms of Service to include more clarity in roles and responsibilities, performance, security and known limitations. *By September 30, 2017*.
- Implement a Service Catalog Process that includes a Customer Advisory Council. *Complete*.

SAO Recommendation 3: To WaTech's Cyber Security Office:

- Conduct outreach to state agencies to determine how additional clarity or guidance could help align practices with the state IT security standards and leading practices
- Develop and provide that additional clarity or guidance to state agencies

STATE RESPONSE:
The State Office of Cyber Security agrees that agencies would benefit from additional clarity and guidance on how agency security controls and procedures could better align with state IT security standards leading best practices. Proper interpretation and application of effective IT security standards and controls has become increasingly important as the IT security threat landscape continues to change and agencies move more critical business applications to the cloud.

- The State Office of Cyber Security has already begun taking action to provide agencies with additional information on emerging IT security threats, guidance on how state IT security standards and best practices can most effectively be applied and training resources to help them protect their most critical IT assets:
  - Monthly Workshops: Every month, the State Office of Cyber Security hosts IT Security workshops. In these sessions, IT security industry experts and Office of Cyber Security

staff members provide agencies with information on new and emerging threats, technical implementations and interpretation of the state's IT security standards. These workshops also serve as a forum where agency IT security professionals can raise questions, share their successes and learn from one another. These workshops commenced in March, 2016.

- Weekly "Office Hours": The State Office of Cyber Security has set aside several hours per week to provide agencies with the opportunity to drop by and interact with staff to discuss any questions they may have regarding IT Security standards compliance, implementation of best practices, threat detection and analysis and other IT security-related questions. The Office Hours program was implemented in September 2016.
- Employee IT Security Awareness Training: In an effort to continually raise the state's overall security posture, the State Office of Cyber Security is in the process of contracting with a second firm to provide online employee IT security awareness training. As a result, agencies will have the option of using one of two curriculums to satisfy annual training requirements for their employees. This training, made available at no cost to agencies, allows all state employees to receive up-to-date instruction on what they can do to protect their work environment from exposure to commonly used threat tactics. The contracted is expected to be executed, and training in place, by December 31, 2016.

Action Steps and Time Frame

- Establish monthly workshops to provide agencies with information on new and emerging threats, technical implementations and interpretation of the state's IT security standards. *Complete.*
- Establish weekly Office Hours" for agencies. *Complete.*
- Contract with a second firm to provide online employee IT security awareness training. *Completed by December 31, 2016.*

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 Results and Recommendations sections 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 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 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 provide additional clarity or guidance to agencies to help them better align their IT security programs with leading practice controls.
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 published by the National Institute of Standards and Technology to assess select agencies' IT security controls.