Washington State Auditor's Office

Government that works for citizens

Performance Audit

Opportunities to Improve City of Mill Creek Information Technology Security

April 7, 2016

Report Number: 1016397

Table of Contents

Introduction 3
Scope and methodology.....3
Audit Results 5
Recommendations.....5
Auditor's Remarks 5
Auditee Response 6
Appendix A: Initiative 900.....7

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

Kelly Collins – Director of Local Audit
360-902-0091, Kelly.Collins@sao.wa.gov

Peg Bodin, CISA – Local Information Systems Audit Manager
360-464-0113, Peggy.Bodin@sao.wa.gov

Adam Wilson – Deputy Director for Communications
360-902-0367, Adam.Wilson@sao.wa.gov

To request public records

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

Introduction

Government organizations have become increasingly dependent on computerized information systems to carry out their operations. These systems are used to process, share and store sensitive and confidential information, including personal and financial data, in order to deliver services to residents.

Risks to a local government's information technology (IT) environment go beyond the activities of hackers stealing credit card numbers or Social Security numbers, or malware being placed to disrupt communications. Errors or misuse of the system by employees or contractors can also jeopardize the smooth, secure operation of any entity that relies on computers and networks.

A study published in 2014 found that governments have a one-in-four chance of experiencing a data breach of more than 10,000 records within the next two years, and estimated that the average cost for each government record lost is $172. That study also found that the public sector experienced the greatest number of cybersecurity incidents and confirmed data losses of any industry.

To help Washington's local governments protect their IT systems, we are offering them the opportunity to participate in a performance audit designed to assess whether there are opportunities to improve their IT security.

The City of Mill Creek was the first local government to take advantage of this opportunity.

Scope and methodology

The performance audit we conducted was designed to answer the following questions:

- Do the local government's IT security policies, standards and procedures align with leading practices?
- Has the local government implemented effective IT security practices to protect its information and are they consistent with leading practices?

Comparing the City's IT security program to leading practices

To determine whether Mill Creek's IT security program aligns with leading practices, we engaged subject matter experts to compare the City's IT security policies, procedures and practices to leading practices, and identify areas that could benefit from revision to make them stronger. The leading practices we used for our comparison were primarily based 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) in Special Publication 800-53, Revision 4 "Security and Privacy Controls for Federal Information Systems and Organizations".

In conducting our analysis we also reviewed documentation and conducted interviews with City staff.

Evaluating effective implementation of IT security practices

To determine if the City has implemented effective IT security practices, our subject matter experts used customized software scripts to determine if controls were implemented properly and functioning effectively.

Additionally, our subject matter experts conducted vulnerability tests on the City's IT infrastructure and ranked the identified weaknesses by the severity and ease in which the identified weakness could be exploited, based on their professional experience.

We gave City management the results of the tests as they were completed, then conducted follow-up testing to determine if they had successfully mitigated the weaknesses we identified.

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 local government programs and services are reviewed by the local government's legislative body and/or by other committees of the local government whose members wish to consider findings and recommendations on specific topics. Representatives of the State Auditor's Office will review this audit with the City of Mill Creek's legislative body in the City of Mill Creek. The public will have the opportunity to comment at this hearing. Please check the City of Mill Creek website for the exact date, time and location. 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 City of Mill Creek has already addressed the most significant issues but opportunities exist to further strengthen its IT systems

The City of Mill Creek has taken measures to protect its IT systems from risks, but opportunities exist to strengthen its IT security. We found that while the City's information security policies and practices partially align with industry leading practices, there are several areas where improvements can be made. The City of Mill Creek has already addressed the most significant issues we identified and is continuing to improve its security program.

We have provided the management of the City of Mill Creek the details of our results and recommendations. To protect the City's IT systems, and the confidential and sensitive information contained in those systems, this report does not include detailed descriptions of our results. These detailed results are exempt from public disclosure in accordance with RCW 42.56.420 (4).

Recommendations

To help ensure the City of Mill Creek protects its information technology systems and the information contained in those systems, we make the following recommendations:

- Continue remediating identified gaps.
- Revise the City's IT security policies and procedures to more closely align with leading practices.

Auditor's Remarks

The State Auditor's Office recognizes the City of Mill Creek's willingness to volunteer as the first local government to participate in this audit demonstrating their dedication to making government work better. It is apparent the City's management and staff want to be accountable to the citizens and good stewards of public resources. They understand the value of our audits and have fostered a positive and professional working relationship with the Washington State Auditor's Office.

Auditee Response

March 14, 2016

Jan Jutte
Deputy State Auditor
P.O. Box 40021
Olympia, WA 98504-0021

Dear Ms Jutte:

On behalf of the City of Mill Creek, thank you for the opportunity to review and respond to the State Auditor's Office performance audit report "Opportunities to Improve City of Mill Creek Information Technology Security."

It was a pleasure to work with Peg Bodin, Aaron Munn, and other staff from your office as well as the subject matter experts who evaluated Mill Creek's IT security program. We have been continually impressed with the professionalism and collaborative approach taken by your office in our many interactions.

Thank you for recognizing the measures we have already taken to protect our IT systems from numerous threats. We appreciate the efforts of your staff and subject matter experts to evaluate our current IT security posture and recommend opportunities for improvement. Many of the recommendations have already been put into place and have strengthened our IT security program. We remain committed to continuous improvement to address the recommendations in the report.

Sincerely,

James Busch
Director of IT
City of Mill Creek

15728 Main Street Mill Creek, WA 98012 • Administration ph: 425-745-1891 fx: 425-745-9650
Police ph: 425-745-6175 fx: 425-745-4680 • www.cityofmillcreek.com

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 objectives were focused on improving information security and did not identify cost savings.
2.	Identify services that can be reduced or eliminated	**No.** The audit objectives were focused on improving information security and did not address services that could be reduced or eliminated.
3.	Identify programs or services that can be transferred to the private sector	**No.** The audit objectives were focused on improving information security and did not address programs or services that can be transferred to the private sector.
4.	Analyze gaps or overlaps in programs or services and provide recommendations to correct them	**Yes.** The audit identified gaps in the City's information security program.
5.	Assess feasibility of pooling information technology systems within the department	**No.** The audit objectives were focused on improving information security and did not address pooling information technology systems.
6.	Analyze departmental roles and functions, and provide recommendations to change or eliminate them	**Yes.** The audit identified recommendations to improve the City's information security function.
7.	Provide recommendations for statutory or regulatory changes that may be necessary for the department to properly carry out its functions	**No.** The audit objectives were focused on improving information security and did not identify a need for statutory or regulatory change.
8.	Analyze departmental performance, data performance measures, and self-assessment systems	**No.** The audit objectives were focused on improving information security and did not address the local government's performance measures and self-assessment systems.
9.	Identify relevant best practices	**Yes.** The audit used leading practices to identify improvements that can be made to the City's information security program.