Office of the Washington State Auditor

Pat McCarthy

Performance Audit

Opportunities to Improve King County's Information Technology Security

May 2, 2019

Report Number: 1023665

Table of Contents

The mission of the State Auditor's Office

Provide citizens with independent and transparent examinations of how state and local governments use public funds, and develop strategies that make government more efficient and effective.

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 & IT Audit
360-902-0376, **Scott.Frank@sao.wa.gov**

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

Peg Bodin, CISA – Assistant Director of IT Audit
360-464-0113, **Peggy.Bodin@sao.wa.gov**

Kathleen Cooper – Director of Communications
360-902-0470, **Kathleen.Cooper@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 process, store and share 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 information, Social Security numbers, or installing malware to disrupt communications. Errors or misuse of the system by employees or contractors can also jeopardize the operation of any entity that relies on computers and networks.

Furthermore, research by Verizon Wireless in their 2018 Data Breach Investigation Report shows that the public sector reported the most cyber security incidents. A 2018 study by the Ponemon Institute, a research center that focuses on privacy, data protection and information security policy, found that governments pay an average of $75 per record lost in a data breach.

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 the security of their IT systems.

King County chose to participate in this audit.

Scope and methodology

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

- Is the County's public-facing IT presence secure from known external threats?

Evaluating the County's IT systems against external and internal threats

To determine if the County's IT systems are secure against external threats, our subject matter experts conducted tests on the County's external IT infrastructure, and ranked the identified weaknesses by the severity and ease with which the identified weakness could be exploited based on their professional experience.

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

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 King County's legislative body in Seattle, Washington. The public will have the opportunity to comment at this hearing. Please check the King County 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. See **Appendix A**, which addresses the I-900 areas covered in the audit.

Audit Results

The results of our audit work and recommendations were communicated to King County management for their review, response and action. We found that there were areas where improvements can be made. The County has already addressed issues we identified, and is continuing to make improvements.

Because the public distribution of tests performed and test results could increase the risk to the County, distribution of this information is kept confidential under RCW 42.56.420(4), and under Generally Accepted Government Auditing Standards, Sections 7.40-43.

Recommendations

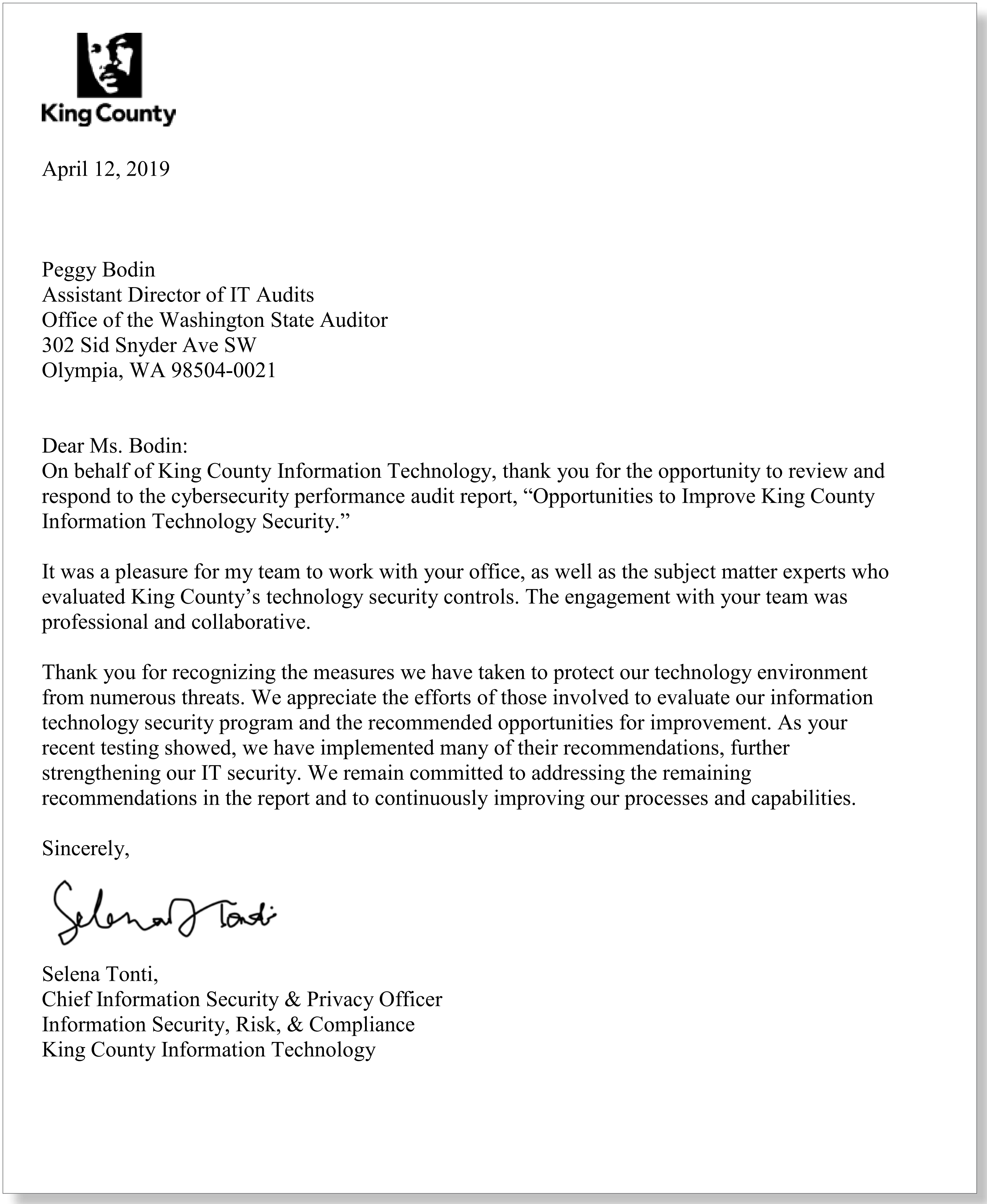
To help ensure that King County protects its information technology systems and the information contained in those systems, we make the following recommendation:

- Continue remediating identified gaps

Auditor's Remarks

The State Auditor's Office recognizes King County's willingness to volunteer to participate in this audit, demonstrating its dedication to making government work better. It is apparent the County's management and staff want to be accountable to the people and good stewards of public resources. Throughout the audit, they fostered a positive and professional working relationship with the Washington State Auditor's Office.

Auditee Response



King County

April 12, 2019

Peggy Bodin
Assistant Director of IT Audits
Office of the Washington State Auditor
302 Sid Snyder Ave SW
Olympia, WA 98504-0021

Dear Ms. Bodin:

On behalf of King County Information Technology, thank you for the opportunity to review and respond to the cybersecurity performance audit report, “Opportunities to Improve King County Information Technology Security.”

It was a pleasure for my team to work with your office, as well as the subject matter experts who evaluated King County’s technology security controls. The engagement with your team was professional and collaborative.

Thank you for recognizing the measures we have taken to protect our technology environment from numerous threats. We appreciate the efforts of those involved to evaluate our information technology security program and the recommended opportunities for improvement. As your recent testing showed, we have implemented many of their recommendations, further strengthening our IT security. We remain committed to addressing the remaining recommendations in the report and to continuously improving our processes and capabilities.

Sincerely,

Selena Tonti

Selena Tonti,
Chief Information Security & Privacy Officer
Information Security, Risk, & Compliance
King County Information Technology

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 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 the County avoid or mitigate costs associated with a data breach.
2. Identify services that can be reduced or eliminated	**No.** The audit objectives 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 the County's information system security program.
4. Analyze gaps or overlaps in programs or services and provide recommendations to correct them	**Yes.** The audit compares the County's IT security 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 the County's IT security posture.
6. Analyze departmental roles and functions, and provide recommendations to change or eliminate them	**No.** The audit did not analyze departmental roles and functions.
7. Provide recommendations for statutory or regulatory changes that may be necessary for the department to properly carry out its functions	**No.** The audit did not identify a need for statutory or regulatory change.
8. Analyze departmental performance, data performance measures, and self-assessment systems	**Yes.** Our audit examined and made recommendations to improve IT security control performance.
9. Identify relevant best practices	**Yes.** Our audit tested the County's externally facing assets for vulnerabilities that could be used to compromise the County's IT systems.

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.