PUBLIC TESTIMONY SUMMARY

I-900 STATE AUDITOR'S PERFORMANCE AUDIT:

Safe Data Disposal – Protecting Confidential Information (April 10, 2014)

As Heard by the Joint Legislative Audit & Review Sub-Committee on I-900 Performance Audits on April 23, 2014

The performance audit being discussed at this hearing was conducted solely and independently by the office of the State Auditor, under the authority of legislation approved by the voters in Initiative 900. The State Auditor is elected directly by the people of the State of Washington and operates independently of the Legislature and the Joint Legislative Audit & Review Committee. Staff to the Joint Legislative Audit & Review Committee prepare a summary of public testimony on State Auditor reports. These summaries are for informational purposes only, and do not serve as an assessment by committee staff of the findings and recommendations issued by the State Auditor nor do they reflect a staff opinion on legislative intent.

Title: Safe Data Disposal – Protecting Confidential Information

Audit Scope and Objectives:

SAO indicates it designed this audit to answer the following questions:

1. Do state organizations remove confidential data stored in their computers before they are released for surplus or destruction?
2. Do state organizations' computer disposal policies, procedures, and processes comply with state requirements and follow best practices?

SAO reports it conducted its analysis by examining a sample of all surplus computers sent to the Department of Enterprise Services surplus program over a six-week period during the summer of 2013.

SAO Findings:

- Computers released as surplus contained confidential data that should have been erased. SAO estimates 9 percent of the computers sent to the surplus program during the SAO review contained confidential data.
- Reasons why data remained on drives varied between organizations, but human error played a part.
- Discrepancies were found between physical count and inventory lists at the DES warehouse.

SAO Findings (continued)

- Organizations did not always comply with the Office of the Chief Information Officer (OCIO) requirements or employ best practices for disposing of computers.
- Having a documented procedure does not guarantee completely erased computer hard drives.
- Even at organizations that did not have confidential data on their computers in the SAO sample, policies and procedures did not always meet OCIO Standards.

After SAO shared its audit test results with the state organizations and the OCIO, SAO reports they reacted swiftly to address the problem.

SAO Recommendations:

In addition to the actions the OCIO has already taken, SAO recommends the OCIO:

- Engage state IT and security leaders to modernize the methods available to organizations to meet the OCIO Standards (hard drive destruction and recycling services).
- Revise the current version of the OCIO's Security Standards Section 8.3 to:
    - Require state organizations to employ the NIST best practices, which would address OCIO Step 8.3.3 by replacing the word “ensure” with “verify”.
    - Require proper documentation stating that data has been properly deleted from computer hard drives, or that hard drives have been properly destroyed.
- Review the state organizations' documented media handling and disposal procedures to ensure they meet the OCIO Standards Section 8.3.
- Continue to halt the release of computers for organizations whenever the OCIO has reason to doubt their compliance with the OCIO Standards Section 8.3.

SAO makes two recommendations to state organizations:

1. The following organizations establish documented procedures to ensure safe and secure disposal of sensitive and confidential information. The procedures should align with the OCIO Security Standards for computer handling and hard drive disposal:

   * Department of Social and Health Services
   * Department of Transportation
   * State Parks & Recreation Commission
   *State Senate

2. As a best practice, the following organizations should include in their procedures a step to verify and record that confidential data is appropriately removed from computer hard drives before releasing to surplus:

   * Department of Ecology
   * Department of Fish and Wildlife
   * Department of Health
   * Department of Labor and Industries
   * Department of Natural Resources
   * Department of Revenue
   * Department of Social and Health Services
   * Department of Transportation
   * Office of the Insurance Commissioner
   * State Parks & Recreation Commission
   * State Senate

Agency Responses in Audit Report?	Yes, beginning on page 16
Legislative Action Requested?	There are no actions requested for the Legislature as a whole. SAO makes the two recommendations above to a number of organizations, including the State Senate.

Agencies Testifying:

The Office of Financial Management (Tracy Guerin, Deputy Director)

The Office of the Chief Information Officer (Michael Cockrill, Chief Information Officer)

Summary of Testimony from Audited Agencies:

We thank the SAO staff for working closely on this audit with the OCIO and the affected agencies. As the audit points out, agencies were able to take corrective actions immediately after their notification of the issues. The state takes its responsibilities seriously and is committed to protecting personal information and eliminating security vulnerabilities. The written response from the agencies provides some dates by which certain actions will be accomplished. A second document describes the Computers for Kids program, which explains how the computers are wiped a second time before being released to this program.

This audit was different than most SAO audits because the audit found an ongoing vulnerability, and we appreciate how they worked with us to resolve it. In the computer security world, there is a model called “the responsible disclosure” model. We took a parallel model to make sure all the vulnerabilities were eliminated before any public disclosure was made about the vulnerability.

When a vulnerability is identified, a three-step process follows that OCIO and each of the agencies went through: 1) eliminate the vulnerability as quickly as possible; 2) find the root cause; and 3) figure out a mitigation plan. For the first step, we froze the shipments out of the surplus warehouse, and most of the agencies did something similar about further shipments to the warehouse. To investigate the root cause, we asked if there was a systemic problem or if this was human error. We reviewed the OCIO policies and procedures and compared these to national standards, and the agencies reviewed their policies and procedures for compliance with the state standards. What we found was not a systemic problem but a situation where sometimes human beings made mistakes. Properly wiping a hard drive is actually a complex process; it takes about three hours to do it right, and sometimes we did not do the right double-checks.

There has been no evidence and no reports of personal consumer date being released. The agencies all have policies and procedures in place, but sometimes we don’t follow them properly. The short-term plan for mitigation is what the audit points out – an extra step of human checking. In the long run, if you have humans in the chain who are making errors, attempt to take the humans out of that step. We are looking for ways to do that. The audit intentionally focused on one part of the process, at the agency actions before shipping the computers to the warehouse. What the audit did not reflect was that the majority of computers that leave the warehouse go to a facility in Spokane (Airway Heights) where they undergo another wipe, under a more detailed and documented procedure. This program has been in place since 2000. Also, even on the computers which did have some information on them, the information was not easily accessible.

The program at Airway Heights provides a safety net, and now all computers will go through that process.

We have published the SAO report on the OCIO website, and we also sent some information to other jurisdictions reminding them of the importance of this.

Other Parties Testifying:

(No other parties signed in to testify)

Summary of Testimony from Other Parties:

(No other parties signed in to testify)