Washington State Auditor's Office

Troy Kelley

Independence • Respect • Integrity

Information Technology Security

Pacific NW Intergovernmental Audit Forum

September 25, 2014

Lou Adams, CPA, Deputy Director of Performance Audit

Susan Hoffman, Principal Performance Auditor

Overview

- Safe Data Disposal – Protecting Confidential Information
- Statewide Information Technology Audit Risk Assessment

Safe Data Disposal – Audit Questions

- Do state agencies remove confidential data stored in their computers before they are released for surplus or destruction?

- Do state agencies’ computer disposal policies, procedures, and processes comply with state requirements and follow best practices?

What we did

- We selected a sample of computers from 13 state agencies sent to the surplus program over a **six-week period**.
- We tested the computers to see if they contained confidential information.
- We reviewed agency policies to see if they were sufficient compared to the OCIO Security Standards and nationally recognized best practices.

Surplus computers contained confidential data

Personal information

- Social Security numbers
- Medical records
- Applications for public assistance
- IRS tax forms
- Claims records
- Personal financial

Employee information

- Job applications
- Employee evaluations

IT security information

- Logon and password information

Surplus computers contained confidential data

- We found 11 of the 177 computers we tested contained confidential information
- Using statistical analysis, we projected that 109 of the 1,215 computers sent for surplus contained confidential information

9%

of computers contained confidential data

Why confidential information was not deleted

In most cases, human error appeared to be the cause for data not being deleted.

- Computers were mistakenly released for surplus before data was removed
- Some broken computers were presumed to be clean

Recommendations

We recommend that:

- The OCIO improve its oversight and the security standards they provide to agencies
- State agencies without documented procedures establish them
- State agencies add a step in their procedures to verify and record that confidential data is appropriately removed

Statewide IT Audit Risk Assessment

Purpose: To provide the Washington State Auditor’s Office with an approach and methodology to conduct a comprehensive statewide IT risk assessment, and to:

- Define SAO’s role in auditing the state’s IT programs and functions
- Use the information gathered to develop a multi-year risk-based IT audit work plan
- Position the SAO to effectively execute that work plan

Statewide IT Audit Risk Assessment

Role of IT security in the assessment:

- Gathering input from the key players in ensuring the state's IT security
- Determining what of audits we should be doing
- Determining what skills we need to conduct those audits
- Gaining insight on how to report our findings

Contacts

Troy Kelley
State Auditor
(360) 902-0360
Troy.Kelley@sao.wa.gov

Chuck Pfeil, CPA
Director of Performance Audit,
(360) 902-0366
pfeilc@sao.wa.gov

Lou Adams, CPA
Deputy Director of Performance Audit,
(360) 725-5577
adamsl@sao.wa.gov

Susan Hoffman, MPA
Principal Performance Auditor
(360) 725-5620
hoffmans@sao.wa.gov

Website: www.sao.wa.gov