OFFICIAL STATE CABINET AGENCY RESPONSE TO THE PERFORMANCE AUDIT ON SAFE DATA DISPOSAL – PROTECTING CONFIDENTIAL INFORMATION APRIL 8, 2014

This coordinated management response to the State Auditor's Office (SAO) performance audit report received March 24, 2014, is provided by the Office of Financial Management and the Office of the Chief Information Officer (OCIO) on behalf of the following audited agencies: the departments of Ecology, Enterprise Services, Employment Security, Fish and Wildlife, Health, Labor and Industries, Revenue, Social and Health Services, Transportation, and the State Parks and Recreation Commission. Agencies governed by a separately elected official will respond separately.

SAO Performance Audit Objectives:

1. Do state organizations remove confidential data stored in their data processing equipment before being released for surplus or destruction?
2. Do state organizations' data processing disposal policies, procedures, and processes comply with state requirements and best practices?

SAO Issue 1: Computers released as surplus contained confidential data that should have been erased.

STATE RESPONSE

We agree with the SAO finding that 11 of the 177 computers sampled contained some residual confidential data and other information. These computers were sent to surplus by four agencies. Agencies typically send computers to surplus when they have reached the end of their useful life.

When the agencies investigated how these computers made it to surplus with confidential information, they found that human errors were the cause in most cases. In some cases, the computer drives were wiped, but not properly. We recognize these errors underscore the need for continually reviewing and strengthening erasing processes.

The state took immediate and appropriate corrective actions to resolve the issues. Actions by state agencies include:

Ecology

The Department of Ecology took immediate actions to improve its safe data disposal process to ensure compliance with state requirements and best practices, including:

- Non-leased IT equipment is no longer sent to surplus with the hard drives installed.
  - When non-leased IT equipment is ready for surplus, hard drives are removed and inventoried with a two-person validation process. The drives are then secured in a locked container for monthly/quarterly destruction, which is witnessed by two staff.
- For leased laptop equipment, Ecology requires a two-person validation where devices are wiped clean of data before returning them to the vendor.

- A supervisor's signature is required to validate that devices have been destroyed or wiped, depending on whether the equipment is owned or leased.
- Updating of security policies to make specific reference to safe data disposal policies and standards.

Health

The Department of Health immediately put into place a two-person verification and sign-off process to ensure all hard drives are removed from computers prior to the computers leaving department control. The agency also embarked on a quality improvement initiative to identify additional improvements it can make to its equipment surplus process.

Labor and Industries

The Department of Labor and Industries (L&I) began taking corrective actions as soon as the agency was made aware of the data disposal issue. The performance audit identified issues with a new L&I process used to surplus equipment. Under certain conditions, the data erase step did not completely remove data from the hard drive.

- Once L&I learned about this issue, the agency put an immediate hold on equipment headed for surplus. A technical team was assigned to investigate. Using Lean methodologies, a successful, repeatable data-cleaning process has been reestablished.
- In February 2014, L&I added a verification step to its data disposal process. L&I's surplus process is now in full compliance with the OCIO security standards and best practices. The successful removal of all data from computer equipment targeted for surplus is now officially documented and tracked in L&I's inventory tracking system.
- L&I is confident this new data-cleaning process is efficient and that its surplused equipment will be thoroughly cleaned of all data.

Social and Health Services

The Department of Social and Health Services (DSHS) immediately instituted a process to prevent any machines from going to surplus without signed documentation that all data has been removed. This was communicated to various technology groups in DSHS. A more formal process to ensure safe data disposal has recently been communicated to the agency. It retains the requirement to document the destruction of all data on media, and the DSHS warehouse is instructed to refuse acceptance of any media without the appropriate destruction documentation. A Lean process is scheduled to develop a new disposal procedure that should result in a more streamlined process with even greater protection of data.

Additional Actions

The Department of Enterprise Services also began sending *all* surplus computers it receives from state agencies to the Computers for Kids (C4K) program, where hard drives are immediately removed and wiped to the U.S. Department of Defense standards by a state Department of Corrections employee at the Airway Heights correctional facility. The computers are then refurbished by inmates through the computer production program and given or sold at a sizable discount to Washington public schools. This program has been in existence since 1998, and has provided more than 75,000 computers to schools. All data is securely wiped before computers enter this program, and no inmate is able to access hard drives or storage media before a computer has been securely wiped by a state employee.

Prior to the performance audit, most surplus computers processed by DES were sent to the C4K program and securely wiped. While this does not relieve agencies from their responsibility to remove all data from computers, it did provide an important safety net to ensure confidential data is completely removed from state computers.

Additional Information Found Non-Confidential

The report stated one operating system was still installed. That agency's normal practice is to remove drives before sending computers to surplus; however, one computer made it through due to human error. The agency has added controls including documented verification of removal.

The report also identified that non-work related photos were found on one computer. That agency has already taken action to investigate the issue.

Discrepancy in counts from one agency

The SAO's report identified some discrepancies in the number of computers from one agency at the DES surplus warehouse. According to DES surplus staff, discrepancies like this happen from time to time. When they do, surplus staff contact the agency and determine what happened. In this case, the agency had not been contacted yet because surplus staff were required to freeze all activity while the audit was being conducted.

Action Steps and Time Frame

- *(See OCIO's actions under SAO's recommendations 1-4 and 6)*

SAO ISSUE 2: Organizations did not always comply with the OCIO's requirements or employ best practices for disposing of computers.

SAO RECOMMENDATIONS 1-4 TO THE OCIO:

- Engage state IT and security leaders to modernize methods available to organizations to meet the OCIO Standards (hard drive destruction & recycling services)
- Revise the current version of the OCIO Security Standards 8.3 to:
  - require state organizations to employ 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 end-of-life digital media storage devices for organizations wherever the OCIO has reason to doubt their compliance with the OCIO Standards Section 8.3.

STATE RESPONSE

The state is committed to protecting confidential data and eliminating and preventing security vulnerabilities. As the SAO highlighted in the audit report, the OCIO immediately quarantined all state computers at the surplus store, halted sales, and provided additional guidance to state

agencies. While the state acted quickly to resolve this particular issue, the SAO report reflects the need to continually review each agency's data removal processes. We agree that the state must always work to keep security standards up to date in the ever-evolving cybersecurity landscape.

In addition to the actions mentioned in the performance audit report, the OCIO:

- Conducted an immediate evaluation of IT security standards involving data removal, concluding that proper standards were in place but agencies were not consistently meeting them. The additional guidance for meeting standards was the result of this evaluation.
- Conducted a security assessment of the DES warehouse.
- Conducted a security assessment of the data removal process administered as part of the C4K program.
- Formed a cross-agency task force to make recommendations for updating state data destruction policy, including the promotion of additional methods of meeting OCIO standards such as through physical destruction.

Action Steps and Time Frame

- Complete cross-agency task force work, resulting in more robust methods for agencies to meet the data disposal standards identified in state IT security policy. *By April 30, 2014.*
- Strengthen IT security standards, including the addition of a verification step to ensure that the data has been destroyed. *By April 30, 2014.*
- Work with DES and agencies to update surplus procedures as an additional safeguard. *By May 30, 2014.*
- Update data-wiping procedures and tools available to agencies. *By May 30, 2014.*
- Review each state agency's documented data handling and removal processes. *By June 30, 2014.*

SAO Recommendation 5: The Departments of Social and Health Services (DSHS), Transportation (WSDOT) and State Parks and Recreation Commission (Parks) should 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.

STATE RESPONSE

We agree that our current procedures to ensure safe and secure disposal of all data should be well documented and align with the OCIO's security standards. The three agencies contributing to this response are in various stages of documenting or modifying their data disposal procedures.

Action Steps and Time Frame

- DSHS: Institute a process to document that data was destroyed or removed across all program areas. *Complete.*
- DSHS: Issue a technical bulletin to all program areas to institute a process to document safe data disposal and prevent surplus of any machines with data. *Complete.*

- DSHS: Complete a Lean process to improve all aspects of surplus, including data destruction/disposal. *By December 31, 2014.*
- DSHS: Finalize safe data disposal procedures. *By December 31, 2014.*
- WSDOT: Prior to the audit, WSDOT purchased a hard drive shredder. After making related electrical system improvements in its facility, WSDOT began operating the shredder in November 2013. WSDOT now shreds all hard drives. *Complete*
- WSDOT: Update procedures for safe data disposal to align with OCIO standards. *By June 30, 2014.*
- Parks: Document safe data disposal procedures. *By April 18, 2014.*

SAO Recommendation 6: As a best practice, the Departments of Ecology, Fish and Wildlife, Health, Labor and Industries, Revenue, Social and Health Services, Transportation and State Parks and Recreation Commission 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.

STATE RESPONSE

While many of these agencies were found to be in compliance with OCIO standards at the time of the performance audit, we agree that all agencies should have practices and procedures for verifying that all confidential and other data is completely erased or destroyed prior to release for surplus. The OCIO will make this more clearly required for all state agencies in its standards and will work with them to update their procedures appropriately.

Action Steps and Time Frame

- The OCIO will work with all state agencies/organizations to require them to include a verification step in their data disposal procedures. *By May 30, 2014.*