STATE OF WASHINGTON

April 8, 2014

The Honorable Troy Kelley
Washington State Auditor
P.O. Box 40021
Olympia, WA 98504-0021

Dear Auditor Kelley:

We appreciate the opportunity to respond to the State Auditor's Office (SAO) performance audit report on "Safe Data Disposal – Protecting Confidential Information." The Office of Financial Management and the Office of the Chief Information Officer (OCIO) worked with the audited agencies to provide a consolidated response. Agencies governed by a separately elected official will respond separately.

The state is committed to protecting confidential data and eliminating or preventing security vulnerabilities. While the state acted quickly to resolve this issue, the SAO audit reflects the need to continually review each agency's data removal processes. This audit is an excellent example of government working together to discover, scope and resolve a problem.

Information security is a responsibility shared by every organization and individual in state government. The OCIO governs information technology policy and standards for the executive branch of state government — including security. In this vein, the OCIO is responsible for setting and maintaining security standards in a landscape of constant change. Agencies must adopt policies and procedures that follow these standards and must make sure those standards are working as intended. Agencies must also ensure that all data has been removed from any equipment leaving their custody.

The SAO identified vulnerabilities that will be addressed through changes in policies, procedures and actions. The audit findings include:

- Confidential data and other information on 11 of 177 computers from four agencies.
- Four agencies that did not have documented procedures.
- Ten agencies that did not follow best practices for verifying that data is erased or destroyed.

There have been no reports of personal information being compromised. When agencies investigated how a small number of computers containing confidential information were released to surplus, they found that, in most cases, human error was the cause. In some cases, the computer drives had been wiped, but not thoroughly. At two agencies, the practice was to remove the hard drives before sending computers to surplus, yet a few PCs were surplused with hard drives in place.

As the audit report highlights, the state took swift action when these vulnerabilities were identified. The OCIO immediately quarantined all state computers at the surplus store, halted sales, and provided additional guidance to state agencies. Other actions already taken by the OCIO include:

- Assessing the security of the Department of Enterprise Services' (DES') warehouse and the Airway Heights correctional facility's data removal process as part of the Computers 4 Kids program.
- Initiating a cross-agency task force to make more robust methods available to agencies to meet the data disposal standards identified in state IT security policy.

Additional agency actions are detailed in the attached official audit response action plan.

We agree that current procedures to ensure safe and secure disposal of all data should be well documented and align with the OCIO's security standards. The agencies that are part of this joint response are in varying stages of documenting or modifying their data disposal procedures as outlined in the attached action plan.

While many of the 13 audited agencies were found to be in compliance with OCIO standards, we agree that all agencies should add a step to their procedures to verify that all confidential and other data is completely erased or destroyed prior to releasing the computer to surplus. The OCIO will revise the language in the Security Standard 8.3.3 to more clearly require that agencies verify that data has been erased or destroyed.

Although the performance audit did not address what happens to surplus computers after arriving at the DES warehouse, it is an important step of the process that has been reviewed by the OCIO. The majority of computers were donated by DES to the Computers 4 Kids program, which reconfigures surplus computers for use in Washington public schools. These computers are shipped to the Airway Heights correctional facility, where hard drives are removed in a secure facility and wiped by a state employee to U.S. Department of Defense standards.

Before the OCIO's computer quarantine was lifted, DES put processes in place to ensure that all state computers are sent to the Computers 4 Kids program. While this process offers a good safety net, it does not release agencies from their responsibility to verify computers are fully erased before leaving their custody.

We thank the SAO and the performance audit team for their work on this report. We share your belief that information security is a matter of utmost importance that requires continuous vigilance.

Sincerely,

David Schumacher
Director

Michael Cockrill
Chief Information Officer

cc: Joby Shimomura, Chief of Staff, Office of the Governor
Kelly Wicker, Deputy Chief of Staff, Office of the Governor
Ted Sturdevant, Executive Director for Legislative Affairs, Office of the Governor
Tracy Guerin, Deputy Director, Office of Financial Management
Wendy Korthuis-Smith, Director, Results Washington, Office of the Governor
Tammy Firkins, Performance Audit Liaison, Results Washington, Office of the Governor
Maia Bellon, Director, Department of Ecology
John Wiesman, Secretary, Department of Health
Joel Sacks, Director, Department of Labor and Industries
Kevin Quigley, Secretary, Department of Social and Health Services
Lynn Peterson, Secretary, Department of Transportation
Chris Liu, Director, Department of Enterprise Services
Dale Peinecke, Commissioner, Employment Security Department
Don Hoch, Director, Washington State Parks and Recreation Commission
Phil Anderson, Director, Department of Fish and Wildlife
Carol Nelson, Director, Department of Revenue
Rob St. John, Director, Consolidated Technology Services
Agnes Kirk, Chief Security Officer, Consolidated Technology Services