Washington State Auditor's Office
Troy Kelley
Independence • Respect • Integrity

Performance Audit

Safe Data Disposal – Protecting Confidential Information

April 10, 2014

Before state government organizations release computers they no longer need for sale or surplus, state laws require they erase all data, including confidential information such as Social Security numbers, medical information, and IT system and security information. We checked a sample of computers sent for surplus and estimate that 9 percent of the computers scheduled for sale during our review period contained confidential data that should have been removed.

We recommend state organizations follow a national best practice to conduct a final check to verify all data has been removed before releasing computers. We also recommend the Office of the Chief Information Officer improve its policies and oversight for agency data disposal practices. The OCIO and the organizations involved responded swiftly to our findings, stopping the release of surplus computers and improving data removal policies.

Audit Number: 1011501

Table of Contents

State Auditor's Office contacts

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

Chuck Pfeil, CPA :: Director of State & Performance Audit
360-902-0366, Chuck.Pfeil@sao.wa.gov

Lou Adams, CPA :: Deputy Director of Performance Audit
360-725-9741, Lou.Adams@sao.wa.gov

Todd Larson :: Senior Performance Auditor
360-725-9734, Todd.Larson@sao.wa.gov

Thomas Shapley :: Deputy Director of Communications
360-902-0367, Thomas.Shapley@sao.wa.gov

To request public records

Mary Leider :: Public Records Officer
360-725-5617, PublicRecords@sao.wa.gov

Executive Summary

Why we did this audit

In the last two years, Washington's state agencies, boards and commissions sent almost 20,000 computers to surplus when they were no longer needed. The Department of Enterprise Services (DES) surplus program distributes some of these computers to other state organizations, school districts, or non-profit groups. The remaining computers are sold to the public through the surplus program website or at the DES Surplus Store in Tumwater, WA. The revenue collected from the sale of these computers is used to fund the surplus program and purchase new equipment for state organizations.

Before state organizations release computer equipment for disposal, state laws require them to erase all data, including confidential information such as social security numbers and personal medical information, as well as Information Technology (IT) system and security data from their hard drives. State standards also require state organizations to document their computer disposal procedures. Leaving confidential data on computers can expose both individuals and organizations to identity theft and fraud, and violates state and federal law.

We wanted to assess how well state organizations comply with statutes and employ best practices as identified in the Office of the Chief Information Officer (OCIO) Security Standard 141.10. The OCIO is responsible for the state's IT security standards. We also wanted to identify opportunities to improve computer disposal operations and minimize the risk of confidential data being released.

We designed our audit to determine if state organizations remove confidential data stored in their data processing equipment before releasing them for surplus or destruction, and if their data processing disposal policies, procedures and actual processes comply with state requirements and employ best practices.

Not all state organizations removed confidential data stored in their computers before releasing them for surplus or destruction.

Four of the 13 organizations whose surplus computers we tested had released equipment containing confidential data. They were the:

- Department of Ecology
- Department of Health
- Department of Labor & Industries
- Department of Social and Health Services

The State Auditor's Office created a stratified statistical sample of all surplus computers and inspected computers from 13 state organizations sent to the surplus program over a six-week period. We estimate that 9 percent, or 109, of the 1,215 computers scheduled for surplus during our review period contained confidential information.

We recovered files from the computers' hard drives. With the right knowledge of data retrieval, the confidential information we found could be obtained in a few minutes. Had these computers been sold, the presence of confidential information on their hard drives posed a risk of harm to private individuals and the state.

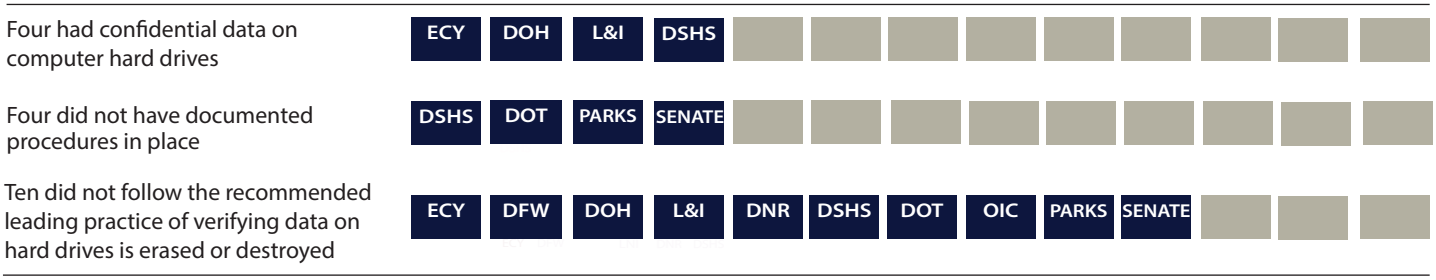
Confidential data found on state surplus computers included:

- ► Applications for public assistance
- ► Medical records
- ► Personal financial statements
- ► Employee performance evaluations
- ► IRS tax forms
- ► Social Security numbers
- ► IT security and system information
- ► Claims records
- ► Employment applications

Not all state organizations' data processing disposal policies, procedures, and processes were in compliance with state requirements and followed best practices.

We reviewed the procedures of all 13 organizations and found significant inconsistencies between and within them.

Of the 13 state organizations whose surplused computers and data disposal processes and policies we examined…



We also compared the OCIO Security Standards to guidance published by the National Institute of Standards and Technology (NIST). The OCIO'S standards refer to the NIST guidance as "best practices," but we found that the standards did not clearly require state organizations to employ those best practices. The NIST best practices specifically include steps to verify and document data is properly deleted.

Two state organizations did employ best practices by including a step in their procedures to verify that data was removed from their computer hard drives, as recommend by NIST. Those organizations were the Employment Security Department and the Department of Enterprise Services.

The state responded swiftly to our audit test findings

After we shared our audit test results with the state organizations and the OCIO, the state organizations reacted swiftly to address the problem.

The OCIO immediately quarantined computers at the surplus store, halted sales, and provided additional guidance to state organizations and is in the process of evaluating its computer disposal policies. The organizations that we found had confidential data on their computers took immediate steps to resolve the problems and are reviewing their procedures. One organization immediately assigned an employee to examine every computer hard drive after it had been sanitized to verify that no data remained.

Recommendations

In order to ensure state organizations comply with state requirements and follow best practices in properly removing confidential data stored in computers before they are released for surplus or destruction, we make the following recommendations:

In addition to the actions the OCIO has already taken, we recommend 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 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

We also recommend the OCIO:

- 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

Our recommendations for 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 and Recreation Commission
   - State Senate
2. As a best practice, the following organizations 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 & Industries
   - Department of Natural Resources
   - Department of Revenue
   - Department of Social and Health Services
   - Department of Transportation
   - Office of the Insurance Commissioner
   - State Parks and Recreation Commission
   - State Senate

Introduction

In the 21st century, almost nothing ages as quickly as computer software and hardware. Improvements in processing speed and memory capacity make machines only a few years old obsolete, while innovative or upgraded software can sometimes run only on newer computers. Personal and business users can dispose of their old computers through recycling centers across the state, which process the scrap boxes and hard drives. Washington's state agencies, boards and commissions must meet stricter guidelines and proceed carefully when they decommission computers they no longer need.

In the last two years, state government organizations decommissioned almost 20,000 computers using the Department of Enterprise Services (DES) surplus program. Some are redistributed to other state agencies, school districts or non-profit organizations. The rest are sold to the public through the surplus program website or at the DES Surplus Store in Tumwater, WA. The revenue collected from the sale of these computers is used to fund the surplus program and to purchase new equipment for state organizations.

Before state organizations release computer equipment for disposal, state laws require them to safeguard confidential information such as Social Security numbers, personal medical information, and organization Information Technology (IT) system and security data. Leaving confidential data on computers can expose individuals and organizations to identity theft or fraud; it also violates state and federal law.

While DES runs the surplus store, the Office of the Chief Information Officer (OCIO) sets state IT security standards, including those for safeguarding confidential information.

State government organizations can choose to completely erase the information, leaving the computer hard drive intact, or remove the drive and destroy it. State standards require them to document their hard drive erasing and disposal procedures.

We 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?

Washington's data safeguarding requirements

1. State law RCW 19.215.020 "Destruction of information - Liability - Exception - Civil action"
2. State law RCW 42.56.420 "Security"
3. State law RCW 43.19.1919 "Surplus personal property - Sale, exchange - Exceptions and limitations"
4. Washington State Office of the Chief Information Officer Security Standard 141.10 - Section 8.3 "Media Handling and Disposal" pg. 22, which makes reference to best practices such as the federal National Institute of Standards and Technology (NIST) Special Publication 800-88 "Guidelines for Media Sanitation"

Audit Scope & Methodology

As we addressed the two primary audit questions, we developed additional objectives based on the results of our tests:

- If we found data on the hard drive of a surplused computer, we tried to find out how this happened. This included interviewing organization staff and examining the organization's hard drive erasing and disposal policies and procedures.
- If we found surplus computers without hard drives, we asked the organizations why it removed the drives and what was done with them.
- If an organization successfully disposed of computers with completely erased hard drives, we examined its data disposal policies and procedures to see how they compared to the Office of Chief Information Officer's (OCIO's) Security Standards and best practices.

Processes for examining computers sent to DES for surplus

We reviewed relevant laws and standards that classify confidential data and require its destruction prior to disposal. The (OCIO) Security Standards 141.10, page 8, section 4.1 Data Classification states:

> Agencies must classify data into categories based on the sensitivity of the data.
>
> Agency data classifications must translate to or include the following classification categories:
>
> 1. Category 1 – Public Information
>   Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.
> 2. Category 2 – Sensitive Information
>   Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.
> 3. Category 3 – Confidential Information
>   Confidential information is information that is specifically protected from disclosure by law. It may include but is not limited to:
>   a. Personal information about individuals, regardless of how that information is obtained.
>   b. Information concerning employee personnel records.
>   c. Information regarding IT infrastructure and security of computer and telecommunications systems.

We focused our audit on Category 3 – Confidential data. We created a statistical sample (specifically, a stratified random sample) of all surplus computers sent to the DES surplus program over a six-week period during the summer of 2013 to examine them for compliance.

Each week, the DES Warehouse Manager gave the audit team a list of the organizations due to send computers to surplus and their inventory count. We selected a sample of about 30 desktops or laptops and went to the DES Surplus Store to examine them. If the computer contained a hard drive, we brought it to our office for testing to see if the drive contained any confidential data. At the end of the six weeks, we had examined 177 of the 1,215 desktop and laptop computers sent to the surplus program. The sampled computers came from 13 different state organizations. For complete results of our sample, see **Appendix D**.

Understanding current best practices guided our evaluation of state organizations' disposal processes

In addition to familiarizing ourselves with the OCIO's Security Standards Section 8.3 "Media Handling and Disposal," we also reviewed the National Institute of Standards and Technology (NIST) 800-88 "Guidelines for Media Sanitation" which is referenced in Section 8.3 of the Standards as a media sanitation "best practice." See **Appendix B**, which lists this best practice resource that government organizations at the state and local level might find helpful as they review their policies and procedures. **Appendix C** provides a list of free software erasure tools that the OCIO recommends to state organizations. These tools could also help small or local government organizations maintain high standards of data security on decommissioned computers without adding high costs to the process.

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. See **Appendix A**, which addresses the I-900 areas covered in the audit.

Next steps

Our performance audits of state programs and services are reviewed by the Joint Legislative & Audit Review Committee (JLARC) and/or by other legislative committees whose members wish to consider findings and recommendations on specific topics. Representatives of the State Auditor's Office will review this audit with JLARC's Initiative 900 Subcommittee in Olympia. The public will have the opportunity to comment at this hearing. Please check the JLARC website for the exact date, time, and location (www.leg.wa.gov/JLARC). 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.

Audit results

We found data on computers from four different state organizations – the departments of Ecology, Health, Labor & Industries, and Social and Health Services – sent to the DES surplus warehouse in six separate shipments. Based on the stratified sampling method we used to select computers, we estimate 9 percent, or 109, of the 1,215 computers sent to the surplus program during our six-week review period contained confidential information.

We also found that state organizations employed a variety of policies and practices to ensure data did not remain on the computers placed in the DES surplus program. Of the 13 agencies that shipped computers we tested, only two – the departments of Enterprise Services and Employment Security – had policies and procedures that included a step to verify data was removed from computer hard drives, or that the hard drives were destroyed, as NIST recommends as a best practice. The Department of Revenue also had fully compliant policies and procedures, and a process to verify data was removed from their hard drives, but had not documented the verification step in its procedures.

In the case of the other 10 organizations' policies and procedures, we found some were incompletely documented and some did not conform to the OCIO's Security Standards, while some had documented and compliant policies, but staff did not fully follow them.

9%

We estimate that 9% of the state-owned computers sent to the DES surplus program during our test period contained confidential data.

Question 1: Do state organizations properly remove confidential data stored in their data processing equipment before releasing them for surplus or destruction?

Computers released as surplus contained confidential data that should have been erased

We estimate 9 percent of the computers sent to the surplus program during our review contained confidential data that state law required organizations to remove before releasing their computers for surplus.

The confidential data included:

- Social Security numbers
- Dates of birth
- Addresses
- Phone numbers
- Medical records
- Financial information
- Applications for public assistance
- IRS tax forms
- Employment applications
- Employee personnel evaluations
- Employee citizenship information
- IT security and system information

In addition to confidential information, one of these computer hard drives still had its operating system installed.

Another computer hard drive contained no confidential information, but did have dozens of inappropriate photos.

It appeared one state organization attempted to use software to erase the hard drives, but the erasure was not successful. The nature of un-erased data reflected to some degree the sensitive nature of state agencies' work. Computers from another organization contained several documents that fall in to the OCIO Security Standards Confidential Information Category 3.a, "Personal information" about individuals, such as applications for benefits, a medical history record, a psychiatric evaluation, IRS tax forms, and banking and credit information of the agency's clients.

We saw some types of confidential data recur more frequently during our tests, including employee performance evaluations and personnel information, user names and passwords, and network access instructions. We also found a computer loaded with a fully functional operating system, although it required a username and password to log on to the computer.

We also found computers that had their hard drives removed completely. The matter of absent hard drives is discussed below.

Reasons why data remained on drives varied between organizations, but human error played a part

For every computer we found that contained data, we sought reasons why it had been sent to the surplus warehouse before being completely erased. We interviewed IT managers or staff at the four agencies, and asked them to identify the combination of issues that led to the incomplete removal of confidential data. Agency staff supplied the following causes of incomplete processes, human error, and technological failures.

For example, agencies suggested:

- Computers that did not start were released for surplus on the assumption that they were actually broken and unusable, when the computer hard drives still contained confidential data.
- Computers were mistakenly set aside for surplus delivery before the data had been erased from their hard drives.
- Tape indicating the hard drive had been removed was mistakenly placed on a computer with its hard drive intact.
- Computers with installed hard drives planned for reuse were instead sent for surplus without data removal.

Why hard drives were absent

State organizations can either remove and destroy computer hard drives, or erase data on the hard drives and reuse them. According to the OCIO Security Standard, both approaches are an acceptable solution to safely disposing confidential data.

- In one agency, regional offices remove hard drives in order to destroy them, while some drives are removed to copy data stored on them. In the latter case, the hard drives are erased and sent to DES Surplus separately from the computers.
- One agency described removing hard drives to send them to a contractor for destruction. The process calls for a technician to place blue tape labeled "HD out" on decommissioned computers after the hard drive has been removed; the computers are then stacked on pallets until DES collects them to take to the surplus warehouse. The hard drives are placed in a locked bin and later destroyed.

Discrepancies were found between physical count and inventory lists at the DES warehouse

We found significant discrepancies between the number of desktops and laptops we physically counted at the DES warehouse and the number listed on the surplus program inventory sheet submitted by one agency. One of the shipments we sampled included 23 more desktops than inventoried, while the other shipment included 74 more desktops and eight fewer laptops. We were unable to determine how or why this happened.

Question 2: Do state organizations' computer disposal policies, procedures, and processes comply with state requirements and follow best practices?

Organizations did not always comply with the OCIO's requirements or employ best practices for disposing of computers

We wanted to know how well state organizations complied with the OCIO's data disposal standards, and whether those organizations with data-contaminated drives had met the requirements for documented policies and procedures. We also wanted to see how closely Washington's computer disposal policies and recommended procedures aligned with best practice as outlined by industry and government experts.

We compared the OCIO Standards Section 8.3 "Media Handling and Disposal" to the NIST 800-88 "Guidelines for Media Sanitation." We found that Section 8.3 of the Standards makes reference to "best practices such as NIST SP 800-88," and OCIO Standards Section 8.3.3 for state organizations to "ensure the safe and secure disposal of sensitive media." The standards do not, however, specifically require state organizations to employ NIST best practices, which include verifying data has been removed or the storage media has been destroyed.

The NIST best practices provide organizations:

- An overview of the need for data sanitization and the basic types of information, sanitization, and media
- A process flow, including validation and documentation steps, to assist with data sanitization decision making
- Guidance on how to verify the effectiveness of selected data sanitization processes, equipment and personnel competencies

Having a documented procedure does not guarantee completely erased computer hard drives

Of the four organizations with confidential data on their drives, three – Department of Ecology, Department of Health, and Department of Labor & Industries – met the state standards requirement to have documented procedures explaining how they remove data from surplus computers. The procedures and the processes described by the Department of Social and Health Services were not sufficient to ensure data was removed from computers. Furthermore, the procedures were inconsistent within the agency, in that some of its regional and field offices used software that erased and reformatted drives while other offices physically removed hard drives.

The very diverse explanations given by the four organizations for having confidential data on their surplused computers indicated a lack of controls. Furthermore, when mistakes were made, the organizations did not have mitigating controls documented and in use to prevent the release of confidential data.

None of the procedures or processes we reviewed for these organizations required computer hard drives to be checked after the data removal step was supposed to be completed, to confirm that hard drives were removed or completely erased before being sent to surplus. This is a necessary step to verify that confidential data is not released.

Even at organizations that did not have confidential data on their computers in our sample, policies and procedures did not always meet OCIO Standards

Some state organizations did not have documented computer disposal procedures as required by the OCIO Standards. Although we did not discover confidential data on the computers we checked for the State Senate and the State Parks and Recreations Commission, neither had documented computer hard drive erasing and/or disposal policies and procedures as required by the OCIO Standards.

The most frequently observed issue with state organizations' computer disposal policies or procedures was the lack of a documented step in their procedures to verify that data had been erased or hard drives destroyed as recommended by the NIST's guidelines for media handling and disposal best practices. Eleven of the 13 organizations we audited lacked such a step to verify and document data is properly deleted.

We could not determine if only four state organizations had confidential data on their computers

Our random sample included computers from only 13 state organizations. Although the computers we tested from nine organizations did not contain data, we cannot be sure that all their computers were free of data. Not all organizations were tested, either because none of their computers were selected in our sample or they did not send computers to surplus during our audit period. For this reason, we cannot determine if this problem is isolated to four organizations.

In addition, after discussions with the other nine organizations we audited, we found that these organizations were also at varying levels of proficiency in their surplus disposal process. A couple of these organizations did not have documented procedures. Several of them did not include a documented step in their procedure to verify that data was removed from hard drives.

We also learned that one organization that leases its computers returns them to leasing companies rather than sending them to surplus. We were not able to test any of these computers to determine if data was left on their hard drives. However, leaving confidential data on these computers is still a violation of state and federal laws, and state organizations should ensure that returned lease computers are free of data.

The state reacted swiftly to our audit findings

After we shared our audit test results with the state organizations and the OCIO, they reacted swiftly to address the problem. The OCIO immediately quarantined and halted the distribution and sale of surplus computers and plans to provide additional guidance to state organizations and also evaluate its end of life digital policies. Some organizations we identified as having confidential data on their computers are taking immediate steps to resolve the problems and are reviewing their procedures and processes:

1. The Department of Social and Health Services is considering options to standardize and centralize its data removal process and recognized that it could improve inventory control procedures to verify the number of computers as they move through the surplus process and to track hard drives that are removed.
2. The Department of Ecology has assigned an employee to examine every computer after it has been erased to ensure no data is left on the hard drive and is developing a new procedure with sufficient controls.
3. The Department of Labor & Industries recognized that its procedure was incomplete and staff did not have instructions for instances where they could not load the wiping software and is reassessing its process. The Department has revised its data removal processes, added a verification step to confirm completion, and will provide formal training to staff with these responsibilities.
4. The Department of Health acknowledged that its surplus process could be improved.

Chief Information Officer Michael Cockrill wrote in a letter to all agencies:

"The security risks arising from unintended exposure of state data are very real."

Recommendations

In order to ensure state organizations comply with state requirements and follow best practices in properly removing confidential data stored in computers before they are released for surplus or destruction, we make the following recommendations:

In addition to the actions the OCIO has already taken, we recommend 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 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

We also recommend the OCIO:

- 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

Our recommendations for 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 and 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 & Industries
   - Department of Natural Resources
   - Department of Revenue
   - Department of Social and Health Services
   - Department of Transportation
   - Office of the Insurance Commissioner
   - State Parks and Recreation Commission
   - State Senate

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

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.*

MIKE KREIDLER
STATE INSURANCE COMMISSIONER

STATE OF WASHINGTON

OFFICE OF
INSURANCE COMMISSIONER

Phone: (360) 725-7000
www.insurance.wa.gov

April 3, 2014

Chuck Pfeil, Director of Performance Audit
Washington State Auditor's Office
PO Box 40021
Olympia, WA 98504-0021

Dear Mr. Pfeil:

This letter serves as the Office of Insurance Commissioner's (OIC) formal written response to the Safe Data Disposal Performance Audit. The OIC appreciates the opportunity to review and respond to your recent performance audit on Safe Data Disposal.

I am pleased to see that the sample audit findings did not indicate the OIC had released surplus equipment containing confidential data. In addition, based on guidance from the state Office of the Chief Information Officer and industry trends, over the past year the OIC has adopted thin client technology for our user base. Through this effort, we have already removed the vast majority of OIC desktop computers, replacing them with thin client units. As such, we have very few personal computers on desktops, further mitigating any risk of an inadvertent release of confidential data.

The OIC will continue to surplus any remaining personal computers following our procedures, which comply with guidelines provided by the state Office of the CIO. Further, we will document our existing verification step, ensuring it is clear that we have removed data appropriately from the hard drives.

Sincerely,

James T. Odiorne, CPA, JD
Chief Deputy Insurance Commissioner

Mailing Address: P. O. Box 40255 • Olympia, WA 98504-0255
Street Address: 5000 Capitol Blvd. • Tumwater, WA 98501

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. General 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 section of this report.

I-900 element	Addressed in the audit
1. Identification of cost savings	**No.** The audit did not identify cost savings
2. Identification of services that can be reduced or eliminated	**No.** The audit did not address services that could be reduced or eliminated.
3. Identification of programs or services that can be transferred to the private sector	**No.** The audit did not assess whether sanitizing or destruction of hard drives could be transferred to the private sector.
4. Analysis of gaps or overlaps in programs or services and recommendations to correct gaps or overlaps	**Yes.** We performed fieldwork at agencies that we discovered protected data on their surplus PC and/or laptop hard drives during Objective 1 fieldwork. We discovered that the OCIO 141.10 Security Standard does not give enough direction to agencies on necessary procedures to ensure they meet the state's data disposal requirements.
5. Feasibility of pooling information technology systems within the department	**No.** The audit did not address pooling of information technology systems.
6. Analysis of the roles and functions of the department, and recommendations to change or eliminate departmental roles or functions	**Yes.** We analyzed how state organizations managed their surplus computer materials and recommended improvements to their data disposal processes.
7. Recommendations for statutory or regulatory changes that may be necessary for the department to properly carry out its functions	**Yes.** The audit report does recommendation that the OCIO 141.10 Standard be revised to give entities more clear direction on safeguarding data when sending hard drives to surplus.
8. Analysis of departmental performance, data performance measures, and self-assessment systems	**No.** The audit did not address the agency's performance measures and self-assessment systems.
9. Identification of best practices	**Yes.** The National Institute of Standards and Technology (NIST) Special Publication 800-88 - Guidelines for Media Sanitation.

Appendix B: OCIO Best Practice Guidance

On February 12, 2014, the State Chief Information Officer, Michael Cockrill, sent an email to the Chief Information Officers of our state organizations with the following message and information on media handling best practices.

> *"The Office of the CIO (OCIO) has been working with the Washington State Auditor regarding an in-progress audit that has exposed a need for us to refocus on how we handle the deletion of data from end-of-life PCs and electronic devices.*
>
> *To ensure state data does not fall into the wrong hands, we have a responsibility to guarantee that all state data is removed from PCs and other electronic devices before they are disposed. The security risks arising from unintended exposure of state data are very real. For this reason, I ask that you make the deletion of data from PCs and other electronic devices prior to disposal a priority in your agency.*
>
> *The requirements for securely deposing data from media can be found in Section 8.3 of the OCIO Security Standards. This section provides information on how media is to be sanitized and references guidelines to be used to ensure data is securely deleted.*
>
> *In addition to our existing standards, today I am announcing that the OCIO is now providing information on best practices for data disposal and locations where free tools can be found to satisfy the requirements. These can be found on the OCIO website in the document Media Handling and Data Disposal Best Practices.*
>
> *As the cyber security threat landscape continues to evolve, it is necessary to employ new, modern measures to protect our data assets from unauthorized exposure as well. During the next monthly CIO meeting, I will ask for volunteers from the CIO community to help us modernize our approach to deleting data from end-of-life devices, elevating hard drive destruction and recycling as a preferred option for agencies.*
>
> *Thank you in advance for bringing this important matter to the attention of your staff and your cooperation in making sure that sensitive state information remains secure."*
>
> *Michael Cockrill*
> *Chief Information Officer*

OCIO's Media Handling and Data Disposal Best Practices Information

The rest of this section is information the CIO included in the February 12, 2014 email to state organizations:

Agencies must establish formal, documented media disposal procedures. Documented procedures are critical, as they help ensure that effective processes are consistently applied, regardless of staffing changes or turnover.

While the OCIO IT Security Standards provide some latitude on how the requirements in Section 8.3, Media Handling and Disposal, can be met, there are many best practices that agencies can adopt to ensure they are protected from unauthorized access to agency data. In addition, agencies should be mindful of the data retention requirements for any data contained on storage media to be disposed.

Maintain secure control and custody of media to be disposed

- Media to be disposed must stay within the control of the agency from the time it is collected to the time it is sanitized.
- Pick-up/Transit – Storage media to be disposed should be collected by be in the constant possession of a dedicated, trusted personnel
- Media should be maintained in a secure, locked area until it can be sanitized

Render all data on the media unusable

When files are deleted from a computer, emptied from the Recycle Bin or even by reformatting, if it is not overwritten it can be easily recovered using commonly available tools.

- Don't delete the data– destroy it
- All data should be rendered unusable using special software designed for this purpose (See examples at bottom of page)
- Meets the requirements of Section 8.3 of the OCIO IT Security Standards

Physical destruction is an option

- Agencies may physically destroy the media itself rather than sanitize the media
- This typically takes the form of shredding or pulverization, ensuring the media can never be used again.
- Any media that cannot be sanitized through the use of software tools must be physically destroyed.

Private companies are available to perform this service, and agencies must be sure that they can maintain control of the media from the time it leaves the agency until the time it is actually destroyed. When pursuing this option, agencies should consider those companies that dispose or recycle these materials in an environmentally responsible way.

Keep Detailed Records

Agencies should maintain records that document all media disposal activities, as this can provide agencies with the means of confirming that specific media was disposed of properly if it is later called into question.

Records for disposed media should include:

- Information about the media (type, serial number, other unique identifiers)
- The date the media was sanitized
- The person performing the activity
- The method used to render all data unusable (e.g. software tool used or physical destruction of the media)
- The signature of the person responsible for ensuring that all data on the storage media has been rendered unusable.

Provide evidence of disposal

In addition to keeping records, it is a good idea to identify media that has been sanitized. This can include:

- Affixing a sticker or a document to the device or CPU indicating that the data sanitation process was completed. This helps agencies easily identify and segregate machines internally, and lets others, such as DES Surplus, know that the media has been wiped and can be made available for use by others.

The National Institute of Standards and Technology (NIST) 800-88 "Guidelines for Media Sanitation"

The OCIO Security Standards Section 8.3 references The National Institute of Standards and Technology (NIST) 800-88 "Guidelines for Media Sanitation" as a best practice which in Section 4, page 12 and Sections 4.7 and 4.8, page 15 (see excerpts below) recommends that processes used by organizations to remove confidential data should include a documented verification step to ensure confidential data and/or hard drives have been removed from computers before they are sent to surplus.

See also NIST website: http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf

NIST 800-88 - Section 4, Page 12:

Information Sanitation and Disposition Decision Making

Organizations can use Figure 4-1 with the descriptions in this section to assist them in making sanitization decisions that are commensurate with the security categorization of the confidentiality of information contained on their media. The decision process is based on the confidentiality of the information, not the type of media. Once organizations decide what type of sanitization is best for their individual case, then the media type will influence the technique used to achieve this sanitization goal.

Exhibit A: An example of data disposal decision flow from the NIST guidance

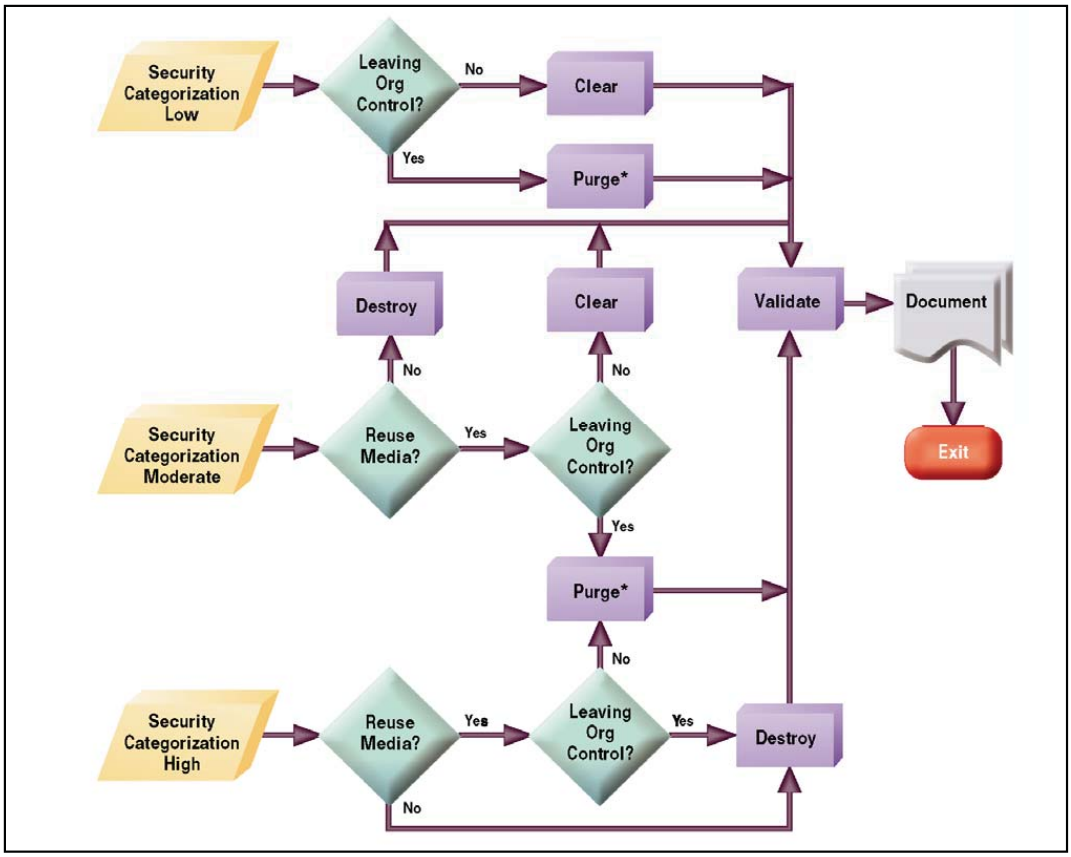


Figure 4-1. Sanitization and Disposition Decision Flow

NIST 800-88 - Sections 4.7 and 4.8, Page 15:

4.7 Verify Methods

Verifying the selected information sanitization and disposal process is an essential step in maintaining confidentiality. A representative sampling of media should be tested for proper sanitization to assure the organization that proper protection is maintained. Verification of the process should be conducted by personnel without a stake in any part of the process.

4.7.1 Verification of Equipment

Verification of the sanitization process is not the only assurance required by the organization. If the organization is using sanitization tools (e.g., a degausser), then equipment calibration, as well as equipment testing, and scheduled maintenance, is also required.

4.7.2 Verification of Personnel Competencies

Another key element is the potential training needs and current expertise of personnel conducting the sanitization. Organizations should ensure that equipment operators are competent to perform sanitization functions.

4.8 Documentation

It is critical that an organization maintain a record of its sanitization to document what media were sanitized, when, how they were sanitized, and the final disposition of the media. Often when an organization is suspected of losing control of its information, it is because of inadequate record keeping of media sanitization. Organizations should ensure that property management officials are included in documenting the media sanitization process in order to establish proper accountability of equipment and inventory control.

Organizations should conduct sensible documentation activities for media containing low security category information. These are generally considered a consumable or perishable item by property management.

Appendix C: Free Data Erasure Software

On February 12, 2014, the State Chief Information Officer, Michael Cockrill, gave state organizations the following list of free software utilities that can be used to meet the Office of the CIO's IT Security Standards data and media disposal requirements:

DBAN (Darik's Boot and Nuke) - http://www.dban.org/

- Data Sanitization Methods: DoD 5220.22-M, RCMP TSSIT OPS-II, Gutmann, Random Data, Write Zero

Eraser Portable - http://portableapps.com/apps/security/eraser-portable

- Data Sanitization Methods: DoD 5220.22-M, AFSSI-5020, AR 380-19, RCMP TSSIT OPS-II, HMG IS5, VSITR, GOST R 50739-95, Gutmann, Schneier, Random Data

Microsoft's SDelete - http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx

- Data Sanitization Methods: DoD 5220.22-M, Gutmann, Random Data

Freeraser - http://download.cnet.com/Freeraser/3000-2144_4-10909403.html

- Data Sanitization Methods: DoD 5220.22-M, Gutmann, Random Data

Appendix D: Statistical Sampling Results

During our six-week review period, 1,215 computers were sent to the state surplus program. We developed a stratified random sample to test about 30 computers during each week. Based on the data we reviewed, our estimate is that 109 of the 1,215 computers contained confidential data. See the table below for information on our weekly reviews during the sample period.

Stratified statistical sample results of computers sent to the surplus program

Time period	Computers sent for disposal	Computers in our sample	Computers with confidential data
Week 1	535	31	5
Week 2	253	29	1
Week 3	48	30	3
Week 4	100	27	1
Week 5	97	26	0
Week 6	182	34	1
Total	**1,215**	**177**	**11**

Source: State Auditor's Office analysis.

The table below shows our overall estimate for computers containing confidential data during our six week testing period, as well as the lower and upper limits.

Estimates of computers with confidential data during the sample period

	Percent of computers	Number of computers
Estimate	9%	109
Lower limit	3%	38
Upper limit	15%	180

Source: State Auditor's Office analysis based on a 90% confidence level.