Office of the Washington State Auditor
Pat McCarthy

Performance Audit

Safe Data Disposal: State Reduces the Risk of Disclosing Confidential Information

December 17, 2018

Report Number: 1022845

Table of Contents

State Auditor's Office contacts

State Auditor Pat McCarthy
360-902-0360, Pat.McCarthy@sao.wa.gov

Scott Frank – Director of Performance Audit
360-902-0376, Scott.Frank@sao.wa.gov

Shauna Good – Principal Performance Auditor
360-725-5615, Shauna.Good@sao.wa.gov

Patrick Anderson – Lead Performance Auditor
360-725-5634, Patrick.Anderson@sao.wa.gov

Rhianna Hruska – Performance Auditor
360-725-5361, Rhianna.Hruska@sao.wa.gov

Kathleen Cooper – Director of Communications
360-902-0470, Kathleen.Cooper@sao.wa.gov

To request public records

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

Executive Summary

Background

State agencies regularly send thousands of items to the state's surplus warehouse, where the Department of Enterprise Services (DES) helps agencies dispose of equipment they no longer need. When agencies dispose of IT equipment, they are responsible for ensuring it does not contain any confidential information.

In 2014, the Office of the Washington State Auditor conducted a performance audit to determine whether agencies were removing data from their computers in accordance with state law and the Office of the Chief Information Officer (OCIO) requirements. This follow-up audit addresses whether the state has improved controls designed to ensure agencies do not disclose confidential information through surplus. It includes agencies where auditors found issues in the 2014 audit and a selection of agencies that surplused equipment during the spring of 2018.

Does the state have adequate controls in place to ensure that the surplus of state-owned IT devices does not disclose confidential data?

We found confidential information on fewer than 1 percent of the computers and IT devices tested, indicating improvements since 2014. One difference that likely contributed to this improvement is that more agencies now remove and physically destroy computer hard drives before surplusing the machines.

While most agencies had written policies for disposing of IT equipment, most did not fully incorporate state requirements and best practices. Gaps in agency policies included not verifying data disposal, not keeping records of disposed equipment and not including guidance for other IT devices.

The state's Computers 4 Kids (C4K) program, which allows state agencies to donate surplus computers and computer-related equipment to public schools, serves as a safety net for the disposal of some IT devices. Before DES sends surplus computers to schools, it sends them to the C4K program where they are wiped again and refurbished. However, it is the responsibility of individual agencies to ensure confidential information is not disclosed.

State Auditor's Conclusions

Agencies have improved their practices and reduced the risk of disclosing confidential information, and they should remain diligent in reviewing and updating their data-disposal policies. The audit identified very few instances of confidential data on devices, and those instances illustrate the importance of strong policies and procedures that align with state requirements and best practices.

Technology changes quickly, and new risks emerge. As agencies increasingly use laptop computers and tablets rather than desktop computers, they must adapt their policies and procedures to address risks specific to mobile technology.

Emphasizing safe data disposal practices and revising those practices to keep up with the evolving environment will help state and local government agencies avoid the significant consequences of improperly disclosing confidential data.

Recommendations

We made recommendations to the agencies to address specific areas where their policies and procedures did not align with state requirements and best practices. We also made general recommendations to all state agencies to annually review and update their disposal policies.

Next steps

Our performance audits of state programs and services are reviewed by the Joint Legislative Audit and 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. See **Appendix A**, which addresses the I-900 areas covered in the audit. **Appendix B** contains information about our methodology.

Background

The Department of Enterprise Services (DES) operates a surplus program to help agencies dispose of items they no longer need, including IT equipment

As agencies update and replace their equipment, they are left with thousands of items they can no longer use. The DES surplus program recycles, reuses or sells a large variety of materials on behalf of state and local government agencies. DES reports these efforts keep more than 600,000 pounds of waste out of landfills each year. Surplus items include computers and other IT devices such as printers, copiers, tablets and cellphones. DES makes much of this equipment available to the public for purchase through its surplus store and website.

When agencies dispose of surplus IT equipment, they are responsible for ensuring it does not contain any confidential information

State laws and the Office of the Chief Information Officer (OCIO) oblige agency officials to remove or destroy all data including confidential information, such as Social Security and driver's license numbers, personal medical information and addresses, before releasing IT equipment for surplus. Releasing such information could expose people to identity theft, result in legal and regulatory violations for the state, and erode the public's trust in government.

To comply with their obligations, agencies need strong controls to ensure they remove confidential data from computers and other IT devices before making them available to the public. State agencies may choose to erase the information, or to remove the drive and destroy it. OCIO Security Standard 141.10, "Securing Information Technology Assets," also requires agencies to document their procedures. The National Institute of Standards and Technology (NIST), a leading authority on IT security standards, includes mention of documentation in its publications regarding best practices in safe data disposal.

This audit examined the effectiveness of the state's controls designed to ensure confidential information is not disclosed through the state's surplus process

In 2014, our Office conducted a similar performance audit, examining state agencies' practices for disposing of surplus computers. In that audit we found confidential data on an estimated 9 percent of the computers sent to the DES surplus warehouse. At that time, only three of 13 agencies we reviewed had policies and procedures that included a step to verify they had destroyed or removed all data from computer hard drives. The audit also found that policies and procedures had not been documented or staff were not fully following them.

This performance audit follows up on the results of the 2014 audit. It was designed to determine if agencies are removing confidential data from state surplus computers, and if they have implemented the recommendations made in the earlier audit. It also broadened the scope to include other IT devices, such as cellphones and tablets. Specifically, the audit answers the following question:

Does the state have adequate controls in place to ensure that the surplus of state-owned IT devices does not disclose confidential data?

Audit Results

Does the state have adequate controls in place to ensure that the surplus of state-owned IT devices does not disclose confidential data?

Answer in brief

Overall, we found confidential information on fewer than 1 percent of the devices tested, indicating improvements have been made since 2014. One difference that likely contributed to this improvement is that more agencies now remove and physically destroy computer hard drives before surplus. While most agencies had written policies for disposing of IT equipment, they did not fully incorporate state requirements and best practices.

The state's Computers 4 Kids (C4K) program, which allows state agencies to donate surplus computers and computer-related equipment to public schools, serves as a safety net for the disposal of some IT devices. Before DES sends surplus computers to schools, it sends them to the C4K program where they are wiped again and refurbished. However, agencies are still responsible for ensuring they do not disclose confidential information.

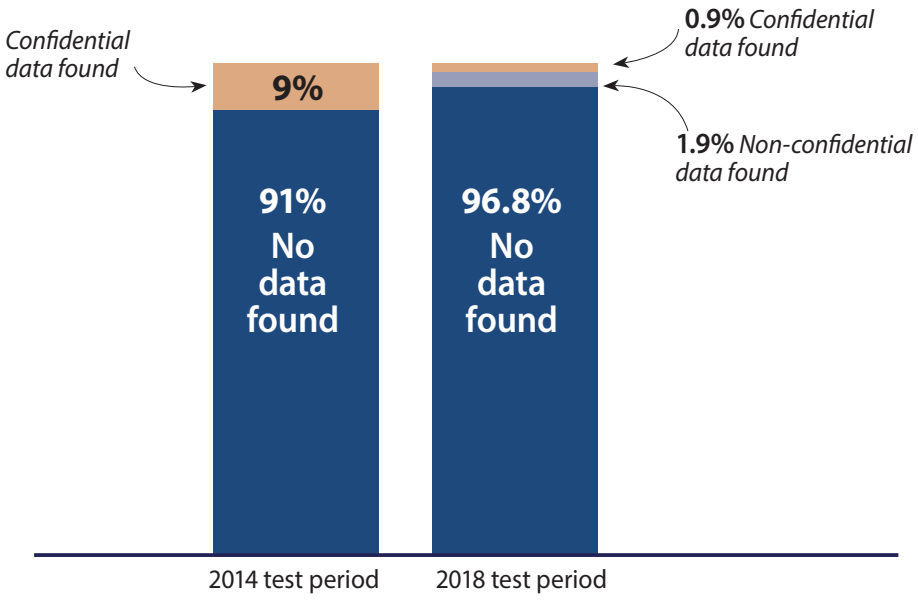
We found confidential information on fewer than 1 percent of the devices tested, indicating improvements since 2014

For five weeks, beginning in May 2018, DES gave us a weekly inventory of the electronic devices agencies intended to send to the state surplus center. We randomly selected items from these inventory lists, inspecting each device for removable storage hardware like a computer hard drive. Any hard drive or other storage device discovered was digitally inspected using Microsoft Windows File Explorer and Forensic Toolkit. For devices with storage that could not be removed, we checked to see if the device was factory reset.

We tested 317 computers (176 desktops and 141 laptops) sent to the state surplus center during our five-week testing period. We also tested 154 other IT devices that capture and store data (77 tablets, 40 printers, 25 cellphones, and 12 copiers). The results of this analysis can be projected to the total number of devices surplused during the five-week testing period.

We identified confidential information on fewer than 1 percent (three devices) of the computers in our sample (**Exhibit 1**). This is a significant improvement over the 2014 audit results, in which auditors estimated 9 percent of the computers sent to the surplus center contained confidential information.

Exhibit 1 – Confidential data found on state surplus computers decreased from 2014

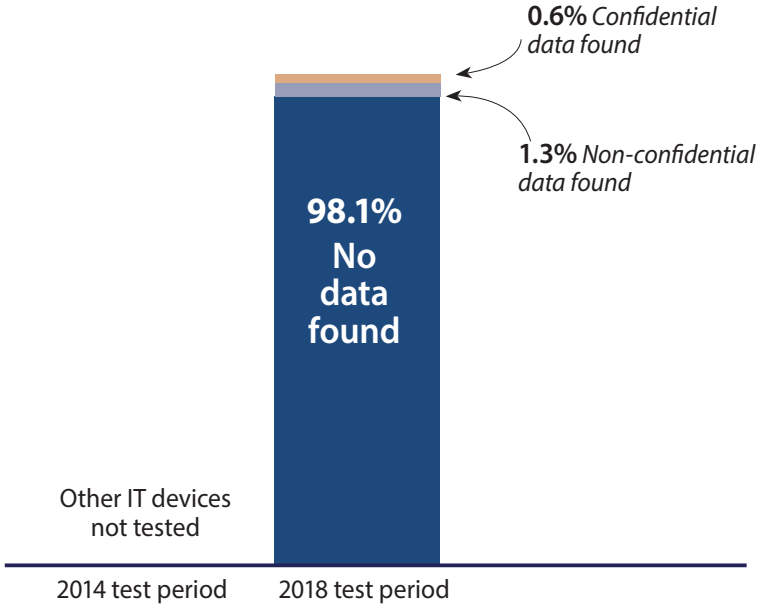


Note: In 2014, auditors did not test for non-confidential data on surplus computers. During the 2018 testing period, one device (0.3%) could not be tested due to physical defect.

The results were similar for the other, non-computer IT devices. We also found confidential information on fewer than 1 percent (one device) of these devices (**Exhibit 2**). Although these types of devices were not tested as part of the 2014 audit, it is likely – given how little we found – that agencies have improved their surplus and disposal practices for these devices as well.

It is important to note the 2018 audit found some non-confidential data files on several devices (shown in exhibits 1 and 2). While these files do not strictly speaking pose a security issue, their presence indicates potential gaps in agency surplus and disposal policies and procedures. All data, confidential or otherwise, should be erased to meet OCIO requirements.

Exhibit 2 – Results from other surplused IT devices

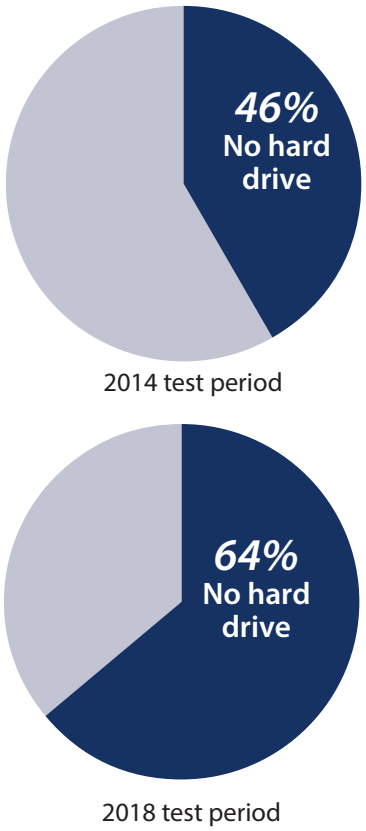


Compared to 2014, more agencies remove and physically destroy computer hard drives before surplus

According to OCIO Security Standard 141.10, state agencies may either remove and destroy computer hard drives, or erase the data drives contain. During this audit, DES officials stated the number of agencies sending computers with hard drives to surplus has decreased since our initial audit in 2014. This aligns with what we observed while testing the devices. As shown in **Exhibit 3**, 64 percent of computers tested had their hard drives removed. This is an increase from 2014, when the first audit found 46 percent of sampled computers did not contain a hard drive. This shift in approach likely contributed to the improvement in audit testing results.

Since the 2014 audit, some agencies have modified their surplus and disposal practices to mitigate the risk of releasing confidential information. One agency, for example, erased hard drives using software before the 2014 audit. Now, the agency physically removes the hard drives and arranges for a state-approved contracted vendor to shred them. Similarly, another agency mitigates its risk of disclosing confidential information by removing hard drives, degaussing (which means neutralizing them with magnets), and placing them in a secure bin where they are later shredded by a state-approved vendor.

Exhibit 3 – Percent of computers with hard drives has dropped



While most agencies had written policies for disposing of IT equipment, most did not fully incorporate state requirements and best practices

State law and OCIO standards require, and National Institute of Standards and Technology (NIST) best practices encourage, agencies to have surplus and data destruction policies and procedures. While it is possible that agencies are complying with OCIO requirements and state laws as well as following best practices in their surplus process, the lack of complete documented policies and procedures means agencies cannot demonstrate compliance with state requirements. They are also likely to be at greater risk of disclosing information.

To reduce risk, agencies need documented and comprehensive data disposal policies and procedures that include these elements: prescribing the removal of all data, maintaining a record of cleared devices, and training staff to verify that the devices have been properly sanitized or destroyed. State law requires the first two of these elements; OCIO and NIST guide agencies to include all three in their policies and procedures.

Nearly all agencies we evaluated had written data disposal policies

We requested written data disposal policies from all 28 agencies included in the audit. All but two of the agencies had documented safe data disposal policies. One reason these two agencies did not have written policies was they were unaware of the requirements, though one agency had informal procedures pertaining to data surplus and disposal.

Overall, compliance with written policy requirements improved since the 2014 safe data disposal audit, which found that nine of 13 state agencies reviewed had documented procedures. All 13 of those agencies now have policies and procedures in place.

However, few agencies had data disposal policies that fully complied with state requirements and incorporated best practices

Although more of the reviewed agencies now have safe data policies and procedures, some were more comprehensive than others. For example, one agency had only a few lines in its IT policy addressing safe data disposal, while another devoted 50 pages to the subject.

Auditors conducted an in-depth review of policies and procedures at a sample of 20 agencies. This sample included agencies that left data on surplus computers during at least one of the 2014 and 2018 audits and agencies where auditors identified other issues in the 2014 audit. The review looked for specific language in the policies and procedures that directly addressed state law, OCIO requirements or NIST best practices. Only four of the agencies had policies and procedures that fully complied with state law and OCIO requirements. These agencies also fully incorporated best practices.

Gaps in agency policies included not verifying data disposal, not keeping records of disposed equipment, and not including guidance addressing other IT devices

Some agencies' policies did not direct staff to verify the data has been erased or destroyed, which the OCIO requires before releasing equipment. In the 2014 audit, just three of the 13 agencies (33 percent) included a step in their policies and procedures to verify that data had been erased or destroyed. Fifteen of the 20 agencies (75 percent) in the 2018 audit included such a verification step. Though more agencies are verifying that data has been properly disposed of, and the audit found very few instances of data left on devices, auditors did find four instances of confidential information left on devices. This could have been prevented by an effective verification process. In one of those instances, a computer's hard drive was not removed and was mistakenly sent through the surplus process; a reviewer could have prevented this.

Ten of the 20 agencies (50 percent) did not include training for staff on how to dispose of IT equipment in their policies and procedures. Proper training could help ensure that steps in the verification process are completed correctly.

An agency degaussing hard drives before placing them in a secure shred bin.

A few agencies did not maintain records to document their properly disposed of IT equipment. State law, OCIO requirements, and NIST best practices all direct agencies to document the property they dispose of. Many agencies keep records and are in compliance. Of those that do keep records, many use contractors that provide a certificate of destruction as a record that the devices were destroyed. However, four agencies do not retain a record of disposed surplus property and cannot guarantee the devices were destroyed. Maintaining accurate surplus and disposal records helps to establish accountability, and can even help protect agencies from legal and financial penalties if confidential information were to be disclosed.

Four agencies do not have clear policies on how to dispose of other IT devices. Sufficient guidance around IT devices other than computers includes information about who is responsible for disposing of the cellphones, tablets, copiers or printers, as well as how to remove or destroy data on each of those devices. Agencies that do not include data disposal for other IT devices in their policies and procedures may not properly erase or destroy these devices. Policies for 10 of the agencies reviewed do not specifically reference cellphones, and 16 do not directly address the surplus and destruction of tablets. Six agencies have policies that refer to IT devices other than computers, but do not provide specific directions for how to properly surplus and dispose of these devices. These gaps in policies increase the risk of inappropriate disclosure.

A factory reset being performed on a phone containing confidential information from an agency.

For example, auditors identified confidential information on an agency cellphone that was not password protected or factory reset. Performing a factory data reset is critical to ensuring all data is removed from cellphones. The confidential data was the employee's personal medical information; it was left on the phone in part because the agency lacks policies and procedures for how to dispose of cellphones. Agency policies include information on how to factory reset an Android phone or iPhone; however, the policies are unclear about which employee is responsible for resetting the cellphone, as well as what happens to the phone after the reset process is complete. Because of this lack of clarity and verification, the cellphone was placed in a cabinet and ultimately sent to surplus without being factory reset.

State agencies must ensure that data is not disclosed from their IT devices during the surplus process. Following data destruction policies and procedures helps to prevent confidential information from entering the public domain and thus protects people from identity theft and significant monetary losses.

Although the state's Computers 4 Kids (C4K) program serves as a safety net for the disposal of some IT devices, agencies are still responsible for ensuring they do not disclose confidential information

The state's security policies require DES to send all surplus computers to the C4K program for disposal

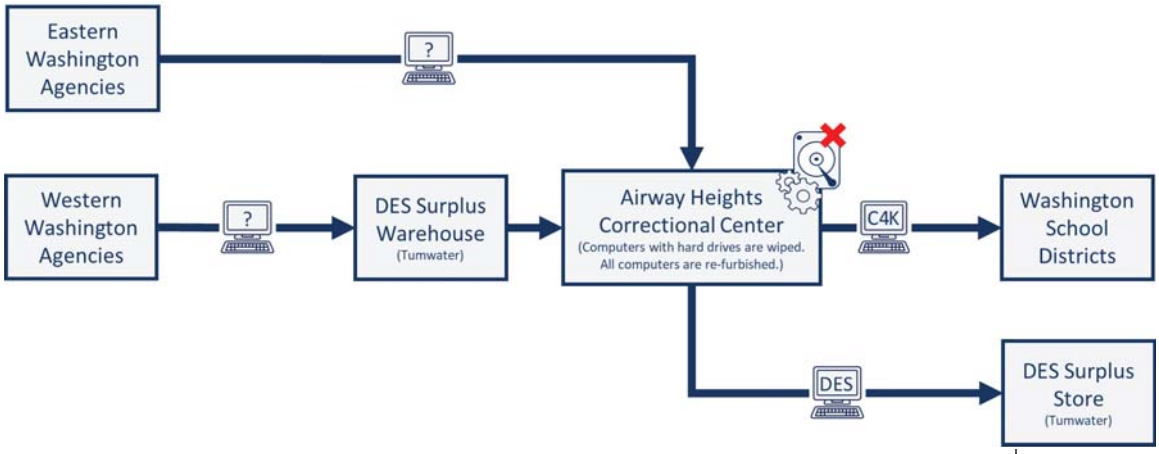
In response to our 2014 audit, the OCIO instructed DES to send all state-owned computers to Washington's Computers 4 Kids (C4K) program as a way to ensure these devices are cleared of all data before they are sent to schools. The C4K program makes it possible for state agencies to donate state-owned surplus computers and computer-related equipment to any public school district or educational service district in Washington so long as the computers meet minimum configuration standards. DES partners with the Office of Superintendent of Public Instruction (OSPI) and the Department of Corrections to administer the program.

Although agencies are responsible for ensuring no data remains on computers before sending them to DES, this process provides additional assurance that state-owned computers are clear before release.

DES sends all state-owned computers to C4K at the Airway Heights Corrections Center, where a Corrections employee wipes all hard drives before incarcerated individuals are given the computers to refurbish. Auditors visited the Corrections Center and observed the wiping and refurbishment processes. The hard drives are always under the control of Corrections staff or are securely locked. DES sells the remaining computers that do not meet C4K specifications to the public through the surplus program website or at its Surplus Store in Tumwater. **Exhibit 4** illustrates this process, starting at an agency and ending with donation or sale of the device.

Hard drives being erased at the Airway Heights Corrections Center as part of the Computers 4 Kids program.

Exhibit 4 – Department of Corrections erases data from state-owned computers at Airway Heights Corrections Center before sending them to schools or releasing them back to DES for sale



Although the C4K program helps ensure surplus computers do not contain confidential information, state agencies are ultimately responsible

Despite the added layer of protection provided by the C4K program, agency action is still important, because DES officials noted that not all government IT equipment is sent through the program. The C4K program primarily refurbishes computers. The program only recently started to refurbish tablet devices because of the increasing demand from public schools. The program does not refurbish copiers or cellphones.

Further, DES-leased equipment may bypass the Airway Heights data-wipe process. The DES Technology Leasing Program helps state agencies and other public institutions afford large purchases of IT equipment. The DES Master Lease Agreement is written in such a way as to give agencies options for surplusing IT equipment. Specifically, section 9.1 states:

> "Upon expiration or termination of this Lease, Lessee, at its own risk and expense, shall… prepare equipment for pickup by Computers for Kids (C4K) ***school districts or schools***..." [emphasis added]

As a result, IT equipment can bypass the safety net offered by the Airway Heights additional processing. This scenario serves as a reminder that agencies must not rely on others to erase data on surplus devices. While the C4K program serves as a safety net for the state, it does not absolve agencies and other public institutions of their responsibility to ensure that IT devices are properly erased before leaving their custody.

State Auditor's Conclusions

Agencies have improved their practices and reduced the risk of disclosing confidential information, and they should remain diligent in reviewing and updating their data-disposal policies. The audit identified very few instances of confidential data on devices, and those instances illustrate the importance of strong policies and procedures that align with state requirements and best practices.

Technology changes quickly, and new risks emerge. As agencies increasingly use laptop computers and tablets rather than desktop computers, they must adapt their policies and procedures to address risks specific to mobile technology.

Emphasizing safe data disposal practices and updating those practices to keep up with the evolving environment will help state and local government agencies avoid the significant consequences of improperly disclosing confidential data.

Recommendations

To the state agencies included in the audit

Due to security concerns associated with identifying vulnerabilities at specific agencies, confidential management letters were sent to each of the 20 agencies that had their policies and procedures reviewed. These letters contained detailed information about how to better comply with state laws related to data disposal, as well as OCIO requirements and NIST best practices. We recommend these agencies review and address the issues described in those letters.

Guidance for all Washington state agencies

We consider the audit results so broadly applicable that it is in the state's best interest for every state agency to undertake the actions communicated to the few that participated directly in the audit. We therefore suggest all Washington state agencies consider the practices listed below as they process surplused IT equipment in the future.

1. Annually review policies and procedures, and revise them as necessary to ensure they include the following state requirements and NIST best practices:
    - Designating management responsibility for the disposal of IT devices
    - Maintaining records of disposed equipment
    - Documenting the date equipment was sanitized, the method used, and the name and signature of the person responsible
    - Keeping disposal records secure from unauthorized access
    - Sanitizing equipment using a method consistent with NIST guidelines
    - Verifying equipment is fully sanitized
    - Keeping equipment secure before and during sanitization
    - Physically destroying storage media if sanitization tools fail
2. Update policies and procedures to include state-approved methods for erasing data from mobile devices such as cellphones and tablets.

Agency Response

Auditor's Note:

We gave copies of the final report to agencies governed by separately elected officials or the judicial branch for their review. Some of these agencies have decided not to provide a formal written response. They told us they generally agree with the report's findings and conclusions, and indicated they have begun to address the gaps found in their policies and procedures.

STATE OF WASHINGTON

December 13, 2018

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

Dear Auditor McCarthy:

Thank you for the opportunity to review and respond to the State Auditor's Office performance audit report, "Safe Data Disposal: State Reduces the Risk of Disclosing Confidential Information." The Office of Financial Management and Office of the Chief Information Officer worked with the audited agencies to provide a consolidated response. Agencies governed by a separately elected official or the judicial branch will respond separately.

We appreciate the report confirming that agencies have improved and reduced the risk of disclosing confidential information since the first performance audit in 2014. Your team found confidential information on less than 1 percent of the devices tested. It is great news to know we are moving in the right direction.

We also appreciate the report pointing out the gaps in most of the audited agencies' policies so we can further improve. Based on that information, some audited agencies have already begun to address those gaps. Every organization and person in state government shares responsibility in securing information and protecting confidential data.

Please thank your team for its work on this performance audit. As technology continuously evolves, we all need to be diligent and adjust as new risks emerge.

Sincerely,

James A. Weaver
Chief Information Officer
Washington Technology Solutions

David Schumacher
Director
Office of Financial Management

cc: David Postman, Chief of Staff, Office of the Governor
Kelly Wicker, Deputy Chief of Staff, Office of the Governor
Drew Shirk, Executive Director of Legislative Affairs
Pat Lashway, Deputy Director, Office of Financial Management
Scott Merriman, Legislative Liaison, Office of Financial Management
Keith Phillips, Director of Policy, Office of the Governor
Inger Brinck, Director, Results Washington, Office of the Governor
Tammy Firkins, Performance Audit Liaison, Results Washington, Office of the Governor
John Cooper, Senior Performance Project Manager, Results Washington, Office of the Governor
Scott Bream, Chief Information Security Officer, Washington Technology Solutions
Scott Frank, Director of Performance Audit, Office of the Washington State Auditor

Washington State Senate

312A Legislative Building
PO Box 40482
Olympia, WA 98504-0482

Brad Hendrickson
Secretary of the Senate

Phone: (360) 786-7550
E-mail: Brad.Hendrickson@leg.wa.gov

November 29, 2018

Mr. Scott Frank
Director of Performance Audit and IT audit
Office of the Washington State Auditor
302 Sid Snyder Avenue SW
Olympia, WA 98504-0021

Dear Mr. Scott:

Thank you for your recent letter regarding the State Auditor's Safe Data Disposal Performance Audit. The handling, storage and destruction of confidential data are of the utmost concern to the Washington State Senate.

The Senate works closely with legislative IT staff to ensure that data security controls and processes are designed appropriately and are operating effectively. We continue to evaluate our data security environments and controls to continually improve and assess risk to confidential data. We agree with the Safe Data Disposal Audit report, as written and conducted by the Office of the Washington State Auditor. I am pleased to learn that Senate policies and procedures aligned with all requirements and best practices.

Please take a few moments to update the Senate contact information. I replaced Hunter Goodman as Secretary of the Senate on December 1, 2017, and Hunter has not been employed by the Senate since November 2017.

I sincerely appreciate the State Auditor's Office work on this important matter.

Sincerely,

Brad Hendrickson
Secretary of the Senate

Appendix A: Initiative 900 and Auditing Standards

Initiative 900 requirements

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. Government 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. Identify cost savings	**No.** The audit focused on agency controls to protect sensitive data and did not identify cost savings.
2. Identify services that can be reduced or eliminated	**No.** Protecting sensitive data from inappropriate disclosure is the state's responsibility and is not a service that should be reduced or eliminated.
3. Identify programs or services that can be transferred to the private sector	**No.** Protecting sensitive data from disclosure is the state's responsibility, and the erasure or destruction of data-processing equipment should not be trans-ferred to the private sector.
4. Analyze gaps or overlaps in programs or services and provide recommendations to correct them	**Yes.** The audit sought to identify gaps in agency data disposal policies and procedures.
5. Assess feasibility of pooling information technology systems within the department	**No.** The audit focused on computer processing equipment that can be surplused, not information technology systems.
6. Analyze departmental roles and functions, and provide recommendations to change or eliminate them	**Yes.** The audit analyzed how state agencies manage their surplus data processing equipment and recommended improvements to their data disposal processes.
7. Provide recommendations for statutory or regulatory changes that may be necessary for the department to properly carry out its functions	**No.** The audit did not recommend statutory or regulatory changes.
8. Analyze departmental performance data, performance measures and self-assessment systems	**No.** The audit focused on agency controls to protect sensitive data and did not address the agency's performance measures or self-assessment systems.
9. Identify relevant best practices	**Yes.** The audit compared agency practices to national data security best practices.

Compliance with generally accepted government auditing 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 as published in 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.

Appendix B: Scope, Objectives and Methodology

Scope

This audit reviewed surplused computers, printers, copiers, tablets and cellphones from state agencies during May and June 2018. Overall, 26 different state agencies submitted IT devices that were examined. The audit also sought to review the current (July 2018) policies and procedures from agencies identified in an initial safe data disposal performance audit conducted in 2014. As a result, this audit reviewed 28 total agencies.

Objectives

This performance audit was designed to determine if agencies removed confidential data from state surplus computers and to determine if agencies have implemented the recommendations from the 2014 audit.

Methodology

Does the state have adequate controls in place to ensure that the surplus of state-owned IT devices does not disclose confidential data?

To address our audit objective, we reviewed relevant laws and standards that classify confidential data and require its destruction before disposal. The Office of the Chief Information Officer (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:

Category 1 – 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.

Category 2 – 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.

Category 3 – 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.

Category 4 – Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which: 1) especially strict handling requirements are dictated, such as by statutes, regulations, or agreements; and 2) serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions."

This audit focused on information designated as category three or higher.

Testing devices

To perform this audit, auditors requested historical records of surplus shipments for the testing period from the Department of Enterprise Services (DES) for all surplus electronics (computers, copiers, printers, tablets and cellphones) from state agencies for the past three years. Auditors calculated the weekly averages for each surplus device received by DES to determine a minimum weekly sample size (**Figure 1**). Because DES did not have historical data for tablets, auditors used the maximum sample size of 32 as a threshold for sampling these devices each week.

Figure 1 – Minimum weekly sample sizes

Device type	Minimum sample
Desktops	32
Laptops	26
Printers	22
Cellphones	12
Copiers	2
Tablets	32

During the audit's five-week testing period, DES surplus officials gave the audit team lists of the organizations scheduled to send surplus electronics and their inventory counts. Using Microsoft Excel, the team generated random numbers for each device category to establish a minimum total number of devices the team intended to test for that week. For any of the device categories, if the random sample was fewer than the minimum weekly sample identified below, auditors tested all of the devices.

During testing, auditors selected computers and other devices based on their random number assignments. If the device contained a hard drive, auditors brought it to our office for testing to see if the drive contained any confidential data. At the end of the five-week testing period, auditors had examined 471 of the 3,242 desktops, laptops, copy machines, printers, tablets and cellphones sent to the state surplus warehouse (**Figure 2**). The devices came from 24 different state organizations.

Figure 2 – Testing results for IT devices sent to the state surplus warehouse

	Desktops	Laptops	Phones	Tablets	Printers	Copiers	Total
Week 1	299	98	0	120	0	0	517
Week 2	253	84	163	0	24	0	524
Week 3	270	221	14	310	60	4	879
Week 4	335	68	20	0	17	2	442
Week 5	556	295	0	0	29	0	880
Total	**1,713**	**766**	**197**	**430**	**130**	**6**	**3,242**

Agency policy review

Auditors requested the data disposal policies and procedures of all 28 agencies included in this audit and conducted an in-depth policy review on 20 agencies (**Figures 3a** and **3b**) that met at least one of the following criteria:

- Left confidential information on surplused equipment during the 2014 audit
- Did not fully meet data disposal requirements or best practices during the 2014 audit
- Left any data on surplused equipment during the 2018 audit

Figure 3a – Agencies included in policy review

Consolidated Technology Services	Department of Veterans Affairs
Department of Agriculture	Office of Superintendent of Public Instruction
Department of Ecology	Office of the Insurance Commissioner
Department of Fish and Wildlife	State Parks and Recreation Commission
Department of Health	State Senate
Department of Labor and Industries	Tacoma Community College
Department of Licensing	The Evergreen State College
Department of Natural Resources	Washington State Patrol
Department of Social and Health Services	Washington Student Achievement Council
Department of Transportation	Yakima Valley College

Figure 3b – Agencies included in audit, but not policy review

Arts Commission	Department of Enterprise Services
Criminal Justice Training Commission	Department of Revenue
Department of Children, Youth, & Families	Office of Administrative Hearings
Department of Corrections	Treasurer's Office

Auditors reviewed agency policies and procedures for data disposal requirements using the following safe data disposal requirements:

State laws

- Agencies must take reasonable steps to destroy confidential information
- Agencies must maintain a record of disposed surplus property

OCIO 141.10 requirements and leading practices described by the National Institute of Standards and Technology

- Agencies must render all data on IT devices unusable before sending those devices to the DES surplus warehouse
- Agencies must maintain an inventory of major IT devices
- Agencies must verify that media is fully sanitized
  - Agencies need to keep records that describe the methods used to sanitize the data
- Agencies must record information about the media being sanitized
  - Date the media was sanitized
  - Who sanitized the media
  - Signature of the person responsible for ensuring the media is unusable

Appendix C: Helpful Safe Data Disposal Resources

This section lists data disposal resources that government organizations at the state and local levels might find helpful as they review their policies and procedures. Our evaluation of state organizations' disposal processes were guided by these requirements and best practices. We reviewed the OCIO's Security Standards Section 8.3, "Media Handling and Disposal," as well as the National Institute of Standards and Technology (NIST) 800-88 "Guidelines for Media Sanitation," which is referenced in Section 8.3 of the OCIO Security Standards as a media sanitation "best practice." State laws related to safe data disposal are also listed below.

Resources

OCIO 141.10: Securing Information Technology Assets Standards

141.10 details the appropriate measures that agencies can take to ensure the security of IT assets. Particularly relevant sections include 8.2 "Asset Management" and 8.3 "Media Handling and Disposal."

https://ocio.wa.gov/policy/securing-information-technology-assets-standards

United States Department of Commerce: National Institute of Standards and Technology (NIST)

NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization

This publication "provides guidance to assist organizations and system owners in making practical sanitization decisions based on the categorization of confidentiality of their information."

https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization

Washington laws related to safe data disposal

RCW 19.215.020 – *Destruction of information – Liability – Exception – Civil action.*

http://apps.leg.wa.gov/RCW/default.aspx?cite=19.215.020

RCW 42.56.420 – *Security.*

http://app.leg.wa.gov/rcw/default.aspx?cite=42.56.420

RCW 42.56.590 – *Personal information – Notice of security breaches.*

http://apps.leg.wa.gov/RCW/default.aspx?cite=42.56.590

RCW 43.19.1919 – *Surplus personal property – Sale, exchange – Exceptions and limitations – Transferring ownership of department-owned vessel.*

http://apps.leg.wa.gov/rcw/default.aspx?cite=43.19.1919