PERFORMANCE AUDIT

Office of the
Washington
State Auditor
Pat McCarthy

Safe Data Disposal at a College

March 11, 2025

Report Number: 1036771

Table of Contents

State Auditor’s Office contacts

State Auditor Pat McCarthy
564-999-0801, Pat.McCarthy@sao.wa.gov

Scott Frank – Director of Performance and IT Audit
564-999-0809, Scott.Frank@sao.wa.gov

Justin Stowe – Assistant Director for Performance Audit
564-201-2970, Justin.Stowe@sao.wa.gov

Olha Bilobran – Audit Lead
564-999-0025, Olha.Bilobran@sao.wa.gov

Kathleen Cooper – Director of Communications
564-999-0800, Kathleen.Cooper@sao.wa.gov

To request public records

Public Records Officer
564-999-0918, PublicRecords@sao.wa.gov

Americans with Disabilities

In accordance with the Americans with Disabilities Act, this document will be made available in alternative formats. Please email Webmaster@sao.wa.gov for more information.

Executive Summary

State Auditor's Conclusions (page 11)

The results of this audit reflect the important progress Washington state government has made in addressing the risks associated with disposing of computers and other information technology (IT) equipment that may contain confidential data. In our first audit of data disposal in 2014, we estimated 9% of state computers scheduled for sale during our review period contained confidential data that should have been removed. This audit looked at how a college that does not participate in the state's centralized surplus program handled IT equipment. We found commendable levels of security and efficiency.

Colleges and universities possess tremendous amounts of confidential data, including personal information for each of their students, making safe data disposal imperative. The college we reviewed assumes every surplus machine contains confidential information and acts accordingly. The college purchased industrial-grade equipment to sanitize surplus hard drives. And its policy calls for physically destroying a drive if staff encounter any difficulties in erasing its data.

We tested a sample of IT equipment in the college's surplus program, and none contained confidential data. We are confident that the process in place is a good one. We do make a recommendation to help improve the college's process. As with every undertaking in government, safely disposing of technology requires a vigilant commitment to improvement. Through that commitment, we better protect the information of everyone who relies on public services.

Background (page 6)

Like most state agencies, public institutions of higher education (see sidebar) have the authority to dispose of all the equipment they no longer need for their operations. Their surplus programs take unwanted property – including information technology (IT) equipment like computers, cell phones and printers – and resell, recycle or otherwise dispose of it.

However, colleges handle many records that contain confidential information, including student identification and Social Security numbers or personal banking and medical information. State law requires them to destroy or

This report uses the term "colleges" to indicate both types of institutions of higher education: colleges and universities.

It also does not disclose detailed results of individual tests we performed to decrease the risk to the audited college's data security. As an added precaution, we also do not disclose the identity of the college we audited.

arrange for the destruction of such data before they can send the IT equipment that stored it to surplus. Releasing such information can harm a person's privacy and financial security, and pose the risk of identity theft.

To help colleges and other agencies comply with the law, Washington Technology Solutions (WaTech) developed the Media Sanitization and Disposal Standard. Following the standard helps ensure that discarded data-handling media – meaning any portion of a device that can store or process data – is securely sanitized using one of three sanitizing methods: clearing, purging or destruction, depending on the data category that is stored in the media.

Our Office has conducted two audits evaluating how well state agencies, including a few colleges, removed confidential data from IT devices before selling them through the Department of Enterprise Services (DES) surplus program. This audit sought to evaluate how surplus IT equipment was handled in a higher education setting that does not participate in the DES program but uses its own procedures.

The college has adopted a strong process and had properly sanitized all the IT equipment we tested (page 8)

The college's process for sanitizing IT equipment has several strengths worth highlighting. For example, the college:

- Only resells IT equipment that can be sanitized
- Treats every device as if it contains confidential information
- Uses professional sanitization systems to sanitize devices

Having a strict approach to media sanitization provides assurance no confidential information remains in the equipment prepared for surplus. To have a policy less strict presents a greater risk of a data breach, should one poorly prepared device fall into the wrong hands.

All surplus IT equipment we tested at the college was properly sanitized: we did not find any confidential data on the tested devices. Because our sample was not truly random, we cannot statistically project our results to all equipment at the college. Nonetheless, given the strong process the college has in place, plus the fact that all the devices we tested were properly sanitized, we are confident that the college has a good process in place to consistently sanitize its IT equipment.

Additionally, to obtain the necessary assurance that its sanitizing procedures are working as intended, the college verifies some of its results through testing. However, to help ensure procedures remain successful, the college should test a greater proportion of sanitized IT equipment.

Recommendations (page 12)

We made a recommendation to the college to improve its verification process of media sanitization results. In developing the process, we recommended the college consult with WaTech to determine the appropriate volume and frequency of testing.

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 Office of the State Auditor 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 (leg.wa.gov/about-the-legislature/committees/joint/jlarc-i-900-subcommittee). Our 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

Surplus programs help public colleges dispose of unwanted items, including IT equipment

Like most state agencies, public institutions of higher education (see sidebar) have the authority to dispose of all the equipment they no longer need for their operations. While state agencies use the surplus program operated by the Department of Enterprise Services (DES), many public colleges dispose of such equipment through their own surplus programs. Their surplus programs take unwanted property and resell, recycle or otherwise dispose of it. The types and volume of surplused goods they must manage varies based on institution size, but can include a wide range of items including lab equipment, furniture and information technology (IT) devices from computers and laptops to cell phones and printers. Much of this equipment is available to the public for purchase through surplus stores or auctions.

This report uses the term "colleges" to indicate both types of institutions of higher education: colleges and universities. It also refers exclusively to publicly funded colleges; private colleges are not governed by state standards for disposing of unwanted IT devices.

Public colleges are responsible for removing confidential information from surplus IT equipment

Colleges handle many records that contain confidential information, and different college offices and departments might retain a wide variety of data, including student identification and Social Security numbers or personal banking and medical information. State law requires governmental agencies, including colleges, to destroy or arrange for the destruction of such confidential data before they can send the IT equipment that stored it to surplus. Releasing information of this nature can harm a person's privacy and financial security, and pose the risk of identity theft.

To help colleges and other agencies comply with the law, Washington Technology Solutions (WaTech) developed Media Sanitization and Disposal Standard based on the guidelines issued by the National Institute of Standards and Technology (NIST). Following the standard helps ensure that discarded data-handling media – meaning any portion of a device that can store or process data – is securely sanitized using one of three sanitizing methods: clearing, purging or destruction, depending on the data category that is stored in the media. The standard also calls for the college to establish and document its procedures.

Among the requirements agencies must follow are:

- Develop media sanitization and disposal procedures to render stored data unusable
- Work with the people responsible for the data to select the appropriate sanitizing method
- Test at least 10% of sanitized media to assure that proper protection is maintained

Although the law requires that only the devices used by colleges' business and administrative offices follow this standard, WaTech encourages colleges to apply this standard to their academic, research, medical and other offices, too.

This audit assessed the effectiveness of one college's practices to sanitize surplus IT equipment before selling it

Our Office has conducted two audits evaluating how well state agencies, including a few colleges, removed confidential data from IT devices before selling them through the DES surplus program. Those audits identified several issues with the auditees' data disposal practices and recommended ways to improve them.

However, some colleges make their own surplus arrangements and do not use the DES program, and were thus excluded from earlier audits. This audit sought to evaluate how surplus IT equipment was handled in a higher education setting that does not participate in the DES program but uses its own procedures.

This report does not disclose detailed results of individual tests we performed to decrease the risk to the audited college's data security. As an added precaution, we also do not disclose the identity of the college we audited.

This audit answered the following question:

- Does the institution of higher education remove or destroy confidential information found on computers and other IT equipment before selling them as surplus?

Audit Results

The college has adopted a strong process and had properly sanitized all the IT equipment we tested

Answer in brief

The college's process for sanitizing IT equipment has several strengths worth highlighting. For example, the college:

- Only resells IT equipment that can be sanitized
- Treats every device as if it contains confidential information
- Uses professional sanitization systems to sanitize devices

All surplus IT equipment we tested at the college was properly sanitized. However, to help ensure procedures remain successful, the college should test a greater proportion of sanitized IT equipment.

The college's process for sanitizing IT equipment has several strengths worth highlighting

To identify the effectiveness of the selected college's practices in media sanitization and any potential improvements, we reviewed its procedures for sanitizing and destroying IT equipment, and toured the surplus store.

We found the college had a very thorough and efficient approach to ensuring data-processing or data-storing equipment. The college approaches media sanitization with three important factors in place to ensure discarded IT equipment has been properly prepared for disposal.

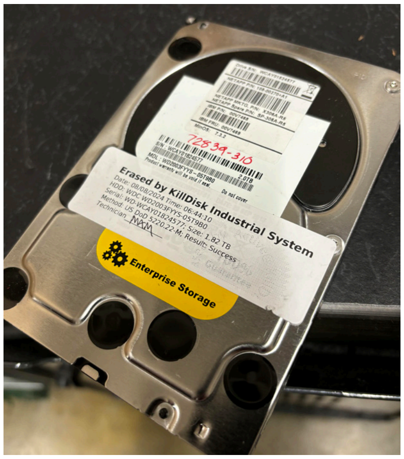
1. **Only resell IT equipment that can be sanitized.** The audited college sanitizes and then resells different types of IT equipment with media that can process or store data in place, including desktop computers, laptops and servers. However, the college does not resell the equipment it is not able to sanitize in-house. Instead, the college's protocols instruct staff to send several types of devices, such as cellphones and Android tablets, directly to its electronics recycling vendor to be destroyed and recycled. Staff at the college said the

volume of items sent for surplus increased after the COVID-19 pandemic, and the college lacks sufficient staff to sanitize it all themselves. They also said it can be a time-consuming and laborious process to sanitize some of the equipment. Destroying it is more straightforward and much easier.

College staff showed auditors a box of destroyed hard drives.

Photo credit: State Auditor's Office.

2. **Treat every device as if it contains confidential information.** Instead of evaluating each individual device and the sensitivity of information it might contain, the college treats every device as if it contains confidential data. This assumption made it safer to establish a strict process for sanitizing all hard drives. Depending on the type of hard drive, they are either erased or destroyed. If an error happens while the hard drive is being erased, the documented procedures instruct an employee to destroy the hard drive instead of making another attempt at erasing the data. According to the college staff, they destroy about 75% of hard drives.
3. **Use professional sanitization systems to sanitize devices.** The college uses an industrial grade data-erasing system to sanitize hard drives. Although such systems can be expensive (staff said prices for this particular tool range between $15,000 and $20,000), it helps the college sanitize a large volume of devices with a high degree of confidence.



An example of a sanitized hard drive at the college.

Photo credit: State Auditor's Office.

Having a strict approach to media sanitization provides assurance no confidential information remains in the equipment prepared for surplus. To have a policy less strict presents a greater risk of a data breach, should one poorly prepared device fall into the wrong hands.

All surplus IT equipment we tested at the college was properly sanitized

To determine whether the college had taken appropriate steps to remove any confidential data from IT equipment, we selected for testing 32 devices (16 devices for each of two tests) that were ready for sale. We chose an arbitrary selection of devices available at the surplus store. The devices we tested included desktop and laptop computers, a variety of hard disks and solid-state hard drives, iMacs and iPads. (For more information about our methodology, see Appendix B.)

We conducted two separate tests to ensure confidential information was properly removed. For the first test, we inspected 16 devices to ensure hard drives were removed. For the second test, we inspected 16 hard drives to ensure they were properly sanitized. To do this, we plugged the selected hard drive into State Auditor's Office laptop and then used free file recovery software to examine the hard drive and computer system.

In all cases, we confirmed that hard drives had either been removed from the device or that they had been properly sanitized before the device was made available for sale to the public.

Even though we did not find any confidential data on the tested devices, we cannot statistically project our results to all equipment at the college because our sample was not truly random. However, given the strong process the college has in place, plus the fact that all the devices we tested were properly sanitized, we are confident that the college has a good process in place to consistently sanitize its IT equipment.

Testing a greater proportion of sanitized IT equipment would help ensure procedures remain successful

To obtain the necessary assurance that its sanitizing procedures are working as intended, an organization must periodically verify its results through testing. WaTech's standard requires state agencies to test 10% of their sanitized media. While the standard does not specify the frequency of testing or whether all sanitized media must be tested, guidelines issued by the National Institute of Standards and Technology (NIST) do. They suggest either full verification every time media is sanitized or verifying a representative sample of treated items.

College staff said they do fully verify sanitized hard drives that are inside the computers available for sale to the public in the college's surplus store. However, they do not apply this procedure to the hard drives sold through auction. College staff said they do not verify auctioned drives because they were very confident the college's sanitization protocol – erasing all data or destroying any hard drives that meet certain criteria – ensures data has been wiped from all devices.

Staff said the college destroys the majority of hard drives and the results of our tests confirmed the sanitization process appeared to be working well. However, periodically testing a portion of sanitized devices would provide additional assurance that the sanitization process is working as intended to help prevent the release of confidential data to the public.

State Auditor's Conclusions

The results of this audit reflect the important progress Washington state government has made in addressing the risks associated with disposing of computers and other technology that may contain confidential data. In our first audit of data disposal in 2014, we estimated 9% of state computers scheduled for sale during our review period contained confidential data that should have been removed. This audit looked at how a college that does not participate in the state's centralized surplus program handled IT equipment. We found commendable levels of security and efficiency.

Colleges and universities possess tremendous amounts of confidential data, including personal information for each of their students, making safe data disposal imperative. The college we reviewed assumes every surplus machine contains confidential information and acts accordingly. The college purchased industrial-grade equipment to sanitize surplus hard drives. And its policy calls for physically destroying a drive if staff encounter any difficulties in erasing its data.

We tested a sample of IT equipment in the college's surplus program, and none contained confidential data. We are confident that the process in place is a good one. We do make a recommendation to help improve the college's process. As with every undertaking in government, safely disposing of technology requires a vigilant commitment to improvement. Through that commitment, we better protect the information of everyone who relies on public services.

Recommendations

For the audited college

To ensure proper protection of confidential data, as described on page 10, we recommend the college:

1. Develop and document a procedure to periodically test its sanitized equipment sold through auction to ensure no confidential data is left in the media. In developing the process, consult with WaTech to determine the appropriate volume and frequency of testing.

Agency Response

We gave copies of the final report to the public college's surplus program and its management. In keeping with our concerns about exposing it to additional risk, the college has not provided a formal written response, but officials said they generally agree with the report's findings and conclusions, and that they have begun to address the gap found in their verification process.

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 sections of this report.

I-900 element	Addressed in the audit
1. Identify cost savings	**No.**
2. Identify services that can be reduced or eliminated	**No.**
3. Identify programs or services that can be transferred to the private sector	**No.**
4. Analyze gaps or overlaps in programs or services and provide recommendations to correct them	**No.**
5. Assess feasibility of pooling information technology systems within the department	**No.**

I-900 element	Addressed in the audit
6. Analyze departmental roles and functions, and provide recommendations to change or eliminate them	**No.**
7. Provide recommendations for statutory or regulatory changes that may be necessary for the department to properly carry out its functions	**No.**
8. Analyze departmental performance data, performance measures and self-assessment systems	**No.**
9. Identify relevant best practices	**Yes.** The audit identified the best practices related to media handling and sanitizing when preparing IT devices for surplus.

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* (July 2018 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.

The mission of the Office of the Washington State Auditor

To provide citizens with independent and transparent examinations of how state and local governments use public funds, and develop strategies that make government more efficient and effective. The results of our work are widely distributed through a variety of reports, which are available on our website and through our free, electronic subscription service. We take our role as partners in accountability seriously. We provide training and technical assistance to governments and have an extensive quality assurance program. For more information about the State Auditor's Office, visit www.sao.wa.gov.

Appendix B: Objectives, Scope and Methodology

Objectives

The purpose of this performance audit is to assess the effectiveness of a selected public college's practices to ensure IT equipment does not contain any confidential data before it is sold to the public. The audit addressed the following objective:

- Does the institution of higher education remove or destroy confidential information found on computers and other IT equipment before selling them as surplus?

Scope

To see whether the college complies with the Media Sanitization and Disposal Standard issued by Washington Technology Solutions (WaTech), and whether college staff understand what controls they should have in place to ensure security of the data, we reviewed the college's procedures on data sanitization and destruction that were in effect during our audit.

To evaluate the effectiveness of the selected college's practices, we tested computer media to determine if any data remained detectable after college staff prepared the items for sale. We limited our testing to only those devices that were ready to be sold at the time of our testing. The equipment relevant to our specific audit objectives included different types of computers, a variety of hard disks and solid-state hard drives, iMacs and iPads. We did not test items that were actively being auctioned for two reasons:

- Doing so would have caused significant disruption to the auction process
- We already had a large number of items we could test that were ready for auction but had not yet been posted for sale

Neither did we test:

- Any hard drives that were destroyed
- Devices that were sent to a third-party vendor for recycling
- Devices that were not available at the store on the day of testing

Methodology

We obtained the evidence used to support the findings, conclusions and recommendations in this audit report during our fieldwork period (late September to mid-November 2024). We have summarized the work we performed to address the audit objective below.

Objective 1: Does the institution of higher education remove or destroy confidential information found on computers and other IT equipment before selling them as surplus?

To understand media sanitization and data protection requirements, we reviewed relevant laws and standards related to the protection of confidential information, media sanitization and destruction.

To understand the college's approach to these activities in regard to its surplus IT equipment, we reviewed college's written procedures on media sanitization, visited its surplus store and observed some of the steps the college takes to protect the confidential information. We also interviewed staff tasked with ensuring no data is left on the IT equipment when preparing it to be sold at the surplus store and at auction.

Testing devices

To determine whether the college had taken appropriate steps to remove any confidential data from IT equipment it intended to surplus, we identified our overall sample size of 32 devices (16 devices for each of two tests) using the Raosoft sample size calculator. This sample size was drawn from the entire population and was not based on the sanitization method applied to these devices. To determine the sample size, we used an estimated monthly population of about 2,250 electronic devices, a 5% margin of error, 95% confidence level, and 99% response distribution.

To select the equipment for our sample, we chose an arbitrary selection of devices available at the surplus store on the day of testing. The devices we tested included desktop computers, laptop computers, a variety of hard disks and solid-state hard drives, iMacs and iPads.

We conducted two separate tests to ensure confidential information was properly removed. For the first test, we inspected 16 devices to ensure hard drives were removed. For the second test, we inspected 16 hard drives to ensure they were properly sanitized. To do this, we plugged the selected hard drive into State Auditor's Office laptop, and then used free file recovery software to examine the hard drive and computer system.

Although we did not find any confidential information on the tested equipment, we cannot project our results to all equipment at the college for two reasons:

- We did not select each device based on the sanitization method applied to it
- Our sample was not truly random

However, given the strong procedures the college has in place and the fact that all the devices we tested were properly sanitized, we are confident that the college has a good process to consistently sanitize its IT equipment.

Work on internal controls

We identified key internal controls and assessed their design and operating effectiveness.

To assess the design of internal controls, we reviewed the college's procedures on media sanitization and destruction, toured the surplus store and interviewed staff. Based on our conducted work, we identified a deficiency in the design of internal controls: the college does not have a process to test all its sanitized media because the staff is very confident in its sanitization methods.

To assess the operating effectiveness of internal controls, we tested IT equipment prepared for surplus to see if it contains any confidential information. We did not find any confidential information on the tested equipment. Based on this work, we identified no deficiencies in the operating effectiveness of internal controls.

Reporting confidential or sensitive information

This report does not disclose detailed results of individual tests we performed to decrease the risk to the audited college's data security. As an added precaution, we also do not disclose the identity of the college we audited.

"Our vision is to increase **trust** in government. We are the public's window into how tax money is spent."

– Pat McCarthy, State Auditor

Washington State Auditor's Office
P.O. Box 40031 Olympia WA 98504

www.sao.wa.gov

1-564-999-0950

Office of the Washington State Auditor
Pat McCarthy