Office of the Washington State Auditor
Pat McCarthy

Performance Audit

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

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 information technology (IT) equipment, they are responsible for ensuring it does not contain any confidential information.

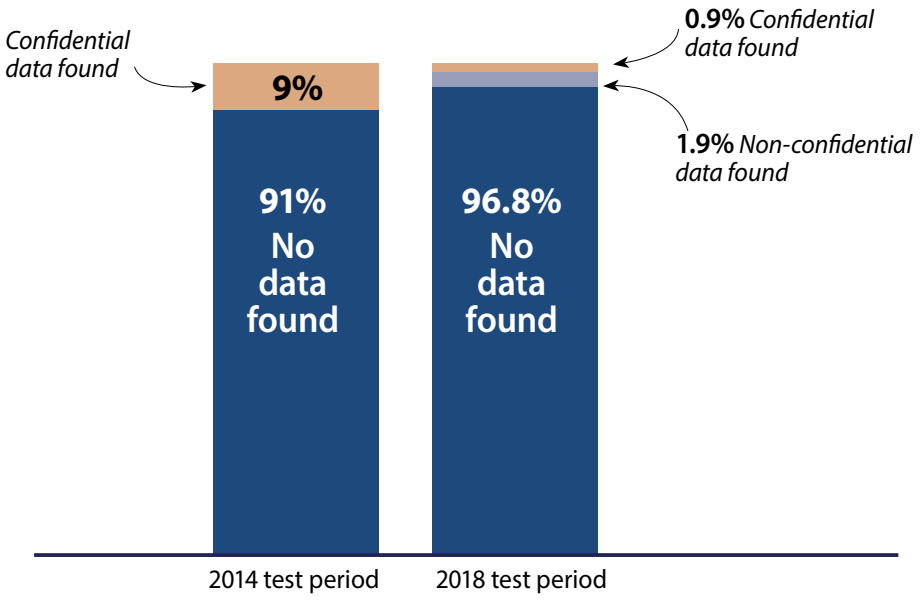
In 2014, the Office of the Washington State Auditor conducted a performance audit to determine whether agencies were removing data from their IT devices in accordance with state law and the Office of the Chief Information Officer (OCIO) requirements. This follow-up audit addresses whether the state has 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 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.

Confidential data found on state surplus computers dropped 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.

Report number 1022845, published 12/17/2018

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.

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

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.

We made recommendations to the agencies to address specific areas where their policies and procedures did not align with state requirements and best practices.

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

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.

- ☑ Annually review policies and procedures, and revise them as necessary to ensure they include the following state requirements and National Institute of Standards and Technology (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
- ☑ Update policies and procedures to include state-approved methods for erasing data from mobile devices, such as cellphones and tablets