

# STATE OF FLORIDA AUDITOR GENERAL

## Information Technology Operational Audit

Report No. 2016-166  
March 2016

### DEPARTMENT OF ENVIRONMENTAL PROTECTION, DEPARTMENT OF LAW ENFORCEMENT, AND STATE BOARD OF ADMINISTRATION

Surplus Computer Hard Drive Disposal Processes



Sherrill F. Norman, CPA  
Auditor General

## **Secretary of the Department of Environmental Protection**

Pursuant to Section 20.255(1), Florida Statutes, the Secretary of the Department of Environmental Protection is appointed by the Governor with the concurrence of three members of the Cabinet and is confirmed by the Senate. Jonathan Steverson served as Secretary during the period of our audit.

## **Executive Director of the Department of Law Enforcement**

Pursuant to Section 20.201(1), Florida Statutes, the head of the Department of Law Enforcement is the Governor and the Cabinet, which consists of the Governor, Attorney General, Chief Financial Officer, and Commissioner of Agriculture. The Executive Director of the Department of Law Enforcement is appointed by the Governor with the approval of three members of the Cabinet and is subject to confirmation by the Senate. Richard L. Swearingen served as Executive Director during the period of our audit.

## **Board of Trustees and Executive Director of the State Board of Administration**

The State Board of Administration's Board of Trustees is composed of the Governor, as Chair; the Chief Financial Officer; and the Attorney General. The Trustees delegate administrative and investment authority to an appointed Executive Director. Ashbel Williams served as Executive Director during the period of our audit.

The team leader was Benjamin Ho and the audit was supervised by Brenda Shiner, CISA.

Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at [arthart@aud.state.fl.us](mailto:arthart@aud.state.fl.us) or by telephone at (850) 412-2923.

This report and other reports prepared by the Auditor General are available at:

[www.myflorida.com/audgen](http://www.myflorida.com/audgen)

Printed copies of our reports may be requested by contacting us at:

**State of Florida Auditor General**

**Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722**

# DEPARTMENT OF ENVIRONMENTAL PROTECTION, DEPARTMENT OF LAW ENFORCEMENT, AND STATE BOARD OF ADMINISTRATION

## Surplus Computer Hard Drive Disposal Processes

### **SUMMARY**

---

This operational audit focused on evaluating selected information technology (IT) controls applicable to the storage and safeguarding of surplus computer hard drives awaiting disposal at the Department of Environmental Protection (DEP), Department of Law Enforcement (DLE), and State Board of Administration (SBA) and included a review of the surplus computer hard drive disposal processes followed by the DEP, DLE, and SBA when sanitizing (erasing data from or destroying) and disposing of hard drives. Our audit disclosed the following:

**Finding 1:** Documentation of surplus computer hard drive sanitization and disposition needs improvement to better demonstrate that appropriate actions were taken to prevent inappropriate or unauthorized access to confidential or exempt information.

**Finding 2:** Certain security controls related to surplus computer hard drive disposal processes need improvement to better ensure the continued protection of confidential and exempt information.

### **BACKGROUND**

---

State governmental entities replace computers (i.e., desktops, laptops, and servers) on a periodic basis, often according to a planned replacement cycle. It is important for State governmental entities to follow an orderly and controlled process for disposing of unneeded surplus computers in an economic, efficient, and effective manner. Most importantly, if surplus computers are to be made available by State governmental entities to other entities (e.g., by donation to nonprofit organizations) or disposed of, appropriate procedures need to be followed to sanitize the surplus computer hard drives to ensure that confidential or exempt information is physically removed and not inappropriately disclosed. Sanitization methods for hard drives include erasure by overwriting (wiping) the data, degaussing (demagnetizing), or physical destruction.

Deleting files on surplus computer hard drives through normal system means does not physically remove data as it only removes the operating system's ability to locate the information. Unless appropriate sanitization methods are followed to overwrite, degauss, or physically destroy the hard drives, the information contained therein can be easily recovered using commercially available specialized software. This creates the risk that any confidential or exempt information contained on the hard drives may be inappropriately disclosed.

Many Federal and State laws limit the disclosure of certain information. For example, Section 119.071(5)(a)5., Florida Statutes, provides that social security numbers held by an agency are confidential and exempt from public disclosure. Consequently, State governmental entities may not be

in compliance with applicable laws if due diligence is not exercised throughout surplus computer hard drive disposal processes.

## ***FINDINGS AND RECOMMENDATIONS***

---

### **Finding 1: Surplus Computer Hard Drive Sanitization and Disposition Documentation**

Effective security controls include the proper safeguarding of computer hard drives awaiting disposal to better ensure appropriate accountability and control of hard drives and the protection of confidential and exempt information contained therein. It is critical that State governmental entities maintain complete and accurate disposal records to document the surplus computer hard drives that had been sanitized, when and how they were sanitized, and the final disposition.

As part of our audit, we evaluated the sanitization documentation and disposition records maintained by the selected State governmental entities and noted that the documentation was not always accurate or complete. Specifically, we noted that:

- **Department of Environmental Protection (DEP)**. The DEP documented the sanitization of surplus computers on the *DEP Certification of Surplus Property* (certification) form. DEP staff stated that, for surplus servers located at the Bob Martinez Center in Tallahassee, hard drives were removed and physically destroyed prior to their disposition. On September 25, 2015, we inspected hard drives that had been physically destroyed by drilling holes through the hard drives. DEP staff further stated that the physically destroyed hard drives were associated with three servers approved for surplus and listed on the certification form dated August 31, 2015. However, our examination of the certification form disclosed that the quantity and serial numbers of the physically destroyed hard drives were not noted on the certification form. Furthermore, the DEP did not provide us with any other documentation that associated the physically destroyed hard drives with the surplus servers. Therefore, we were unable to determine that the hard drives associated with the surplus servers were properly sanitized.
- **Department of Law Enforcement (DLE)**. *DLE Information Resource Management (IRM) Procedure 1.200, Physical Property Management*, provides that all physical media containing information is to be destroyed on-site by a third-party vendor and documentation of the disposition is to be maintained. DLE staff stated that hard drives were removed from surplus computers and stored in the DLE Headquarters facility pending destruction. However, the DLE did not maintain documentation that associated the removed hard drives with the originating surplus computers. As a result, the DLE could not demonstrate that all removed hard drives associated with the surplus computers remained at the DLE Headquarters facility and were properly controlled while awaiting sanitization and disposition. Additionally, in response to our audit inquiry, DLE management indicated that hard drives removed from surplus computers had not been destroyed since February 5, 2014, and that, as of November 12, 2015, over 500 removed hard drives were awaiting destruction.
- **State Board of Administration (SBA)**. *SBA KillDisk 4.1 Procedures (Procedures)* provide step-by-step instructions for sanitizing hard drives within functional computers using LSoft Technologies Inc., Active@ KillDisk hard drive erasure software. Additionally, the *Procedures* provide instructions for disassembling and disposing of hard drives when the originating computer is not functional and require staff to complete a *Sanitization Method Log* that includes the method of sanitization used. We reviewed the *Sanitization Method Log*, as of August 25, 2015, that listed 35 computers as being sanitized and ready for disposal. For 5 of the 35 computers, the *Sanitization Method Log* indicated that the surplus computers did not contain hard drives. In

response to our audit inquiry, SBA staff stated that the 5 hard drives had been removed from the surplus computers because the computers were not functional. However, the serial numbers of the removed hard drives were not documented on the *Sanitization Method Log* and SBA staff could not provide documentation that the hard drives had been disassembled and disposed of in accordance with the *Procedures*.

Without accurate and complete documentation of surplus computer hard drive sanitization and disposition, management's assurance that proper accountability and adequate control of hard drives has been established to prevent inappropriate or unauthorized access to confidential or exempt information is limited.

**Recommendation: We recommend that DEP, DLE, and SBA management improve documentation of surplus computer hard drive sanitization and disposition to better demonstrate that appropriate actions were taken to prevent inappropriate or unauthorized access to confidential or exempt information.**

## **Finding 2: Security Controls – Surplus Computer Hard Drive Disposal Processes**

Security controls are intended to protect the confidentiality, integrity, and availability of data and information technology (IT) resources. Our audit procedures disclosed certain security controls related to the surplus computer hard drive disposal processes at the DEP, DLE, and SBA that need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising those entities' information. However, we have notified appropriate management of the specific issues. Without appropriate security controls related to surplus computer hard drive disposal processes, the risk is increased that DEP, DLE, and SBA information may be compromised.

**Recommendation: We recommend that DEP, DLE, and SBA management improve security controls related to surplus computer hard drive disposal processes to better ensure the continued protection of confidential and exempt information.**

## **OBJECTIVES, SCOPE, AND METHODOLOGY**

The Auditor General conducts operational audits of State governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit from August 2015 through October 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected security controls applicable to the storage and safeguarding of surplus computer hard drives awaiting disposal at the Department of Environmental Protection (DEP), Department of Law Enforcement (DLE), and State Board of Administration (SBA) during the period August 2015 through October 2015 and selected actions through November 12, 2015. The overall objectives of the audit were:

- To obtain an understanding of the procedures and key processes for the storage, sanitization, and disposition of surplus computers at the DEP, DLE, and SBA.
- To evaluate the effectiveness of selected State governmental entities' security controls for the storage and safeguarding of surplus computers awaiting disposal.
- To evaluate the effectiveness of selected State governmental entities' controls for removal of confidential or exempt information from surplus computer hard drives before surplus computers are made available for reuse or disposal.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the security controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular security controls, legal compliance matters, and records considered.

As described in more detail below, for the security controls included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of the security controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of security controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of State governmental entities management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Interviewed personnel at the selected State governmental entities.
- Obtained an understanding of the procedures and key processes used for the storage, sanitization, and disposition of surplus computers at the selected State governmental entities.
- Observed and evaluated the effectiveness of security controls for the secure storage of surplus computers at the selected State governmental entities. Specifically, we evaluated:
  - For the DEP, the physical access controls for all surplus computers located at the Bob Martinez Center and the Carr Building as of August 19, 2015.
  - For the DLE, the physical access controls for all surplus computers located in the Tallahassee Regional Operations Center as of August 26, 2015.

- For the SBA, the physical access controls for all surplus computers at various locations in the Hermitage Centre as of August 26, 2015, and September 23, 2015.
- Evaluated the sanitization documentation and disposition records maintained by the selected State governmental entities.
- Observed and evaluated the effectiveness of security controls related to the sanitization and disposition of surplus computer hard drives at the selected State governmental entities. Specifically, we evaluated the entities' sanitization and disposition actions related to:
  - For the DEP, 12 of 58 surplus desktop and laptop computers as of September 11, 2015, and all 3 surplus servers as of September 25, 2015.
  - For the DLE, all surplus hard drives as of November 12, 2015.
  - For the SBA, 5 of 35 surplus computers as of August 25, 2015, and 5 of 11 removed computer hard drives as of August 28, 2015.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for managements' responses the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Managements' responses are included in this report under the heading **MANAGEMENTS' RESPONSES**.

## **AUTHORITY**

---

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any State governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.



Sherrill F. Norman, CPA  
Auditor General

# MANAGEMENTS' RESPONSES

---



## Florida Department of Environmental Protection

Marjory Stoneman Douglas Building  
3900 Commonwealth Boulevard  
Tallahassee, Florida 32399-3000

Rick Scott  
Governor

Carlos Lopez-Cantera  
Lt. Governor

Jonathan P. Steverson  
Secretary

March 4, 2016

Ms. Sherrill F. Norman, CPA  
State of Florida Auditor General  
111 West Madison Street  
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

As required in Section 11.45(4)(d), Florida Statutes, enclosed is the Department of Environmental Protection's (DEP) response to the preliminary and tentative findings and recommendations for your multi agency audit of Surplus Computer Hard Drive Disposal Processes.

We appreciate the professionalism displayed by your audit staff. If further information is needed, please contact DEP's Inspector General, Candie Fuller, at 850/245-2548.

Sincerely,

A handwritten signature in blue ink, appearing to be "Jonathan P. Steverson", with a long horizontal line extending to the right.

Jonathan P. Steverson  
Secretary

Enclosure

cc: Candie Fuller, Inspector General, DEP



**Preliminary and Tentative Audit Findings (Response)  
Surplus Computer Hard Drive Disposal Processes**

**Office of Technology & Information Services (OTIS)**

**March 4, 2016**

**FINDING NUMBER 1:**

**Surplus Computer Hard Drive Sanitization and Disposition Documentation**

**RECOMMENDATION:**

Recommendation is for DEP management to improve documentation of surplus computer hard drive sanitization and disposition to better demonstrate that appropriate actions were taken to prevent inappropriate or unauthorized access to confidential or exempt information.

**DEP RESPONSE:**

DEP concurs with the finding and will work to improve documentation of these hard drives through the following actions:

- I. DEP will develop a policy and process requiring additional steps to be taken to document serial numbers for surplus computer hard drives being destroyed and disposed.
- II. Staff responsible for the following functions must adhere to the policy:
  - a. sanitizing surplus computer hard drives
  - b. completing "DEP Certification of Surplus Property" form

**FINDING NUMBER 2:**

**Security Controls – Surplus Computer Hard Drive Disposal Processes**

**RECOMMENDATION:**

It is recommended that DEP management improve security controls related to surplus computer hard drive disposal processes to better ensure the continued protection of confidential and exempt information.

**DEP RESPONSE:**

DEP concurs with the finding and will improve security controls related to surplus computer hard drive disposal processes to better ensure the continued protection of confidential and exempt information.

Page 1 of 1



Florida Department of  
Law Enforcement

Richard L. Swearingen  
Commissioner

Office of Executive Director  
Post Office Box 1489  
Tallahassee, Florida 32302-1489  
(850) 410-7001  
www.fdle.state.fl.us

Rick Scott, *Governor*  
Pam Bondi, *Attorney General*  
Jeff Atwater, *Chief Financial Officer*  
Adam Putnam, *Commissioner of Agriculture*

February 23, 2016

Ms. Sherrill F. Norman  
Auditor General  
G74 Claude Pepper Building  
111 West Madison Street  
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

The enclosed response is provided for the Preliminary and Tentative Findings Report on the Information Technology Operational Audit Surplus Computer Hard Drive Disposal Processes for the Florida Department of Law Enforcement.

**Finding 1: Surplus Computer Hard Drive Sanitization and Disposition Documentation**

**Recommendation:**

We recommend that DEP, DLE, and SBA management improve documentation of surplus computer hard drive sanitization and disposition to better demonstrate that appropriate actions were taken to prevent inappropriate or unauthorized access to confidential or exempt information.

**Response**

We agree with this finding and are moving forward with the recommendation of improving our documentation.

**Finding 2: Security Controls – Surplus Computer Hard Drive Disposal Processes**

**Recommendation:**

We recommend that DEP, DLE, and SBA management improve security controls related to surplus computer hard drive disposal processes to better ensure the continued protection of confidential and exempt information.

**Response:**

We agree that more security controls related to surplus computer hard drive disposal processes can be added.

If you require further information regarding the actual or proposed corrective actions, please contact me or Inspector General Lourdes Howell-Thomas at (850) 410-7241.

Sincerely,

Richard L. Swearingen  
Commissioner

RLS/sc

*Service • Integrity • Respect • Quality*



STATE BOARD OF ADMINISTRATION  
OF FLORIDA

1801 HERMITAGE BOULEVARD  
TALLAHASSEE, FLORIDA 32308  
(850) 488-4406

POST OFFICE BOX 13300  
32317-3300

RICK SCOTT  
GOVERNOR  
CHAIR

JEFF ATWATER  
CHIEF FINANCIAL OFFICER

PAMBONDI  
ATTORNEY GENERAL

ASH WILLIAMS  
EXECUTIVE DIRECTOR & CIO

February 29, 2016

Ms. Sherrill F. Norman  
Auditor General, State of Florida  
G74 Claude Pepper Building  
111 West Madison Street  
Tallahassee, FL 32399-1450

Dear Ms. Norman:

Our responses to the preliminary and tentative findings and recommendations which are included in your report on the Surplus Computer Hard Drive Disposal Processes of the State Board of Administration are below:

**Finding 1:**

**Surplus Computer Hard Drive Sanitization and Disposition Documentation**

**Recommendation:** We recommend that SBA management improve documentation of surplus computer hard drive sanitization and disposition to better demonstrate that appropriate actions were taken to prevent inappropriate or unauthorized access to confidential or exempt information.

**Response:** The SBA agrees and has already taken corrective action.

**Finding 2:**

**Security Controls – Surplus Computer Hard Drive Disposal Processes**

**Recommendation:** We recommend that SBA management improve security controls related to surplus computer hard drive disposal processes to better ensure the continued protection of confidential and exempt information.

**Response:** The SBA agrees and has already taken corrective action.

Ms. Sherrill F. Norman  
February 29, 2016  
Page 2

We would like to thank the Office of the Auditor General for its diligence, professionalism and efforts.

Sincerely,

A handwritten signature in blue ink that reads "Ashbel C. Williams". The signature is written in a cursive style with a prominent initial "A".

Ashbel C. Williams  
Executive Director & CIO