REPORT NO. 2014-187
APRIL 2014

SURPLUS COMPUTER HARD DRIVE DISPOSAL PROCESSES

AT SELECTED STATE AGENCIES

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

STATE AGENCY HEADS

The Florida Statutes establish the various State agencies and provide the title and selection process for the head of each State agency. The five State agencies included within the scope of this IT operational audit and the respective agency heads who served during the period of our audit were as follows:

Department of	Established By Florida Statutes	State Agency Head	Dates of Service
Education	Section 20.15	Pam Stewart, Commissioner	From September 2013
The Lottery	Chapter 24	Cynthia F. O'Connell, Secretary	From February 2011
Management Services	Section 20.22	Craig J. Nichols, Secretary	From July 2012
Revenue	Section 20.21	Marshall Stranburg, Executive Director	From April 2013
Transportation	Section 20.23	Ananth Prasad, Secretary	From April 2011

The audit team leader was Robert McKee, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 412-2722; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

SURPLUS COMPUTER HARD DRIVE DISPOSAL PROCESSES

At Selected State Agencies

SUMMARY

To promote the economic, efficient, and effective operation of State government and to minimize the risk of inappropriate or illegal disclosure of confidential or exempt information, surplus computer hard drives must be disposed of in a well-controlled fashion. Agency for Enterprise Information Technology (AEIT)[1] Rule 71A-2.009(2)(c), Florida Administrative Code, provides that agencies shall implement procedures for the removal of confidential or exempt information from electronic media prior to transfer or final disposition.

Our operational audit focused on information technology (IT) controls applicable to the storage and disposal of surplus computer hard drives at the following State agencies: Department of Education (DOE), Department of the Lottery (DOL), Department of Management Services (DMS), Department of Revenue (DOR), and Department of Transportation (DOT). This audit included a review of the procedures followed by the agencies in sanitizing (erasing data from) surplus computer hard drives.

Our audit disclosed areas in which enhancements to surplus computer hard drive disposal processes and controls were needed. The results of our audit are summarized below:

Finding No. 1: Certain security controls related to surplus computer hard drive disposal processes needed improvement.

Finding No. 2: DMS lacked adequate documentation regarding the sanitization of surplus computer hard drives.

BACKGROUND

State agencies replace computers on a frequent basis, often according to a planned replacement cycle. It is important for State agencies 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 released by a State agency to another entity, such as by donation to a nonprofit organization, appropriate procedures need to be followed to sanitize the surplus computer hard drives to ensure that confidential or exempt information is not unintentionally disclosed.

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

Many Federal and State laws exist that 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 agencies may not be in compliance with applicable State laws if due diligence is not exercised throughout the surplus computer hard drive disposal processes.

[1] During the 2012 Legislative Session, HB 5011 that abolished AEIT and reassigned the functions and duties of AEIT to a new State agency was passed by the Legislature and presented to the Governor for signature. The bill was vetoed by the Governor on April 20, 2012. However, AEIT underwent defacto dissolution as the 2012 General Appropriations Act made no appropriations for the funding of positions in AEIT. As of the completion of our audit, rulemaking authority and responsibility for promoting or enforcing compliance with existing AEIT rules had not been established.

FINDINGS AND RECOMMENDATIONS

Our IT operational audit focused on the effectiveness of procedures over surplus computer hard drive disposal processes including appropriately safeguarding surplus computers awaiting disposal and accurately removing confidential or exempt information from the surplus computer hard drives prior to disposal at DOE, DOL, DMS, DOR, and DOT. Our audit disclosed that the surplus computer hard drive disposal processes at DOL and DOR were operating effectively, while the processes at DOE, DMS, and DOT needed improvement.

Finding No. 1: Surplus Computer Hard Drive Disposal Processes

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Effective IT security includes controls that limit unintentional access to confidential or exempt information during the surplus computer hard drive disposal process.

Our audit disclosed certain security controls related to surplus computer hard drive disposal processes that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising confidential agency information. However, we have notified appropriate agency management of the specific issues. Due to the confidential nature of these findings, we have requested that the selected State agencies not provide a written response to this finding and, accordingly, no response to this finding is included in this report.

Without adequate security controls related to surplus computer hard drive disposal processes, the risk is increased that confidential and exempt information may be compromised.

Recommendation: Security controls over the surplus computer hard drive disposal processes should be improved to ensure the continued protection of confidential and exempt information.

Finding No. 2: Surplus Computer Hard Drive Sanitization Documentation

It is critical that a State agency maintain sanitization records of its surplus computer hard drives to document that the hard drives were sanitized; when and how they were sanitized; and the final disposition. Ensuring that sanitization processes are appropriately documented helps establish proper accountability and control of surplus computer hard drives.

DMS policy, *Information Technology 09-101, Electronic Media Sanitization*, required that all electronic storage media devices, including hard disk drives, magnetic tape, optical storage drives, and electronic circuit memory devices, that may contain confidential or exempt information must be properly sanitized in accordance with *National Institute of Standards and Technology (NIST) Special Publication 800-88, Guidelines for Media Sanitization (Special Pub 800-88)* prior to repurposing outside of the division of ownership or leaving the custody of the Department for disposition. According to *NIST Special Pub 800-88*, a record of the sanitization of surplus IT media property, including what, when, and how the media were sanitized and the final disposition of the media is necessary.

DMS maintained documentation of the disposal of surplus computers, but did not maintain any records documenting that surplus computer hard drives were properly sanitized prior to the disposal of the computers. Without appropriately documenting the sanitization of surplus computer hard drives, the risk is increased that there will not be proper accountability and control of surplus computer hard drives containing confidential or exempt information resulting in potentially unauthorized disclosure of the information.

Recommendation: DMS should document, in accordance with established policy, the sanitization of surplus computer hard drives before disposal of the computers.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of 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 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 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 objectives of this IT operational audit were to determine the effectiveness of selected State agencies' procedures for the storage and safeguarding of surplus computers awaiting disposal and for the removal of confidential or exempt information from the surplus computer hard drives prior to disposal.

The scope of our audit focused on IT controls over the surplus computer hard drive disposal processes during the period October 2013 through January 2014 at DOE, DOL, DMS, DOR, and DOT.

This audit was designed to identify, for the IT 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 IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT controls included within the scope of our 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 our audit; obtaining an understanding of the IT 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 our audit's findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our audit included the selection and examination of IT 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 agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting our audit, we:

- Interviewed appropriate personnel at the selected State agencies.

- Obtained an understanding of the key processes used for the storage and disposal of surplus computers at the selected State agencies.
- Observed and evaluated the controls related to the secure storage, erasure, and documentation of surplus computer hard drives at the selected State agencies.
- Evaluated the effectiveness of DOE, DOL, DOR, and DOT controls from October 18, 2013, through November 12, 2013, related to the removal of confidential or exempt information from surplus computer hard drives before being made available for reuse or disposal. DMS did not have surplus computers available at the time of testing.
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.

AUTHORITY

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.



David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

The applicable agency management's response is included as **EXHIBIT A**.

EXHIBIT A
MANAGEMENT'S RESPONSE

FLORIDA DEPARTMENT of management SERVICES
We serve those who serve Florida

4050 Esplanade Way
Tallahassee, FL 32399-0950
Tel: 850-488-2786 | Fax: 850-922-6149

Rick Scott, Governor

Craig J. Nichols, Agency Secretary

April 10, 2014

Mr. David W. Martin, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Martin:

Pursuant to subsection 11.45(4)(d), Florida Statutes, this is our response to your report, ***Information Technology Operational Audit-Surplus Information Technology Property Controls***. Our response corresponds with the finding and recommendation related to the Department of Management Services contained in the draft report.

If further information is needed concerning our response, please contact Walter Sachs, Inspector General, at 488-5285.

Sincerely,

Craig J. Nichols
Agency Secretary

Attachment

cc: Erin Rock, Chief of Staff
Stacy Arias, Deputy Secretary, Business Operations
Debra Forbess, Director, Administration
Linda Allbritton, Chief Information Officer
Mitchell Clark, Chief, Bureau of Financial Management Services
Walter Sachs, Inspector General
Yolanda Lockett, Audit Director

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

FLORIDA DEPARTMENT of management SERVICES
We serve those who serve Florida

4050 Esplanade Way
Tallahassee, FL 32399-0950
Tel: 850-488-2786 | Fax: 850-922-6149

Rick Scott, Governor

Craig J. Nichols, Agency Secretary

Department of Management Services' Response
To the Auditor Generals' Information Technology Operational Audit

Surplus Computer Hard Drive Disposal Processes

Finding No. 2: Surplus Computer Hard Drive Sanitization Documentation
DMS lacked adequate documentation regarding the sanitization of surplus computer hard drives.

Recommendation:
DMS should document, in accordance with established policy, the sanitization of surplus computer hard drives before disposal of the computers.

Response:
☒**Concur**
☐**Non-Concur**

DMS has updated its property disposal form to document and track the sanitization of surplus computer hard drives by including the following information:

a) Date sanitization occurred
b) Name (*technician who removed the hard drive*)
c) Method of sanitization