New York State Office of the State Comptroller
Thomas P. DiNapoli

Division of State Government Accountability

Disposal of Electronic Devices

State University of New York at Albany

Report 2012-S-40 September 2013

Executive Summary

Purpose

To determine if electronic devices being surplused by the State University of New York at Albany (University at Albany) through the Office of General Services (OGS) are permanently cleaned of all data, including personal, private and sensitive information. The audit covers the period of January 1, 2012 through May 26, 2012.

Background

Office of Cyber Security Policy requires all State entities to establish formal processes to address the risk that personal, private or sensitive information may be improperly disclosed. One way information can be compromised is through careless disposal of electronic devices. This policy also requires that all laptops containing, or with access to, State information must be encrypted. Agencies can dispose of electronic devices on their own; however, OGS' Surplus Unit provides this service for many State agencies. Agencies are required to remove all information prior to disposal and, if sending them to OGS, to certify in writing that the devices no longer contain any retrievable information. OGS' Surplus Unit does not accept any responsibility for clearing the data from these devices. At the time of our audit, the University at Albany had 36 electronic devices ready for disposal through OGS' Surplus Unit.

Key Findings

- Seven of the 36 computer hard drives readied for surplus still contained data, even though University at Albany had provided OGS with certifications indicating all information had been removed.
- Two of these hard drives contained personal, private and/or sensitive information including social security numbers, dates of birth, home addresses and financial information. One of these two hard drives also contained potentially inappropriate photographs that could be considered offensive for the work place.
- The other five hard drives also contained retrievable data that included resumes, personal vacation photos, research information and student term papers.
- One of the seven hard drives was taken from a laptop computer, which should have required more stringent security controls and been encrypted.

Key Recommendations

- Reinforce policies and procedures to ensure that all information is removed from electronic devices prior to authorizing the equipment for surplus.
- Ensure that all data on laptop computers is encrypted.

Other Related Audits/Reports of Interest

Office of General Services: Disposal of Electronic Devices (2012-S-04)
Office for the Aging: Disposal of Electronic Devices (2012-S-39)

Office of the State Comptroller
State of New York

Division of State Government Accountability

September 4, 2013

Dr. Robert J. Jones
President
State University of New York at Albany
1400 Washington Avenue
Albany, NY 12222

Dear Dr. Jones:

The Office of the State Comptroller is committed to helping State agencies, public authorities and local government agencies manage government resources efficiently and effectively and, by so doing, providing accountability for tax dollars spent to support government operations. The Comptroller oversees the fiscal affairs of State agencies, public authorities and local government agencies, as well as their compliance with relevant statutes and their observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations. Audits can also identify strategies for reducing costs and strengthening controls that are intended to safeguard assets.

Following is a report of our audit entitled *Disposal of Electronic Devices*. This audit was performed according to the State Comptroller's authority under Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law.

This audit's results and recommendations are resources for you to use in effectively managing your operations and in meeting the expectations of taxpayers. If you have any questions about this report, please feel free to contact us.

Respectfully submitted,

Office of the State Comptroller
Division of State Government Accountability

Table of Contents

State Government Accountability Contact Information:
Audit Director: John Buyce
Phone: (518) 474-3271
Email: StateGovernmentAccountability@osc.state.ny.us
Address:
Office of the State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

This report is also available on our website at: www.osc.state.ny.us

Background

In today's electronic age, unauthorized disclosure of personal, private and sensitive information has become an extremely high-risk area. Various laws and regulations, including the State Technology Law, impose strict requirements on organizations to properly safeguard the information they collect.

In New York, Office of Cyber Security Policy requires all State entities to establish formal processes to address the risk that personal, private or sensitive information may be improperly disclosed through careless disposal or re-use of electronic devices. Personal computers, tablets and smart phones pose a particular concern because they can easily be returned to the manufacturer or sold to the public while still containing personal identifiable information. The policy therefore requires that all electronic media (i.e. hard drives and other memory components) in these devices be securely overwritten or physically destroyed to prevent the unauthorized disclosure of sensitive information. This policy also requires that all laptops containing, or with access to, State information must be encrypted.

Some organizations must also comply with additional provisions of laws applicable to their specific type of business. For example, the federal Gramm-Leach-Bliley Act imposes certain requirements on organizations that deal with individual financial services, including colleges and universities that participate in student loan programs. Organizations that deal with medical services – including student health clinics – must also comply with privacy provisions of the Health Insurance Portability and Accountability Act.

Agencies can dispose of electronic devices on their own. However, the OGS Surplus Unit provides this service for many State agencies. The Surplus Unit does not always take physical custody of the equipment, but instead arranges for the sale or transfer directly by the owner agency. The Surplus Unit does not assume responsibility for removing information from electronic devices or testing devices to ensure information has been removed. Instead, it requires each agency to remove all information and to certify, in writing, that they have done so prior to sending an item for disposal. Once an item is ready for surplus, the Surplus Unit will offer electronic devices for reuse to State agencies and public authorities, then to municipalities and then to school districts. If the items are not transferred to these entities, the Surplus Unit will make them available for sale to the public.

Audit Findings and Recommendations

Removal of Information

During February and March 2012, we tested all hard drives from 36 computers that the University at Albany had readied for surplus disposal by OGS. Fourteen of these devices had been physically transferred to the OGS warehouse facility, while the other 22 were still housed at the University at Albany. Although the University at Albany had certified to OGS that each device had been wiped clean, seven hard drives (19 percent) still contained retrievable data. Two of those hard drives contained personal, private and/or sensitive information including social security numbers, dates of birth, home addresses and financial information. One of these two hard drives also contained potentially inappropriate photographs that, although not pornographic in nature, could be considered offensive for the work place. The other five hard drives also contained retrievable data that included resumes, personal vacation photos, research information and student term papers. One of the seven hard drives was taken from a laptop computer, which should have required more stringent security controls and been encrypted.

We reviewed the University at Albany's method for preparing equipment for surplus and found it to be appropriate, if followed. The University at Albany's procedures state that each department is responsible for removing data from electronic devices. The Information Technology staff assigned to each department performs this function and the data is supposed to be overwritten by using wiping software. Subsequently, the Information Technology staff signs off on the equipment record certifying that the device has been wiped clean and can be surplused.

Properly applied, University at Albany's method provides some assurance that information will not be improperly disclosed. However, this assurance is not absolute. As demonstrated by our audit tests of surplus electronic devices, there is always a risk that errors may occur. We met with the Information Technology staff member who signed off on several of the computers that still contained data and learned that no record is maintained of who actually removes the data from each device. Officials informed us that the data wiping process is most often done by computer science students whose work is not verified. Officials theorized that, due to the confined space where the wiping takes place and the short turnaround time expected, it is very possible that some devices were mistakenly certified.

Officials agreed to reinforce their procedures and to consider retaining records to show who actually prepares each device for surplus. However, these measures are still dependent on compliance. Ultimately, removing and destroying a hard drive appears to be the most reliable way of limiting this risk. In light of the potential impact of improper disclosures, at a minimum, we believe this should be done before devices are offered for sale to the public.

Recommendations

1. Reinforce policies and procedures to ensure that all information is removed from electronic devices prior to authorizing the equipment for surplus.

2. Ensure that all data on laptop computers is encrypted.

Audit Scope and Methodology

The objectives of our audit were to determine if electronic devices being surplused had been permanently cleaned of all personal, private and sensitive information, and also whether the University had developed formal processes to minimize the risk of unauthorized disclosure of such information when disposing of its equipment. The audit covers the period of January 1, 2012 through May 26, 2012.

To accomplish our audit objectives, we reviewed relevant industry standards, State laws and agency policies and procedures. We also interviewed representatives of the University at Albany to gain an understanding of their policies and procedures for disposal of electronic devices. We tested all 36 hard drives from computers which the University at Albany had readied and listed for surplus with OGS. Using forensic software, we examined the contents of electronic media contained in these devices while taking steps to ensure that the actual data was unaffected by our testing. For the seven hard drives we found with retrievable data, we reviewed and analyzed the data to determine whether it contained sensitive information.

We conducted our performance 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.

In addition to being the State Auditor, the Comptroller performs certain other constitutionally and statutorily mandated duties as the chief fiscal officer of New York State. These include operating the State's accounting system; preparing the State's financial statements; and approving State contracts, refunds, and other payments. In addition, the Comptroller appoints members to certain boards, commissions and public authorities, some of whom have minority voting rights. These duties may be considered management functions for purposes of evaluating organizational independence under generally accepted government auditing standards. In our opinion, these functions do not affect our ability to conduct independent audits of program performance.

Authority

This audit was done according to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law.

Reporting Requirements

A draft copy of this report was provided to State University of New York at Albany officials for their review and comment. Officials agreed with our recommendations and reported having already taken steps to implement them. A copy of their response is included at the end of this report.

Within 90 days after final release of this report, as required by Section 170 of the Executive Law, the President of the State University of New York at Albany shall report to the Governor, the State Comptroller, and the leaders of the Legislature and fiscal committees, advising what steps were taken to implement the recommendations contained herein, and where the recommendations were not implemented, the reasons why.

Contributors to This Report

John Buyce, Audit Director
Walter Irving, Audit Manager
Bob Mainello, Audit Supervisor
Lynn Freeman, Examiner-in-Charge
Scott Heid, Examiner-in-Charge
Richard Podagrosi, Examiner-in-Charge
Corey Harrell, Supervisor, Information Technology Specialist
Thierry Demoly, Staff Examiner
Michele Krill, Staff Examiner
Alphonso Boyd, Information Technology Specialist
Jared Hoffman, Information Technology Specialist
Sue Gold, Report Editor

Agency Comments

UNIVERSITY AT ALBANY
State University of New York

Division of Finance and Business
Office of the University Controller

August 2, 2013

Mr. Bob Mainello
Office of the State Comptroller
110 State Street, 11th Floor
Albany, NY 12236

Dear Mr. Mainello:

Please find below the official response from the University at Albany to the Office of the State Comptroller Audit Report 2012-S-04, Disposal of Electronic Equipment.

The University at Albany accepts the findings of the Office of the State Comptroller (OSC) included in Audit Report 2012-S-04, Disposal of Electronic Equipment. The University agrees with OSC that the tolerance level for personal, private or sensitive information (PPSI) remaining on electronic devices at the time of disposal or surplus must be zero.

The University has accomplished zero tolerance for PPSI remaining on electronic devices being disposed by contracting for all hard drives on these devices to be shredded prior to disposal of the devices. Further, the University has a procedure whereby all University departments and offices are required to wipe hard drives clean on all devices to be disposed or made available for surplus using University provided software. The devices cited in OSC Audit Report 2012-S-04 all came from the same University department who had not run the wiping software process properly, thus inadvertently leaving PPSI on the devices. In addition, it is the policy of the University that PPSI not be placed on electronic device hard drives and rather be stored on servers that are firewall protected within the University network.

As a result of the findings in OSC Audit Report 2012-S-04, the University has retrained the offending department on both the University policy regarding not storing PPSI on individual electronic device hard drives and how to properly wipe date from electronic device hard drives prior to disposal or surplus. In addition, the University is exploring a more centralized and dependable approach to wiping the hard drives of electronic devices prior to disposal or surplus to insure that no PPSI remains on the device. While resources to dedicate staff to these tasks simply are not available at this time, the University will continue to search for an alternative method of providing this service.

The University appreciates the cooperation and insight shown by OSC during this audit.

Sincerely,

Kevin C. Wilcox
Associate Vice President and Controller

Cc: President Jones
Mr. Kane
Mr. Walser

University Hall, Room 212
1400 Washington Avenue, Albany, New York 12222
PH: 518-956-8120 FX: 518-956-8121
www.ualbany.edu