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

Division of State Government Accountability

Disposal of Electronic Devices

Office of General Services

Report 2012-S-4 December 2012

Executive Summary

Purpose

To determine if electronic devices being surplused through the Office of General Services (OGS) are permanently cleaned of all data, which may include personal, private and sensitive information, and whether State entities using this service have developed formal processes to minimize the risk of disclosure of information when disposing of devices storing this type of information. The audit covers the period of January 1, 2012 through March 26, 2012.

Background

The New York State Office of Cyber Security's Policy requires all State entities to establish formal processes to address the risk that information may be improperly disclosed. One way information can be compromised is through careless disposal of electronic equipment. Agencies can dispose of electronic devices on their own; however OGS' Surplus Unit disposes of them 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 information. OGS' Surplus Unit does not accept any responsibility for clearing the data from these devices. However, OGS' Information Resource Management (IRM) bureau provides information technology support for some State agencies. In these cases, IRM is responsible for removing information from the devices prior to making them available to the Surplus Unit. At the time of our audit, the Surplus Unit had 429 electronic devices in its possession for disposal.

Key Findings

- OGS IRM was responsible for removing information from 25 of the devices on hand, which had been previously assigned to the Division of Veterans Affairs. Of these, three did not have information completely removed (12 percent). One of the three devices still had sensitive information on a hard drive, including multiple social security numbers, medical records and confidential human resource information.
- Through physical inspection and the use of forensic software, we determined the other agencies had used various means to properly eliminate all information from their devices, in some cases by physically removing the hard drives.

Key Recommendation

Work with the Office of Cyber Security to better safeguard information by requiring hard drives to be removed from all electronic devices prior to sale to the public.

Other Related Audits/Reports of Interest

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

New York State
Office of the State Comptroller

Division of State Government Accountability

December 6, 2012

RoAnn M. Destito
Commissioner
Office of General Services
Corning Tower, 41st Floor
Empire State Plaza
Albany, New York 12242

Dear Commissioner Destito:

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

The New York State Office of Cyber Security's Policy requires all State entities to establish formal processes to address the risk that personal, private or sensitive information may be improperly disclosed. Information can be compromised through careless disposal or re-use of electronic devices. As a result, all data should be removed. 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 information. Therefore, the policy requires that all hard drives and other memory components in these devices be securely overwritten or physically destroyed.

Standards for safeguarding sensitive information also exist by industry. For example, because of loan servicing activities, some schools are subject to the Federal Gramm-Leach-Bliley Act, which focuses on personal financial information. Agencies with access to individuals' medical history and information must meet strict requirements established by the Health Insurance Portability and Accountability Act.

Agencies can dispose of electronic devices on their own. However, the Office of General Services' (OGS) Surplus Unit disposes of surplus electronic devices for many State agencies. 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. In some cases, OGS' Information Resource Management (IRM) bureau provides shared administrative support services for State agencies, such as human resources or information technology services. This is known as "hosting." Only when IRM is responsible for providing information technology support services is OGS responsible for the removal of data from devices prior to disposal.

Once received, 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 Recommendation

Removal of Information

We examined OGS' compliance with procedures designed to protect against improper disclosure of information for 429 electronic devices that the Surplus Unit had in its possession and available for disposal at the time of our field visits in February and March 2012. These devices had been transferred to OGS by five State agencies and one public authority. OGS had agency certifications on hand for all 429 devices indicating that all information had been removed. (OGS also had another 14 computers in its physical possession that had been transferred from the State University of New York at Albany. Because the University also had another 22 computers ready for disposal that had not been physically transferred to OGS, we excluded these devices from the scope of this audit and opted instead to examine and report on these 36 computers separately.)

Twenty-five of the devices on hand came from the Division of Veterans Affairs; an agency for which OGS provides information technology services through a hosting arrangement. OGS' IRM staff was therefore responsible for ensuring that information was properly removed from these 25 devices. We found three of these devices had not been properly cleansed, even though OGS records indicated all information had been removed from each unit. One of these devices contained sensitive information related to individual veterans that was easily viewed by our auditors including names, addresses, social security numbers and, in some cases, medical records. The file structures had been removed from the hard drives in the two other devices; however each still contained data. The data had not been overwritten or erased, but was generally not retrievable.

We reviewed IRM's process for preparing equipment for surplus and found it to be appropriate, if followed. IRM can process up to three computers at one time using appropriate software that overwrites the entire contents of each hard drive multiple times making any files unusable. Each computer is then logged as being wiped clean. IRM management determined that the problems we uncovered occurred due to simple human error, in one case when a technician mistakenly missed a secondary hard drive during the wiping process. They indicated that a computer with a secondary hard drive is rare in OGS' environment. Management acted quickly to address the error by reminding all staff of the importance of completeness and accuracy, and indicated they will consider adding an additional step to their process to require independent verification.

For the other 404 devices on hand, we examined the certifications submitted to OGS by the agencies and then tested compliance through physical inspection and the application of forensic software capable of recovering hidden data. Our tests did not identify additional problems, but showed that the five entities had used a variety of processes to protect their data, as follows:

- The Commission on Public Integrity had transferred six Blackberries and one cell phone for disposal, all of which had been reset to factory standards.
- The Hudson River Valley Greenway Commission had also reset its two Blackberries to factory standards.
- The Executive Chamber used appropriate software to remove the file structure and

encrypt any residual data on the 243 computers it transferred.
- The Department of Homeland Security and Emergency Services certified that it had removed the hard drives from the 148 devices it transferred, and would destroy these devices separately.
- The Adirondack Park Agency also removed the hard drives from the four electronic devices it transferred to OGS.

Properly applied, each of these methods provides assurance that information will not be improperly disclosed. However, this assurance is not absolute. As the computer from Veterans Affairs shows, there is always a risk that errors may occur. 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.

Recommendation

1. Work with the Office of Cyber Security to better safeguard information by requiring hard drives to be removed from all electronic devices prior to sale to the public.

   (In responding to our draft report, OGS officials agreed that the risk of releasing private information outweighs the extra expense that a purchaser may incur to replace a hard drive and announced their plans to immediately begin removing hard drives from surplus devices.)

Audit Scope and Methodology

The objectives of our audit were to determine if electronic devices being surplused through OGS are permanently cleaned of all data, which may include personal, private and sensitive information, and whether State entities using this service have developed formal processes to minimize the risk of disclosure of information when disposing of devices storing this type of information. The audit covers the period of January 1, 2012 through March 26, 2012.

To accomplish our audit objectives, we reviewed relevant industry standards, State laws and agency policies and procedures. We also interviewed representatives of OGS, and other State agencies that had surplus equipment at the time of our audit, to review their policies regarding their disposal of electronic devices. We physically examined the electronic devices on hand at the Surplus Unit. 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 one hard drive that we found had readable files, we reviewed and analyzed the data to determine whether it contained sensitive information. In some cases, we were able to limit our testing based on our observations and the results of our forensic software tests.

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 Office of General Services officials for their review and comment. Their comments, which were in general agreement with our findings, were considered in preparing this report and are attached in their entirety at the end of this report.

Within 90 days of the final release of this report, as required by Section 170 of the Executive Law, the Commissioner of the Office of General Services 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 recommendation contained herein, and where the recommendation was 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, Supervising 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

Division of State Government Accountability

Andrew A. SanFilippo, Executive Deputy Comptroller
518-474-4593, asanfilippo@osc.state.ny.us

Elliot Pagliaccio, Deputy Comptroller
518-473-3596, epagliaccio@osc.state.ny.us

Jerry Barber, Assistant Comptroller
518-473-0334, jbarber@osc.state.ny.us

Vision

A team of accountability experts respected for providing information that decision makers value.

Mission

To improve government operations by conducting independent audits, reviews and evaluations of New York State and New York City taxpayer financed programs.

Agency Comments

ANDREW M. CUOMO
GOVERNOR

STATE OF NEW YORK
EXECUTIVE DEPARTMENT
OFFICE OF GENERAL SERVICES
MAYOR ERASTUS CORNING 2ND TOWER
THE GOVERNOR NELSON A. ROCKEFELLER EMPIRE STATE PLAZA
ALBANY, NEW YORK 12242

ROANN M. DESTITO
COMMISSIONER

November 7, 2012

Mr. John Buyce
Audit Director
Office of the State Comptroller
110 State Street, 11th Floor
Albany, New York 12236

Dear Mr. Buyce:

This letter is a response to your Audit 2012-S-4 conveying the results of your audit of the Disposal of Electronic Devices. The Office of General Services (OGS) agrees that the breakdown in our process that allowed three computers with hard drives which had not been wiped clean of data to be released for sale is unacceptable. OGS believes that our process was adequately designed but human error resulted in the computers not being wiped. To address the issue presented in the preliminary audit, OGS immediately instituted a number of changes in the process through which devices must be subjected to prior to being surplussed. The recommendation in your final report has changed to require all hard drives be removed prior to sale to the public. Upon receiving this new recommendation, OGS began evaluating how to implement such a process and the impact it would have on the ability to reuse computers handled by our surplus property program. Our response is in two parts, the first outlining our actions related to the new recommendation and the remainder dealing with the process improvements put in place as a result of the preliminary audit.

The recommendation to remove and shred hard drives before selling computers will result in significant changes in our State Surplus Property Program. To assess whether to implement the recommendation, OGS sought input from the Department of Homeland Security and Emergency Services. They concur that physical destruction of hard drives is the most reliable means of preventing data from being released but acknowledged that there are secure methods of deleting files using software to overwrite drives with random characters but these are more prone to failure than physical destruction of the drive.

The highest priority in the surplus program is to place surplus equipment back into service with another agency or to donate computers to schools through the CREATE program. Removal and shredding the hard drive will lower the reuse potential of computers because the receiving agency would need to purchase new hard drives. Further it is our experience that many computers are damaged when hard drives are removed by agencies that currently remove hard drives. This would impact the agencies that obtain computers from the program as well as a program that provides school districts with surplus computers for use in their educational program. After further consideration of the issue, OGS has determined that the risk of release of private information outweighs the extra expense to a school or agency to purchase hard drives. Therefore, beginning immediately, OGS will begin to remove and shred all hard drives prior to sending them to our Surplus Property Unit. OGS will issue new guidelines to agencies requiring that they also remove and shred hard drives before the surplus computers are transferred to OGS.

The remainder of the response relates to the findings in the report and the process improvements currently in place. The improvements will address concerns that will have arisen if laptops containing sensitive information are lost or stolen. OGS supports the Division of Veterans' Affairs (DVA) in all of their IT needs, including the outfitting and surplussing of PCs and laptops. DVA staff work with veteran documents that contain personal, private or sensitive information (PPSI) on a daily basis and therefore have the highest risk of PPSI data being left behind on a PC. To address this higher level of risk, OGS started encrypting the hard drives of all DVA desktops deployed in 2012 and all laptops in use. The encryption of DVA hard drives will prevent PPSI data from being accessed in the event of the theft of a computer or a mistake like this.

The last change to our process added a second person to verify that the hard drive has in fact been removed prior to shipment to OGS Surplus Property.

These changes to our process will improve our controls and ensure that all computers are wiped. We would like to thank the auditors for their work on this effort. OGS is committed to protecting data from access and the results of this audit have resulted in improvements to our processes. If you have additional questions or comment please contact Robert Curtin at Robert.Curtin@ogs.ny.gov or (518) 474-5090.

Sincerely,

RoAnn M. Destito

RoAnn M. Destito

cc: F. Hecht
K. Baxter
R. Curtin

2