



# REVIEW OF SURPLUS PROCEDURES FOR ELECTRONIC DEVICES WITH STORAGE

OCTOBER 2014

Auditor of Public Accounts  
Martha S. Mavredes, CPA

[www.apa.virginia.gov](http://www.apa.virginia.gov)

(804) 225-3350



## EXECUTIVE SUMMARY

Sensitive data in the Commonwealth of Virginia is at an increased risk of compromise through the sale of retired electronic devices with storage. Our review of Commonwealth electronic devices posted for sale on Govdeals.com where the agency is responsible for sanitizing information found the following.

- **Agencies cannot verify sanitization for devices in five of nine selected “high-risk” advertisements.** We selected nine advertisements on Govdeals.com that we consider “high-risk” because the advertisements *do not* specifically indicate that sanitization occurred.
- **Agencies cannot verify sanitization of devices in eight of 22 (36 percent) sampled “low-risk” advertisements.** We sampled 22 advertisements on Govdeals.com that we consider “low-risk” because the advertisements specifically indicate that sanitization occurred.

Additionally, sanitization responsibility for some Commonwealth owned devices rests with the IT Infrastructure Partnership. Our sanitization review of these devices found the following.

- **The IT Partnership cannot verify sanitization of Commonwealth data for nine of 40 devices (23 percent) before asset transfer or sale.**

Lastly, our physical inspection of devices transferring to the Department of General Services (DGS) warehouse found the following.

- **Agencies did not sanitize one of 42 devices prior to sending it to DGS for sale on Govdeals.com.**

There are also inconsistencies between the Commonwealth’s sanitization standard, SEC514, and the Commonwealth’s information security standard, SEC501. Some of these inconsistencies may cause confusion for agencies as SEC501 is on its sixth update since the last SEC514 update in March 2008. The Commonwealth’s sanitization standard is also not providing sufficient guidance to agencies when compared to industry best practices. Based on our review and findings, we have the following recommendations.

**RECOMMENDATION #1:** We recommend that the Virginia Information Technologies Agency (VITA) review and update the Commonwealth’s data removal standard, SEC514, on a more frequent basis to ensure it provides adequate guidance to agencies and that the Commonwealth’s data sanitization requirements align with industry best practices, such as the National Institutes of Science and Technology Special Publication 800-88 standard.

**RECOMMENDATION #2:** We recommend that VITA update the Commonwealth's data removal standard to include a requirement for agencies to assign sanitization responsibility to one operational position within the organization.

**RECOMMENDATION #3:** We recommend that VITA perform interim corrective action plan reviews between IT Infrastructure Partnership operational audits. The next operational audit that focuses on data sanitization and media surplus is in July 2015 and to ensure that the Partnership is addressing concerns identified in previous audits, VITA should consider reviewing implementation of the corrective action plan from 2013 to ensure timely implementation and to reduce the risk of data compromise.

## –TABLE OF CONTENTS–

	<u>Pages</u>
EXECUTIVE SUMMARY	
BACKGROUND	1-2
STUDY OBJECTIVES AND METHODOLOGY	3-4
REVIEW OF THE COMMONWEALTH DATA REMOVAL STANDARD	5
DATA REMOVAL PROCEDURE TESTS	6-9
LEASED ELECTRONIC MEDIA CONTRACT REVIEW	10
DISCLAIMER	11
TRANSMITTAL LETTER	12
APPENDIX A: THE COMMONWEALTH’S ELECTRONIC MEDIA SANITIZATION PROCESS	13-14
APPENDIX B: SEC 514-03 REQUIREMENTS SUMMARY	15
RESPONSIBLE OFFICIAL’S RESPONSE	16
RESPONSIBLE OFFICIALS	17

## BACKGROUND

The Auditor of Public Accounts (APA) reviewed data removal procedures in 2003 and released the report “Special Review – Surplus Computer Equipment Data Removal.” The 2003 review found that because there were so many different methods of retiring old equipment, the rapidly changing pace of technology, and because no Commonwealth electronic media surplus and sanitization standard existed, the Commonwealth was exposing itself to an elevated risk of confidential data being compromised. It was because of these findings that APA recommended that the Virginia Information Technologies Agency (VITA) create a media surplus and data sanitization standard for the Commonwealth.

In responding to the 2003 review, VITA created the *Removal of Commonwealth Data from Electronic Media Standard, SEC514*, which at its last update in 2008 was on its third iteration. It is the intent of this standard to provide the appropriate requirements and guidance to the Commonwealth’s executive, legislative, and judicial branches, and independent agencies and institutions of higher education (agencies) when electronic media is retired from the organization. The standard defines electronic media as devices with memory, such as the hard drives of personal computers, servers, mainframes, personal digital assistants (PDAs), routers, firewalls, switches, tapes, diskettes, CDs, DVDs, cell phones, printers, and universal serial bus (USB) data storage devices (see Appendix B for more information).

While SEC514’s scope encompasses all agencies, certain institutions of higher education are exempt from following the Commonwealth’s information technology (IT) standards. However, in their agreement with the General Assembly, the exempt institutions are responsible for implementing reasonable controls to protect citizens’ data.

Additionally, in the Commonwealth’s Comprehensive Infrastructure Agreement with Northrop Grumman (NG), also known as the IT Infrastructure Partnership, all equipment that was previously operated and maintained by the Commonwealth, but is now operated and maintained by NG, is to be sanitized by NG before being retired or transferred per the requirements in SEC514.

Similarly, vendors that lease devices to the Commonwealth are responsible for sanitizing these devices upon the termination of the lease and provide the agency with sanitization certificates.

The Department of General Services (DGS) receives all Commonwealth-owned retired devices. DGS determines whether the device is fit for recycling by sale or by destruction. If the device is fit for sale, DGS then acts as an agent to facilitate the sale of the device and puts the device up for bid on a liquidity services marketplace website, Govdeals.com. The public is then able to bid on the device with the goal of the Commonwealth recouping some of its initial investment in the device (see a full explanation of the process in Appendix A).

The removal of data from retired or returned leased devices is an especially relevant concern today as identity theft is increasing. Device memory capacity is also steadily increasing and is now making it possible to store a terabyte worth of information on a device smaller than a thumb (see figure 1). A terabyte worth of information is equivalent to 4.5 million 200-page books.



*Figure 1 - A 1 terabyte USB storage device measuring 2.8" x 1.1" x 0.8"*

The increasing storage capacity of both small (USB storage devices) and large (desktops) devices increases information proliferation. This increases the risk of duplicating confidential information on storage devices that typically may not store this type of information. It is therefore very important that those charged with removing Commonwealth data from storage devices do so according to standards and industry best practices.

## STUDY OBJECTIVES AND METHODOLOGY

We performed this review with the following objectives to determine whether:

- the Commonwealth's data removal standard, SEC 514-03, follows industry best practices and provides adequate guidance to agencies for data sanitization;
- agencies are appropriately sanitizing electronic media storage devices prior to retiring equipment or equipment end-of-lease return; and
- the Commonwealth's contracts for leased equipment with electronic media storage contains adequate language to require data removal certification for returned equipment.

In performing the review, we gained an understanding over the Commonwealth's data removal standard, SEC 514-03, and compared it against an industry best practice, National Institute of Standards and Technology (NIST) Special Publication 800-88, to determine if the standard is thorough enough to provide appropriate guidance for agencies to implement a reasonable data sanitization program. After the standard review and comparison, we reviewed the Commonwealth's contracts for sanitization services of leased equipment.

We then established a population of all of the Commonwealth's devices sold on the Govdeals.com auction website from April 2012 to April 2013. Based on a review of the population, we decided to divide the single population into two populations. One of the two populations included only devices with no language in the Govdeals.com advertisement indicating sanitization. We classified this population as high-risk and performed a judgmental selection for testing.

The other population included only devices with specific language in the Govdeals.com advertisement indicating sanitization. We classified this population as a low-risk population and performed a sample test.

Each of the populations were tested to determine if the related devices making up the total lot and its corresponding data was appropriately sanitized per the Commonwealth's standard and respective organizational policy. This was indicated by a completed sanitization certificate, if it was properly approved and signed off on by a supervisor, and if the certificate was completed in a timely fashion (prior to being posted on the Govdeals.com website as available for inspection) (see Appendix B).

NG is responsible for sanitizing the Commonwealth's legacy in-scope electronic assets that are at the end of useful life. After sanitization occurs, NG then transfers the assets to DGS for surplus and sale on Govdeals.com (see Appendix A). We requested a listing directly from NG of a population of all Commonwealth assets sanitized by NG from April 2012 to April 2013. Based on a review of the established population of the assets, a random sample was tested. This sample determined whether

NG appropriately sanitized the Commonwealth's equipment per the standard and policy. This was indicated by a completed sanitization certificate, if it was properly approved and signed off on by a supervisor, and if it was done so in a timely fashion (prior to being posted on the Govdeals.com website as available for inspection) (see Appendix B).

We also selected and tested Commonwealth devices with current and ongoing advertisements on Govdeals.com. This selection included the ongoing sales on the liquidity services marketplace website from May 2013 to July 2013. We tested these devices by conducting on-site inspection to determine if agencies had sanitized their hard drives prior to listing and auction.

We provide the results of our review and our conclusions relevant to the review objectives in the sections that follow.



## REVIEW OF THE COMMONWEALTH'S DATA REMOVAL STANDARD

The latest version of the Commonwealth's Removal of Commonwealth Data from Electronic Media Standard, SEC514, is dated and effective as of March 15, 2008. Since then, the Virginia Information Technologies Agency (VITA) has not performed an official review or updated the standard.

### Finding #1

VITA does not perform annual reviews of the data removal standard, SEC514, and has not updated the standard since March 2008.

Our review also found that the Commonwealth's data removal standard is not providing sufficient guidance to agencies compared to national standards, such as NIST Special Publication 800-88. We chose to compare the Commonwealth's data removal standard to the NIST standard to keep consistent with the Commonwealth's effort to incorporate NIST standards into its information security standard, SEC501. In comparing the two standards, we found that the Commonwealth's standard is lacking guidance in the following areas.

### Finding #2

The data removal standard, SEC514, does not identify some common devices that may store significant amounts of information, such as digital copy machines. Not including these common devices may result in agencies not including those as part of the sanitization process. (Reference: *NIST SP800-88: Media Sanitization Decision Matrix*)

### Finding #3

The data removal standard, SEC514, lacks a decision tree that can guide the agencies as to what sanitization method to use for different types of data classifications. (Reference: *NIST SP800-88: Sanitization and Disposition Decision Flow*, *NIST SP800-60: Potential Impact Levels*)

### Finding #4

The data removal standard, SEC514, lacks a discussion about how future technologies may impact the methods by which agencies sanitize devices. The rapid change in technologies prohibits standards from being up-to-date even with annual reviews and updates. (Reference: *NIST SP800-88: 2.3 Trends in Data Storage Media*)

Based on the findings in our review the Commonwealth's data removal standard, SEC514, we provide the following recommendation.

### Recommendation #1

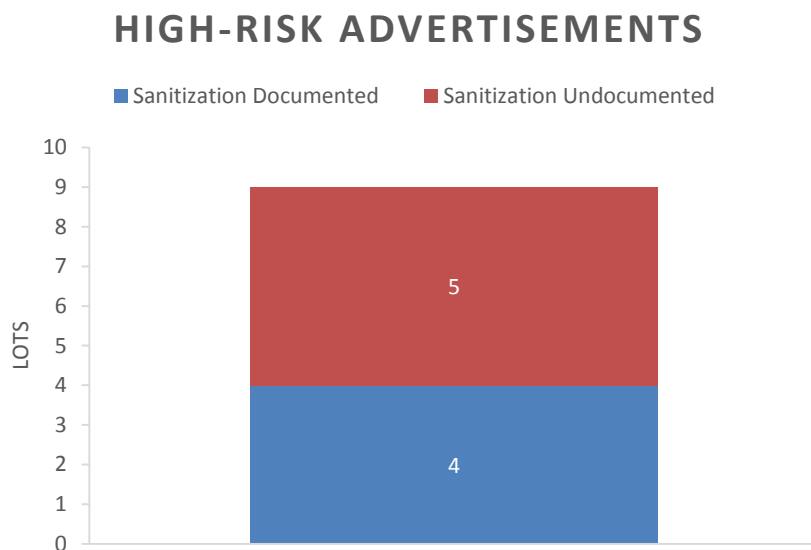
We recommend that the Virginia Information Technologies Agency (VITA) review and update the Commonwealth's data removal standard, SEC514, on a more frequent basis to ensure it provides adequate guidance to agencies and that the Commonwealth's data sanitization requirements align with industry best practices, such as the National Institutes of Science and Technology Special Publication 800-88 standard.

## DATA REMOVAL PROCEDURE TESTS

We conducted four tests to determine whether agencies and the IT Infrastructure Partnership (Partnership) could verify sanitization of retired equipment and in each test found instances where the agencies or Partnership could not verify device sanitization. We discuss the results of our tests in further detail below.

### **First Test – “High-Risk” Advertisement Selection**

The first test judgmentally selected nine advertisements that the Commonwealth sold through Govdeals.com between April 2012 and April 2013, with no mention of sanitization. We classified these advertisements as “high-risk” and found that the responsible agencies for five of the nine selected advertisements could not verify device sanitization.



#### **Finding #5**

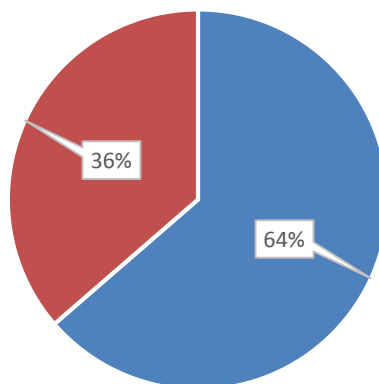
Agencies cannot verify sanitization of devices in five of nine judgmentally selected “high-risk” advertisements on Govdeals.com.

### **Second Test – “Low-Risk” Advertisement Sampling**

The second test randomly sampled 22 of 218 advertisements that the Commonwealth sold through Govdeals.com between April 2012 and April 2013 that specifically mention device sanitization. Agencies representing eight of 22 (36 percent) sampled advertisements could not verify device sanitization.

## LOW-RISK ADVERTISEMENTS

■ Sanitization Documented ■ Sanitization Undocumented



### Finding #6

Agencies cannot verify sanitization of devices in eight of 22 (36%) sampled “low-risk” advertisements on Govdeals.com.

### Third Test – On-site Physical Inspection

The third test included a selection of current devices for sale on Govdeals.com where 42 devices were available for physical inspection during the period May 2013 through July 2013. Each of the selected assets comprising the individual advertisements were tested via on-site inspection to determine if their hard drives had been sanitized prior to being listed for auction. We conducted the inspections on location at the respective agencies, as well as at the DGS warehouse.

The inspection found one device out of the 42 selected not sanitized. In this particular instance, the agency left a device previously used by law enforcement not sanitized and containing a Post-it note with a user name and password. The auditor conducting the investigation was able to gain full access to the information stored on the laptop using these credentials. Based on additional interviews with DGS employees, this was not an isolated incidence.

### Finding #7

One device of 42 selected was not sanitized before it was transferred to DGS for surplus.

### Recommendation #2

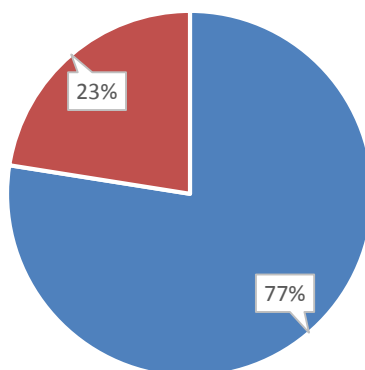
We recommend that VITA update the Commonwealth’s data removal standard to include a requirement for agencies to assign sanitization responsibility to one operational position within the organization.

#### **Fourth Test – IT Infrastructure Partnership**

The fourth test randomly sampled 40 of 356 devices that the IT Infrastructure Partnership (Partnership) retired between January 2012 and June 2013. The responsibility to sanitize these devices rests with the Partnership. The Partnership could not verify sanitization of nine of 40 (23 percent) devices.

### **IT INFRASTRUCTURE PARTNERSHIP SAMPLED DEVICES**

■ Sanitization Documented ■ Sanitization Undocumented



#### **Finding #8**

The IT Infrastructure Partnership cannot verify whether nine of 40 (23 percent) sampled devices were sanitized before sale or transfer.

Additionally, an independent audit firm performs periodic operational reviews over the Partnership's sanitization procedures. The last operational audit focusing on NG's media sanitization procedures covered devices retired from July 2012 to April 2013. The operational audit reached conclusions similar to APA's conclusions and determined that the IT Partnership service provider is not reasonably producing or maintaining sanitization certificates, nor completing the records on a timely basis.

Based on the results of the performed operational audit, the IT Partnership created a corrective action plan with an anticipated implementation date of December 2013. However, the Commonwealth's data remains at an increased risk of compromise because the Partnership has not scheduled the next operational audit with a focus on media surplus and data sanitization until July 2015.

#### **Finding #9**

The IT Infrastructure Partnership has not performed or scheduled an interim review of media sanitization procedures of the Partnership's service provider since July 2013. The next scheduled review over the related processes and controls will not begin until July 2015.

The scheduled follow-up review to test the controls implemented as part of the corrective action plan is too far apart from the original audit and increases the risk of the existence of non-functioning sanitization controls. Therefore, we provide the following recommendation.

#### **Recommendation #3**

We recommend that VITA perform interim corrective action plan reviews between IT Infrastructure Partnership operational audits. The next operational audit that focuses on data sanitization and media surplus is in July 2015 and to ensure that the Partnership is addressing concerns identified in previous audits, VITA should consider reviewing implementation of the corrective action plan from 2013 to ensure timely implementation and to reduce the risk of data compromise.

## LEASED ELECTRONIC MEDIA CONTRACT REVIEW

We reviewed the Commonwealth's contracts for leased equipment with electronic media storage and found that the contracts include language that adequately specifies data sanitization responsibilities between the Commonwealth and its vendors.

## DISCLAIMER

We omitted the names of the agencies and institutions of higher education used to test compliance with the Commonwealth's Removal of Commonwealth Data from Electronic Media Standard, SEC 514-03. The reason is twofold.

First, the main objective of this study is to determine whether the Commonwealth has a sufficient and updated standard. The purpose for testing agency and higher education implementation of this standard is to determine the adequacy and effectiveness of the standard and not individual implementation.

Second, identifying sanitization weaknesses at specific agencies in a public report provides a roadmap to where one can most likely find un-sanitized devices for sale. We determined that publishing such information would put the Commonwealth at an elevated risk of data compromise.

For those reasons, we withheld agency names from this public report per Code of Virginia Section 2.2-3705.2.



Martha S. Mavredes, CPA  
Auditor of Public Accounts

# Commonwealth of Virginia

*Auditor of Public Accounts*

P.O. Box 1295  
Richmond, Virginia 23218

October 30, 2014

The Honorable Terence R. McAuliffe  
Governor of Virginia

The Honorable John C. Watkins  
Chairman, Joint Legislative Audit  
and Review Commission

We have audited the Removal of Commonwealth Data from Electronic Media Standard, SEC514, and are pleased to submit our report entitled **Review of Surplus Procedures for Electronic Devices with Storage**. We conducted this 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.

## **Exit Conference and Report Distribution**

We discussed this report with Virginia Information Technologies Agency's management on November 3, 2014. Management's response to the findings identified in our audit is included in the section titled "Responsible Official's Response." We did not audit management's response and, accordingly, we express no opinion on it.

This report is intended for the information and use of the Governor and General Assembly, management, and the citizens of the Commonwealth of Virginia and is a public record.

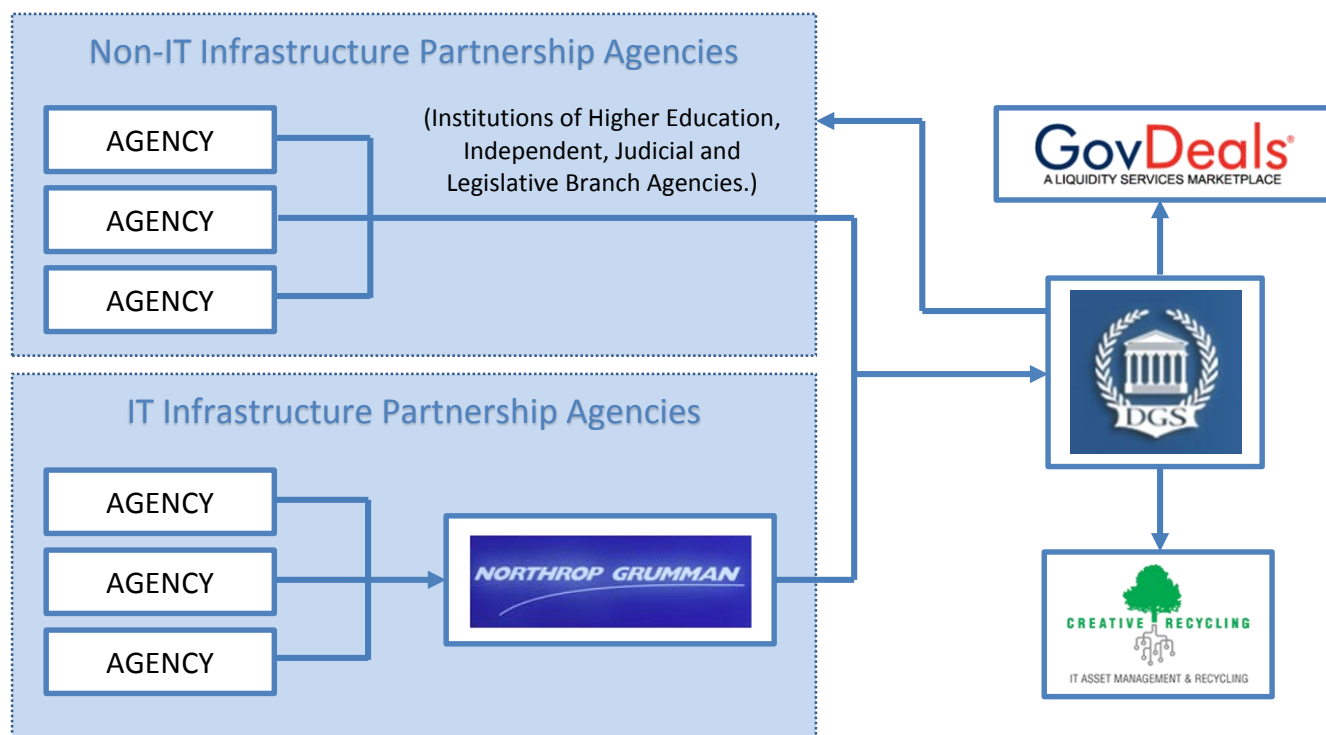
AUDITOR OF PUBLIC ACCOUNTS

GGG/alh



## APPENDIX A: THE COMMONWEALTH'S ELECTRONIC MEDIA SANITIZATION PROCESS

The Commonwealth's data sanitization process for devices that store information on electronic media is slightly different for agencies that participate in the IT Infrastructure Partnership (executive branch agencies) and all other agencies (institutions of higher education, independent, judicial and legislative branch agencies). The following is an illustration of how the Commonwealth processes retired devices.



### Non-IT Infrastructure Partnership Agencies

Agencies are responsible for sanitizing the devices they retire before they leave the agency and are transferred to the Department of General Services (DGS). While some institutions of higher education agencies are exempt from following the Commonwealth's data removal standard, these agencies have to establish a process that is following industry best practices for removing data from retired devices. Additionally, some devices are not physically transferred to DGS, but remain on the agency's property until either sold through Govdeals.com or recycled and destroyed through Creative Recycling.

### IT Infrastructure Partnership Agencies

Agencies are not responsible for sanitizing devices maintained by the Partnership. The Partnership is responsible for sanitizing devices before they leave the Partnership and are transferred

to DGS. The Partnership is responsible for establishing policies and procedures that follow the minimum requirements in the Commonwealth's data removal standard.

### **The Department of General Services**

DGS processes and receives sanitized retired devices from agencies and the IT Infrastructure Partnership (Partnership). DGS does not perform device sanitization. DGS will determine whether the Commonwealth should attempt to sell the device on Govdeals.com or destroy the device through Creative Recycling. Very few devices are reassigned and transferred to other non-Partnership agencies.

## APPENDIX B: SEC 514-03 REQUIREMENTS SUMMARY

The Commonwealth of Virginia's Removal of Commonwealth Data from Electronic Media Standard, SEC 514-03, prescribes recommended best practices for general data removal, and acceptable methods of hard drive data removal, including but not limited to overwriting, degaussing, and physical destruction.

Data overwriting is the replacement "of previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable, but the process must be correctly understood and carefully implemented."

Data degaussing "is a process whereby the magnetic media are erased, (i.e., returned to a zero state). Degaussing (demagnetizing) reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable."

SEC 514-03 also requires periodic internal quality assurance testing over the effectiveness of an agency's data removal process, as well as certification via approved party documentation that all surplus media has had its data effectively removed. This certification must include the type of equipment/media from which Commonwealth data is being removed, the date of removal, the methods utilized in the data removal, the name of the employee removing the data, as well as the name and signature of the employee's supervisor who removed the data. This documentation must be completed, maintained, and available for subsequent audit. Additionally, each piece of equipment must be affixed with a certificate of data sanitization before it leaves the organization and is transferred for surplus or sale.

The most important factor in preventing the release of sensitive information via sale or transfer of surplus equipment is strong control procedures at individual agencies before the equipment is retired. Agencies, in accordance with SEC 514-03, must have written policies and procedures for the preparation of equipment for sale or transfer. Agencies must implement these policies and procedures to ensure that equipment does not leave the organization without having been first sanitized of all Commonwealth data.



## COMMONWEALTH of VIRGINIA

Samuel A. Nixon, Jr.  
Chief Information Officer  
E-mail: [cio@vita.virginia.gov](mailto:cio@vita.virginia.gov)

**Virginia Information Technologies Agency**  
11751 Meadowville Lane  
Chester, Virginia 23836-6315  
(804) 416-6100

TDD VOICE -TEL. NO.  
711

October 31, 2014

Ms. Martha S. Mavredes, CPA  
Auditor of Public Accounts  
James Monroe Building  
Richmond, Virginia 23219

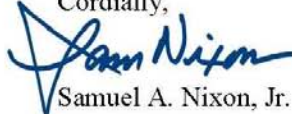
Dear Ms. Mavredes:

Thank you for the opportunity to comment on the *Review of Surplus Procedures for Electronic Devices with Storage*. The review presents findings and recommendations from Chuck Ross and his audit team based on their review of the process used to sanitize surplus electronic devices. On behalf of Virginia Information Technologies Agency (VITA) staff, I want to thank Mr. Ross and the Auditor of Public Accounts (APA) team for their thoroughness and professionalism during the review.

The review recommends that VITA update the Commonwealth's sanitization standard, SEC514, to clarify the processes that state agencies must follow when surplus electronic devices. The review also recommends that VITA more frequently review the process used by Northrop Grumman. We agree with these recommendations and will take steps to address them.

As the review also notes, the Commonwealth's primary Information Security Standard, SEC501, has been updated several times in recent years. These updates have been required to maintain the Commonwealth's alignment with best practices, including those adopted earlier this year by the National Institute of Standards and Technology. Unfortunately, as we have noted in previous reports, staffing constraints impede VITA's ability to fully accomplish its statutory responsibilities for IT security and risk management. However, in accordance with report's recommendations, I have directed VITA staff to update SEC514 as soon as possible and to evaluate how we can increase our reviews of Northrop Grumman's sanitation process.

Once again, I thank you for the opportunity to respond to the report.

Cordially,  
  
Samuel A. Nixon, Jr.

c: The Honorable Karen R. Jackson, Secretary of Technology

AN EQUAL OPPORTUNITY EMPLOYER

## RESPONSIBLE OFFICIALS

Karen R. Jackson  
Secretary of Technology

Samuel A. Nixon, Jr.  
Chief Information Officer of the Commonwealth

Judy A. Marchand-Hampton  
Executive Director, Relationship Management and Governance

Michael J. Watson  
Chief Information Security Officer of the Commonwealth

Chadwick P. Wirz  
Executive Director, Service Management and Delivery