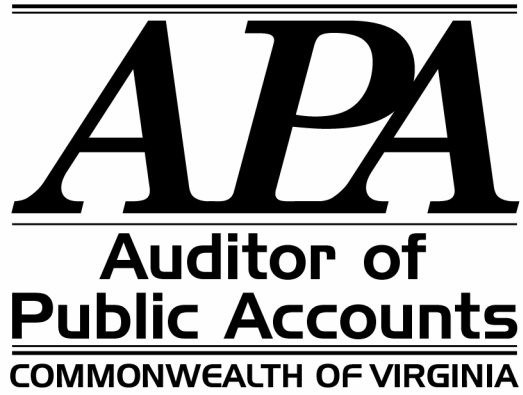
SPECIAL REVIEW - SURPLUS COMPUTER EQUIPMENT DATA REMOVAL

SPECIAL REPORT

OCTOBER 2003



AUDIT SUMMARY

We found sensitive information such as vaccination records, personnel records, credit card numbers, and more on computer equipment ready for auction by the Commonwealth. The Commonwealth regularly sells off old used computer equipment or, in some cases, has private vendors dispose of the computer equipment. The Commonwealth does not have a policy or standard to erase the hard drives before disposing of used equipment.

Our audit included a review of the Commonwealth's policies and the procedures to implement these policies by reviewing seven agencies and one institution of higher education. In addition we tested several computers and hard drives that were ready for sale or transfer to determine if personnel had followed the proper procedures for data removal. We found severe weaknesses that could lead to sensitive data being released or having already been released.

Our review of laptop and desktop computers ready for auction found that they contained the following information.

- Vaccination information;
- Women Infant and Children (WIC) personal information;
- Personnel evaluations of individuals;
- Personnel records of grievances of individuals;
- Scholastic evaluations of individually identifiable students; and
- Personal credit card number of a Dean of a college.

Our recommendations include the following.

- Agency personnel should immediately inspect all computer technology slated for sale or transfer to determine that personnel have removed all data from devices in such a manner that will prevent ready reading or reading by using utility software.
- The Virginia Information Technologies Agency (VITA) should create a policy and procedure which defines the responsibility for the removal of data before sale or transfer of surplus equipment.
- VITA should create a data removal or disk cleaning standard for all agencies and institutions. These standards should make use of disk cleansing utilities or require the destruction of hard drives. Mere formatting of hard drives is insufficient in most cases.
- The Chief Information Officer or designated Information Security Officer of each agency should create an audit function to randomly test equipment that is ready for public auction or transfer.

- T A B L E O F C O N T E N T S -

SPECIAL REVIEW – SURPLUS COMPUTER EQUIPMENT DATA REMOVAL

Background

The Commonwealth uses several means to sell or transfer used computer equipment. Many agencies use the Department of General Services for this service; others contract out the disposal of such equipment, while others such as Institutions of Higher Education sell equipment directly to the public. The Commonwealth disposes of thousands of computers and components in this manner yearly.

The Department of General Services acts as an agent to facilitate the sale of used or surplus equipment. General Services does not have the capacity to cleanse hard drives, but relies on the individual agencies that use them for disposal to provide assurance that they have properly prepared the equipment for sale or transfer. The goal of selling or transferring used equipment is to create savings and provide environmentally responsible recycling.

The disposal process includes direct sales or auctions of many computers and parts to the public, or transfers of equipment to other state and local government units. Whether systems are sold, transferred within government, or dumped as garbage, it is imperative that data and programs be removed by special utility software or by physically destroying the storage media such as the hard drive.

The removal of data from surplus equipment is an especially relevant concern since identity theft is increasing. In addition, both federal and state laws require that agencies exercise due diligence to protect sensitive and personal data that they may obtain. As an example, the federal Health Insurance Portability and Accountability Act (HIPAA) mandates that agencies consider some information "protected health information" (PHI) and provide the proper security to keep citizens' health information private. This law does provide for penalties if the keeper of the information does not protect the information.

Virginia law has various privacy components such as the Computer Invasion of Privacy section of the Virginia Computer Crimes Act and the Government Data Collection and Dissemination Practices Act which stipulates agencies can "collect, maintain, use, and disseminate only that personal information permitted or required by law to be so collected, maintained, used, or disseminated, or necessary to accomplish a proper purpose of the agency."

Best Practice Data Removal Controls

As most users of computers are aware, deleting files does not destroy data. It merely updates a table that designates that area of a hard drive available to store new information. If the user does not store data in this available area, the old data remains viewable. With the advent of large storage hard drives, a computer may never need to use the available old data area for new information.

Just as deleting a file does not really destroy data, reformatting a hard drive really works in much the same manner. It segments the hard drive and prepares it for reuse. However, savvy users may be able to read data with utility software commonly available.

Software is commercially available that performs routines that write over data and programs with in essence the numeral one and zero, and is the most secure method of destroying data. To be most effective different software packages will use a combination of methods or perform the functions multiple times. Inoperable computer equipment should have either their drives destroyed or be cleansed in manner as previously described.

Agency Controls

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. Agencies should have written policies and procedures for the preparation of equipment for sale or transfer. These standards should include authorization of disposal, cleansing of hard drives and other storage media before sale and transfers, secured storage of equipment before cleansing, stamps or other means of tagging devices as cleansed, and the signature of who performed cleansing and date of work. Agencies should send no equipment to the final surplus staging area without the above controls. There is an argument that not all equipment needs thorough cleaning because it does not contain critical data. It should be remembered that just because a system did not contain what the agency considers as critical data it could still contain sensitive material (social security numbers, copied e-mails, draft agency policies etc.).

Study Purpose and Methodology

Because of the rapid changes in technology and the use of public sales and government transfer to dispose of surplus computer equipment, our office undertook a review of the status of policies and procedures and their implementation. The review tried to determine what measures exist to minimize the risk of the inadvertent release of sensitive information.

In performing the review, we researched the Commonwealth of Virginia Accounting Policies and Procedures Manual and Commonwealth's Information Technology Resource Management policies to determine the administrative requirements. We also queried the Department of Medial Assistance (DMAS), Department of Health (VDH), Department of Social Services (DSS), Virginia Employment Commission (VEC), Virginia Retirement System (VRS), Department of Motor Vehicle (DMV), Department of Tax (TAX), Department of General Services (DGS), and Virginia Tech to determine their policies and procedures. Finally, we tested the Department of General Service's and Virginia Tech's surplus sites to determine if sensitive data had been cleansed prior to computer equipment going to public sale or government transfer.

Findings and Recommendations

Control Issues

Test of Information Removal

We judgmentally selected twenty-five laptops and servers ready for sale or transfer for inspection. Of those twenty-five, we could freely read or use data recovery software to read data on twenty two (or 88 percent tested). We did not expand the test since we also found that there was no appropriate procedure in the agencies to cleanse the drives.

We conducted our test of surplus equipment at the Department of General Services surplus warehouse and the Virginia Polytechnic Institute and State University (Virginia Tech). Our review considered the Commonwealth's overall policies and procedure and those at the individual agencies.

On the equipment at the Department of General Service surplus warehouse ready for public sale, we found information exempt from the Freedom of Information Act that was either freely readable or could be read with data recovery software. The data recovery software is commercially available and cost about $150.

The information included citizen vaccination records, Women Infant and Children (WIC program) personal information, credit card information, personnel evaluations, correspondence pertaining to personnel grievances and actions, and scholastic evaluation discussing identifiable students. Some equipment at one

time required passwords; however, in getting the equipment ready for sale or transfer the passwords had a default setting.

At Virginia Tech, we found data on laptops concerning the operation of two departments, their personnel, and other key operational information. Virginia Tech's procedures often include removing the hard drives from the computer chassis before sale; however, of the three such designated computers we selected, all three still had their hard drives. One hard drive was clean, one could be read with data utility software available to anyone and belonging to the student counseling center, the last could be booted and read without utility software and had a department's information on it.

Virginia Tech does have policies and procedures for the preparation of computer equipment for sale and transfer, but relies primarily on individual departments to comply with the procedures. As an example, each department should format the drives before sending out to the Surplus Property. Because Surplus Property often finds this procedure not done, they hire staff from the Information Systems and Computing Department to wipe all hard drives. However, this procedure does not apply to laptop computers.

Virginia Tech policies do not address the internal transfer of equipment or computer components. Therefore, it is also possible that while the information may not become public, that sensitive information could accidentally transfer to another department.

We contacted all of the agencies and departments where we found data on the computer equipment or components. These agencies took immediate action to correct the problem not only of the equipment we tested, but also on any other equipment that they had available for sale or transfer.

Test of Policies and Procedures

We chose to review the policies and procedures at seven agencies and one institution of higher education. We selected these agencies because by their business nature they store and process data that is often sensitive.

Some agencies have policies and procedures pertinent to the removal of data from surplus equipment as seen in the table below. However, many of the policies were not strong and often were not followed. No statewide standard defines what proper preparation should include.

For instance, the Department of Social Services only uses disk formatting procedures before sending equipment to a contracted party for disposal. This method is insufficient in light of HIPAA and state privacy regulations, and data recovery software could recover these files.

SUMMARY OF THE ADEQUACY OF POLICIES AND PROCEDURES

Agency	Appropriate Policies and Procedures
Medical Assistance	NO
Motor Vehicle	NO
Social Services	NO
Tax	NO
Health	YES
Employment Commission	NO
Retirement System	YES
Virginia Tech	NO

Recommendation: All computer technology (laptops, desktops, towers, mainframes, routers, firewall servers, handheld devices such as Personal Data Assistants) that is currently slated for sale or transfer should be inspected by appropriate staff to determine that data has been removed in a manner that it can not be read using utility software.

Recommendation: The Virginia Information Technologies Agency (VITA) should create a policy and procedure which defines the responsibility for the removal of data before sale or transfer of surplus equipment.

Recommendation: The Virginia Information Technologies Agency should create a disk cleaning standard for all agencies and institutions. These standards should make use of disk cleansing utilities or destruction of hard drives that are inoperable. Mere formatting of hard drives is insufficient in most cases.

Recommendation: The Chief Information Officer or designated Information Security Officer of each agency should create an audit function to randomly test equipment that is ready for public auction or transfer.

Commonwealth of Virginia

Walter J. Kucharski, Auditor

Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

October 9, 2003

The Honorable Mark R. Warner
Governor of Virginia
State Capital
Richmond, Virginia

The Honorable Kevin G. Miller
Chairman, Joint Legislative Audit
and Review Commission
General Assembly Building
Richmond, Virginia

Gentlemen:

The Auditor of Public Accounts has reviewed the Commonwealth of Virginia's policies and procedures over removing data from surplus equipment sold to the public or transferred within government. Our objective was to determine if controls exist at both the state-wide and agency level that minimize the risk of sensitive information being released inadvertently via public auction or transfer.

Based on our review and test of equipment designed as ready for sale or transfer, we found severe weaknesses in the policies and procedures and their implementation that can lead to release of sensitive information via public sale or government transfer of surplus computer equipment. Our report includes recommendations to correct this situation.

Exit Conference

We discussed this report with representatives of Virginia Information Technologies Agency on October 20, 2003.

AUDITOR OF PUBLIC ACCOUNTS

KJS:whb
whb:49

COMMONWEALTH of VIRGINIA

George C. Newstrom
Chief Information Officer

Virginia Information Technologies Agency
202 NORTH NINTH STREET
SUITE 506
RICHMOND, VIRGINIA 23219
(804) 786-9579

October 28, 2003

Mr. Walter J. Kucharski
Auditor of Public Accounts
James Monroe Building, 8th Floor
101 North 14th Street
Richmond, Virginia 23219

Dear Mr. Kucharski:

The Chief Information Officer and the management of the Virginia Information Technologies Agency (VITA) agree with the audit findings in your draft study report on the removal of information from hard drives of surplus computer equipment slated for sale through public auction or transfer within state government.

It is the ITRM policy of the Commonwealth that each agency head is responsible for the security of the agency's information technology resources and that all state agencies shall take appropriate steps to secure their IT resources and sensitive information. The current Commonwealth ITRM Security Standard (SEC2001) in section F.1.c) requires that "All sensitive data must be removed from system hardware, software or media by the owner prior to its reuse by another agency, or for reuse by another system within the agency. Similarly, all sensitive data must be removed from system hardware, software or media by the owner prior to its disposal."

In addition to the current ITRM Security policy and standards, VITA has developed a new draft Security standard (Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media), created an internal VITA audit policy to enforce all security standards (including the new draft standard), and worked with the Department of General Services to implement a surplus property process that requires agency certification that all computers, devices or memory media ready for disposition have had all memory storage removed following the requirements in the new draft standard for all such devices currently in DGS custody and prior to accepting any new such devices from agencies for disposal. As an interim precaution, DGS has put a hold on any further sales until the standard is promulgated.

Over the next 18 months, as agencies transition to VITA for operations support, VITA will assume greater responsibility for the actual disposal of computers, devices or memory media, and will play a vital role in ensuring sensitive Commonwealth information is properly secured.

If you have any questions, please contact me at your earliest convenience.

Sincerely,

George C. Newstrom

C: Eugene Huang, Deputy Secretary of Technology
Cheryl Clark, Deputy Chief Information Officer