PERFORMANCE AUDIT

STATE AGENCY REMOVAL OF DATA FROM SURPLUS COMPUTERS

From The Office Of State Auditor Claire McCaskill

Ineffective computer sanitation policies or lack of policies at state agencies exposes the state, its employees and citizens to unnecessary risk of data disclosure.

Report No. 2004-70
September 15, 2004
www.auditor.mo.gov

Office of
Missouri State Auditor
Claire McCaskill

September 2004

YELLOW SHEET

Weak Controls Increase the Risk Sensitive or Confidential Material Is Not Properly Safeguarded

Each year the state disposes of hundreds of computers through surplus property sales to political subdivisions and certain not-for-profit organizations and auctions open to the public. We evaluated state agency and overall state policies and procedures for removal of data from disposed of computers to prevent sensitive or confidential data from being disclosed.

Data removal not always effective or consistently done across state agencies

Test results showed we could read or use data recovery software to read data on 37 of the 56 (66 percent) computers tested, which indicated there had been no attempt to remove data or attempts were ineffective. For 13 of the 37 (36 percent) computers, the agency formatted the drive or removed the partition, attempting to remove data. Changing a hard drive format using the format command or removing the partition on a hard drive are sometimes misunderstood as ways to erase data, but neither technique actually removes data. (See page 3)

Sensitive data remained on computers not sanitized

Twenty-three of the 37 (64 percent) computers which had not been sanitized had sensitive data. The sensitive data included social security numbers, bank account information, computer network access information, and medical data. All 37 computers still had licensed software. (See page 4)

No consistent statewide policy

In August 2004, the Office of Information Technology (OIT) provided guidance to state agencies in establishing computer sanitation standards. Until that time state agencies had received little help regarding computer sanitation. As a result, they had inconsistent data removal policies. Only 2 of 12 agencies tested (Departments of Health and Senior Services, and Mental Health) had established written department-wide polices. Other agencies had informal guidelines that were not consistently used by each agency unit or division or were ineffective based on our test results. State agencies will need to develop their own computer sanitation standards based on the OIT guidance. (See page 5)

All reports are available on our website: www.auditor.mo.gov

STATE AGENCY REMOVAL OF DATA FROM SURPLUS COMPUTERS

TABLE OF CONTENTS

CLAIRE C. McCASKILL

Missouri State Auditor

Honorable Bob Holden, Governor
and
Members of the General Assembly
and
Gerald Wethington, Chief Information Officer
Office of Information Technology
and
State Agency Directors
Jefferson City, MO 65102

Each year the state disposes of hundreds of computers through surplus property sales to political subdivisions and certain not-for-profit organizations and auctions open to the public. Our audit objective was to evaluate state agency and overall state policies and procedures for removal of data from disposed of computers to prevent sensitive or confidential data from being disclosed.

We identified sensitive data on 23 of 56 computers tested. The sensitive data included social security numbers, bank account information, network access information, and patient medical data. Until August 2004, state agencies did not have guidance to follow when establishing computer sanitation policies. State agency's policies and procedures ranged from detailed written procedures to informal procedures that were not consistently followed or were ineffective. As a result, sensitive and/or confidential material was available to the public on surplus computers.

We conducted the audit in accordance with applicable standards contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, and included such tests of the procedures and records as were considered appropriate under the circumstances.

Claire McCaskill

Claire McCaskill
State Auditor

The following auditors contributed to this report:

Director of Audits:	William D. Miller, CIA, CGFM
Assistant Director of Audits:	Jon Halwes, CPA, CGFM
Information Systems Audit Manager:	Jeff Thelen, CPA
In-Charge Auditor:	Jeff Roberts
Audit Staff:	Frank Verslues

RESULTS AND RECOMMENDATIONS

Weak Controls Increase the Risk Sensitive or Confidential Material Is Not Properly Safeguarded

State agencies are not consistently removing data from computer hard drives before they are sold, transferred, or disposed of. As a result, sensitive or confidential material may be compromised causing potential security risks to the state or disclosure of personal information of state employees or citizens. Some agencies had established effective procedures for removal of data while others had informal procedures that were inconsistently applied and ineffective. The state has a fiduciary responsibility to safeguard information provided by the public or sensitive in nature to the state or its employees. Lack of statewide guidance from the Office of Information Technology and sufficient consideration of this issue by state agency management has contributed to the weaknesses identified.

Background

The state uses various means to sell or transfer used computer equipment that is no longer needed either because its technology is outdated or parts are no longer functioning. Many agencies use the Office of Administration - Missouri State Agency for Surplus Property (MOSASP) for this service. Some agencies, including the Department of Conservation, hold public auctions or dispose of equipment including computers without using MOSASP.

MOSASP acts as an agent to facilitate the transfer or sale of surplus equipment. Equipment received by MOSASP may be transferred to another state agency, sold to local school districts and other political subdivisions, certain not-for-profit organizations, or other organizations registered with the division. Items that remain unsold to these organizations are periodically sold as part of public auctions. MOSASP policy states it is each agency's responsibility to remove data from surplus computers.

Data removal methods and controls

Deleting a file does not destroy the data. It only removes the reference to the file location on the hard drive. Removing the reference to the file location makes it appear that the file no longer exists. However, the actual data is not removed and the file remains on the hard drive indefinitely, until its space is needed and overwritten by another file. With the increased use of large storage hard drives, drive space may never be fully used, and files may never be overwritten. Inexpensive data recovery software is commercially available that can easily be used to search for and recover these deleted files from hard drives.

Before a hard drive can be used, a primary partition must be created to allocate disk space to support a file system and assign a drive letter (for example the C: drive). A computer is started or booted from and the operating system is read from the primary partition. Once a hard drive is partitioned, it must be formatted to create a file system. A file system manages the overall structure in which files are named, stored, and organized. After a drive has been partitioned and formatted, the necessary information is stored to allow the hard drive to accept, store, and retrieve data.

Changing a hard drive format using the format command is sometimes misunderstood as a way to erase data, but it only removes the filename link to the physical location of the data. The data remains on the drive, as when data is deleted. The format command actually creates a new file system, leaving all previous data on the hard drive untouched. Removing the partition on a hard drive is also misunderstood as a technique to erase data. When the partition is removed from the drive, the computer will not complete the normal boot process, which makes it appear that all files have been deleted. Data recovery software can also be used to search for and recover files from hard drives that have been formatted or had a partition removed.

Sanitizing (also called overwriting, wiping or purging) a computer means removing all traces of information from a hard drive in a manner that gives assurance the information is unrecoverable by any means. Sanitizing defeats attempts to recover information using data recovery software or more advanced methods. The sanitizing process replaces previously stored data on the hard drive with a predetermined pattern of meaningless information. Sanitizing software is commercially available. To ensure data cannot be recovered using data recovery software or other methods, sanitizing software often has options to overwrite the entire hard drive three or more times.

Methodology

We tested a sample of 56 computers ready for sale or transfer, which had been disposed of by state agencies, to determine if any data, information, or software remained on them or could be recovered. For each computer that had recoverable files, we searched all documents, spreadsheets, and other files for data and information considered sensitive or confidential and licensed software. We met with officials from each of the agencies from which computers were selected to discuss the results of our testing and to determine the policies and procedures used by the agencies for removal of data prior to computer disposal. We also met with officials from the state's Office of Information Technology (OIT)[1] regarding statewide policies and procedures covering this issue. *(See Appendix I, page 10, for more detail on the methodology).*

Data removal not always effective or consistently done across state agencies

Test results showed we could read or use data recovery software to read data on 37 of the 56 (66 percent) computers tested, which indicated there had been no attempt to remove data or attempts were ineffective. Table 1 shows what action state agencies took to remove or destroy data on each computer tested. "No Action Taken" means no procedures were performed to remove data from the hard drive. The computer either booted normally (17 computers) or had a hardware problem (7 computers), such as a missing graphics card, that prevented it from booting normally, but the drive was readable when connected to our computer equipment. If the agency formatted the drive or removed the partition, there had been an attempt to remove data. If the drive had been sanitized, data had been permanently removed.

[1] The OIT is responsible for coordinating information technology initiatives for the state and has the authority to establish statewide policies that will contribute to the effective use of information technology within the state.

Table 1: Computers Selected By Agency and Initial Results

Agency	Number of Computers Tested	No Action Taken	Drive Formatted or Partition Removed	Hard Drive Sanitized
DESE[1] - Administrative and Financial Services	5	5	0	0
Public Safety - Veterans Commission	3	3	0	0
Governor	3	3	0	0
Natural Resources	4	2	0	2
Public Safety - Capitol Police	2	2	0	0
OA[2] - Facilities Management	5	2	2	1
OA - Information Services	3	2	1	0
Corrections - Probation and Parole	1	1	0	0
Higher Education	2	1	0	1
OA - General Services	1	1	0	0
Lieutenant Governor	1	1	0	0
House of Representatives	3	1	2	0
Conservation	5	0	5	0
OA - Design and Construction	3	0	3	0
DESE -Vocational Rehabilitation	4	0	0	4
Health and Senior Services	6	0	0	6
Mental Health	5	0	0	5
Total	56	24	13	19

[1] Department of Elementary and Secondary Education
[2] Office of Administration

Source: SAO analysis

Sensitive data remained on computers not sanitized

We found 23 of the 37 (64 percent) computers which had not been sanitized had sensitive data. We defined sensitive data as any information not considered available to the public such as social security numbers and medical information. Almost all computers (34 of 37) also had non-sensitive data. We defined non-sensitive data as any information that would generally be available to the public. All 37 computers still had licensed software[2] on them. Table 2 shows the results by agency for these 37 computers.

[2] Licensed software included any computer program subject to licensing requirements or restrictions.

Table 2: Data Search Results

Agency	Computers Not Sanitized	Type of Data Found	
		Non-Sensitive	Sensitive
Conservation	5	5	4
Corrections - Probation and Parole	1	1	1
DESE[1] - Administrative and Financial Services	5	5	5
Higher Education	1	1	0
Natural Resources	2	2	0
Public Safety - Capitol Police	2	2	2
Public Safety - Veterans Commission	3	3	2
OA[2] - Design and Construction	3	3	3
OA - Facilities Management	4	2	0
OA - General Services	1	1	1
OA - Information Services	3	2	0
Governor	3	3	1
Lieutenant Governor	1	1	1
House of Representatives	3	3	3
Total	37	34	23

[1] Department of Elementary and Secondary Education
[2] Office of Administration

Source: SAO analysis

The majority of sensitive data found on the hard drives was related to the work performed by the state employee using the computer, such as social security numbers of state employees and state program applicants or participants. Other sensitive data found included:

- Bank account information
- Network access information including the remote dial-in phone number
- A document from the federal government labeled "For Official Use Only"
- Medical history information
- A patient's plan of care
- Report of patients' medicine dosage errors
- Law enforcement official investigation report
- Abuse/neglect occurrence investigation report
- Nursing home complaint forms
- Employee performance appraisals

No consistent statewide policy

As of June 2004, OIT had not established a statewide policy to ensure data is completely removed from computers designated for surplus. As a result, state agencies had inconsistent data removal policies. Only 2 of 12 agencies tested (Departments of Health and Senior Services, and Mental Health) had established written department-wide polices. The Department of Health and Senior Services' policies and procedures were effective based on our hard drive test results and review of the policies. The Department of Mental Health also used an effective sanitation process based on our test results; however, the department's procedures did not include a testing phase to ensure data was completely removed. Other agencies had informal guidelines that were not consistently used by each agency unit or division or were ineffective based on our test results. The Department of Conservation and House of Representatives policies only required hard drives be formatted to alter the original drive's file system and/or remove the drive's partitions, which do not permanently remove data. The Office of Administration and Department of Public Safety had not established organization-wide policies to follow, but some of their agency units or divisions had established informal policies or followed those established by other divisions. Agency officials provided the following reasons why formal written policies had not been established:

- Waiting for guidance from the OIT
- Relying on other state agencies to handle the agency's computer disposal issues
- Did not believe their computers had sensitive or confidential data
- Believed their informal procedures for removing hard drive partitions were effective

Only the Department of Health and Senior Services of the 12 agencies tested, had effective procedures for testing or certifying that computers had been sanitized prior to disposal. Such procedures are necessary to ensure computers are not missed and the sanitation process is working properly. Three agencies (the Departments of Elementary and Secondary Education, Higher Education, and Natural Resources) using effective sanitization methods, disposed of un-sanitized computers at least in part due to not having testing procedures.

OIT addressed the issue of removing data from surplus computers in a February 2003 Information Technology Advisory Board (ITAB) meeting. In the meeting, state information technology officials discussed a media report of state of Kentucky surplus computers still having secure data. The ITAB minutes from that meeting indicated a statewide policy would be developed, but no timeframe was noted. OIT's Chief Information Officer said sanitation of surplus computers was ranked 11th of 42 priority items by his office. OIT finalized computer sanitation guidance at the end of July 2004 and made it available to state agencies in August. He said each state agency would need to develop its own computer sanitation standards based on the guidance. We reviewed the guidance and found it covered the key elements needed when establishing a computer sanitation policy.

Conclusion

Commitment by all state agencies to develop and implement computer sanitation policies and procedures is needed to ensure sensitive or confidential material is appropriately safeguarded and licensed software is removed before the surplus, sale, transfer, or disposal of computer equipment. Ineffective policies or lack of policies at state agencies exposes the state, its employees and citizens to unnecessary risk of data disclosure.

Recommendation

State agencies, using the OIT guidance, develop organization-wide computer sanitation policies. The policies should define the following requirements:

- The responsibility for the removal of data before the surplus, sale, transfer, or disposal of computer equipment.
- The minimum requirements and acceptable methods for the removal of data from an agency's computer hard drives prior to the surplus, sale, transfer, or disposal of the equipment.
- A process to test and certify an agency's removal of data from computer hard drives.

OIT Comments

In response to the audit "State Agency Removal of Data from Surplus Computers", the Office of Information Technology agrees with the finding "Ineffective computer sanitation policies or lack of policies at state agencies exposes the state, its employees and citizens to unnecessary risk of data disclosure." As detailed in the audit report, OIT raised the issue at the February 2003 ITAB meeting and had the issue assigned to the ITAB security committee. Subsequently, the issue was assigned to the Missouri Adaptable Enterprise Architecture (MAEA) Security Domain Committee for action. The issue was assigned a priority of 11 out of 42 security disciplines that had to be addressed. The priority of 11 was assigned, as there were more pressing security issues before the Security Domain Committee that posed greater risk to the State, its employees and citizens. The audit report does point out the resulting time line for the OIT publishing a MAEA Compliance Component on PC Disposal and with respect to the compliance component comments, "We reviewed the guidance and found it covered the key elements needed when establishing a computer sanitation policy."

With respect to further action on this issue, it is worth reporting that at the August 25, 2004 ITAB meeting, OIT directed the Security Domain Committee to develop a Product Compliance Component for PC Disposal to ensure consistency across state agencies with respect to software used to sanitize PCs prior to disposal.

Department of Conservation Comments

The Missouri Department of Conservation will review its policy for the removal of data from surplus computers and will take steps considered necessary to ensure sensitive information is appropriately removed.

Department of Corrections Comments

The department concurs with the recommendation and will await guidance from the Office of Information Technology as specified.

Department of Elementary and Secondary Education Comments

We agree with this recommendation. The department is in the process of developing a department-wide computer sanitation policy.

Department of Mental Health Comments

The Department of Mental Health will follow the guidelines listed in the State Enterprise Architecture Compliance Component that was approved on July 30, 2004. The Department of Mental Health already has a procedure for sanitizing data from computer equipment. The report stated that the department's procedure "did not include a testing phase to ensure data was completely removed." The product that the department procedure requires is Gdisk. While our procedure did not specifically refer to the verification phase, the Gdisk product does indicate upon completion, whether the product was successful or not. Current department procedures are being modified to include:

- *Verifying and recording that the sanitization process was successful*
- *Labeling of sanitized computers*
- *Keeping a record of the sanitization history of all surplused computers*

Department of Natural Resources Comments

We agree with the recommendations noted in the audit and have had procedures on data removal from surplused computers for some time. Following the discussions with your staff, we made procedural modifications to address the weaknesses noted in the audit. These modifications were documented in an August 9, 2004 memo to the department's division directors. These modifications were also discussed in the most recent monthly technical support staff meeting. We will formalize the procedures by developing a written policy in the near future.

Department of Public Safety Comments

The Department of Public Safety agrees with the finding. Divisions within the Department of Public Safety have a policy of wiping the hard drives clean before the computers are sent to surplus. We are in the process of developing a department wide policy that will establish a minimum procedure that each division will follow. The divisions will have the option of implementing stronger standards but they will be required to follow, at least, the minimum standard procedure.

Office of Administration Comments

We agree. In compliance with the Compliance Component that was recently approved by ITAB, OA has drafted a department wide policy that will be issued in September. OA has included the acceptable method for removal of data in its policy and has acquired software to ensure that this is done to meet the requirement of the compliance component. OA has included procedures in its policy to test to ensure data removal was successful. In addition, OA is modifying its Report *of State Owned Surplus Property, MO 300-1249N (8-03), to include a check box that requires the submitting agency to acknowledge whether or not the computers itemized have been sanitized consistent with the Missouri Adaptable Enterprise Architecture's PC Disposal Compliance Component and requires the signature of the individual responsible for sanitization as well as the date sanitized. Finally, the Division of State Surplus Property will in the future not accept PCs for disposal unless the new fields are completed on the form.*

Governor Comments

The Governor's Office does currently overwrite all hard drives on computers that are sent to surplus property. We concur that information that is either sensitive and/or confidential, should be irrevocably erased from computer hard drives before they are disposed of by state departments and entities.

Lt. Governor Comments

Our office strongly supports the need for a uniform data removal policy in order to protect the sensitive nature of citizen inquires. The Office of Administration services the computers in the Lt. Governor's office so we will work with them to ensure compliance with the final procedures.

The Departments of Health and Senior Services and Higher Education and the House of Representatives chose not to provide a response to the recommendation.

OBJECTIVE, SCOPE AND METHODOLOGY

Objective

Our audit objective was to evaluate state agency and overall state policies and procedures for removal of data from disposed of computers to prevent sensitive or confidential data from being disclosed.

Scope and Methodology

On various dates in May and June 2004, we obtained 51 computers, from the Office of Administration - Missouri State Agency for Surplus Property (MOSASP). These computers had been transferred to MOSASP by various state agencies for sale or disposal. We also obtained 5 computers from the Department of Conservation in June 2004, that were being sold by that agency. Computers that contained a hard drive were haphazardly selected for testing. The following procedures were performed on the selected computers:

- A monitor, mouse, and keyboard were plugged into the computer to determine if the system would boot normally. The boot results were noted and the computer shut down. If the computer booted normally, nothing had been done to remove the data, information, or software.

- We removed the hard drive from the original computer and connected it to our computer equipment for further evaluation.

- The hard drive was then scanned using inexpensive, commercially available data recovery software. The hard drive was scanned to recognize information on the drive, which is a prerequisite to recovering deleted partitions, re-formatted drives, and for recovering deleted files on the drive. Use of the data recovery software was not necessary to recover files that had not been deleted.

- If a computer did not boot normally, we used information from the drive and other tools to determine what had been done to prevent the drive from booting. In some cases, the drive had been formatted to alter the drive's original file system or a partition had been removed to change the boot record and logical division of the drive. In these cases, the data recovery software was used to recover files in the same manner as for the computers that booted normally.

- We then searched all documents, spreadsheets, and other readable files for data or information considered sensitive or confidential that would not be available to the public. We also searched for licensed software.

- Per a written agreement with MOSASP officials, we used software to sanitize the hard drive by overwriting all previous data from any computers which still had data before we returned them.

We met with officials from each of the agencies from which computers were selected to discuss the results of our testing and to determine the policies and procedures used by the agencies for removal of data prior to computer disposal. In addition, we met with an official from the Department of Transportation to discuss that agency's policies and procedures, but selected no computers from that agency for testing. We also met with officials from the state's Office of Information Technology regarding statewide policies and procedures covering this issue.