COMPUTER SECURITY AUDIT REPORT

Surplus Computer Equipment: Determining Whether State Agencies Effectively Remove Software and Agency Data From Surplus Computers

A Report to the Legislative Post Audit Committee
By the Legislative Division of Post Audit
State of Kansas
June 2008
THE LEGISLATIVE POST Audit Committee and its audit agency, the Legislative Division of Post Audit, are the audit arm of Kansas government. The programs and activities of State government now cost about $13 billion a year. As legislators and administrators try increasingly to allocate tax dollars effectively and make government work more efficiently, they need information to evaluate the work of governmental agencies. The audit work performed by Legislative Post Audit helps provide that information.

We conduct our audit work in accordance with applicable government auditing standards set forth by the U.S. Government Accountability Office. These standards pertain to the auditor’s professional qualifications, the quality of the audit work, and the characteristics of professional and meaningful reports. The standards also have been endorsed by the American Institute of Certified Public Accountants and adopted by the Legislative Post Audit Committee.

The Legislative Post Audit Committee is a bipartisan committee comprising five senators and five representatives. Of the Senate members, three are appointed by the President of the Senate and two are appointed by the Senate Minority Leader. Of the Representatives, three are appointed by the Speaker of the House and two are appointed by the Minority Leader.

Audits are performed at the direction of the Legislative Post Audit Committee. Legislators or committees should make their requests for performance audits through the Chairman or any other member of the Committee. Copies of all completed performance audits are available from the Division’s office.

LEGISLATIVE POST AUDIT COMMITTEE

Senator Derek Schmidt, Chair
Senator Nick Jordan
Senator Les Donovan
Senator Anthony Hensley
Senator Chris Steineger

Representative Virgil Peck Jr., Vice-Chair
Representative Tom Burroughs
Representative John Grange
Representative Peggy Mast
Representative Tom Sawyer

LEGISLATIVE DIVISION OF POST AUDIT

800 SW Jackson
Suite 1200
Topeka, Kansas 66612-2212
Telephone (785) 296-3792
FAX (785) 296-4482
E-mail: LPA@lpa.state.ks.us
Website: http://kslegislature.org/postaudit
Barbara J. Hinton, Legislative Post Auditor

DO YOU HAVE AN IDEA FOR IMPROVED GOVERNMENT EFFICIENCY OR COST SAVINGS?

The Legislative Post Audit Committee and the Legislative Division of Post Audit have launched an initiative to identify ways to help make State government more efficient. If you have an idea to share with us, send it to ideas@lpa.state.ks.us, or write to us at the address above.

You won’t receive an individual response, but all ideas will be reviewed, and Legislative Post Audit will pass along the best ones to the Legislative Post Audit Committee.

The Legislative Division of Post Audit supports full access to the services of State government for all citizens. Upon request, Legislative Post Audit can provide its audit reports in large print, audio, or other appropriate alternative format to accommodate persons with visual impairments. Persons with hearing or speech disabilities may reach us through the Kansas Relay Center at 1-800-766-3777. Our office hours are 8:00 a.m. to 5:00 p.m., Monday through Friday.
June 12, 2008

To: Members, Legislative Post Audit Committee

Senator Derek Schmidt, Chair                Representative Virgil Peck Jr., Vice-Chair
Senator Les Donovan                         Representative Tom Burroughs
Senator Anthony Hensley                     Representative John Grange
Senator Nick Jordan                         Representative Peggy Mast
Senator Chris Steineger                     Representative Tom Sawyer

This report contains the findings, conclusions, and recommendations from our completed performance audit, *Surplus Computer Equipment: Determining Whether State Agencies Effectively Remove Software and Agency Data From Surplus Computers*. 

The report includes recommendations for the Department of Administration, Adjutant General’s Office, Kansas Health Policy Authority, Kansas Sentencing Commission, Information Technology Executive Council (ITEC), and Chief Information Technology Officers (CITOs) of the Executive, Judicial, and Legislative Branches.

We would be happy to discuss these recommendations or any other items in the report with any legislative committees, individual legislators, or other State officials.

Barbara J. Hinton
Legislative Post Auditor
Get the Big Picture
Read the sections and features:

1. Executive Summary - an overview of the questions we asked and the answers we found.

2. Conclusion and Recommendations - appear in boxes at the end of the report sections. They also are referenced in the Executive Summary.

3. Agency Response - is included as the last Appendix in the report.

Helpful tools for Getting to the Detail

- In many cases, an “At a Glance” description of the agency or program appears within the first few pages of the main report.

- Side Headings point out key issues and findings.

- Charts and Tables found throughout the report help tell the story of what we found.

- Narrative text boxes can highlight interesting information, or provide detailed examples.

- Appendices include additional supporting detail, along with the Scope Statement and Agency Response(s).
Do State Agencies Effectively Purge Surplus Computers and Other Electronic Media Of Software and Agency Data Before Disposing of Them?

Agencies are responsible for removing all data from their computers before they dispose of them. As the custodians of State data, agencies are responsible for removing the data from their computers before they make them available to the public. Many of the records agencies handle are confidential under State or federal law and must be protected, but it’s also a good practice to avoid needlessly exposing data that is sensitive but not confidential. Many common methods people use to take data off a computer don’t actually work, such as reformatting the hard drive. Best practices call for completely removing all data by physically destroying the hard drive, demagnetizing it, or overwriting the entire drive with nonsense characters at least three times. It’s also important to document the work done.

We found recoverable files on computers from four of the six agencies we looked at. We picked 15 computers from Surplus Property and used inexpensive file recovery software to see if any of them contained agency files. We were able to recover files from ten of the computers. Seven computers contained confidential information (social security numbers, Medicaid information, and password files), four contained sensitive files that agencies probably wouldn’t want made public, and one contained copyrighted music files. In general, it didn’t appear that much had been done to most of the computers to remove the data. We found that the data weren’t properly removed from the computers because agencies lacked policies, thought that Surplus Property was removing the data, or did a poor job of keeping track of their computers. Because of the severity of our early findings, the Department of Administration temporarily stopped selling computers in early May until they could make sure data were properly removed from all they had in stock.

The State needs to strengthen its policy for removing data from computers and educate agencies about that policy. Currently, the only enterprise-wide policy on removing data from computers is difficult to find, applies only to confidential data, and lacks any documentation requirements. The Information Technology Executive Council (ITEC) has a policy in draft form that is very close to best practice, but lacks a requirement on the number of times drives should be overwritten and documenting who did the work. Finally, Surplus Property is in a perfect position to act as a final control to protect data on computers from Topeka-based agencies by removing data that agencies miss.
EXECUTIVE SUMMARY
Legislative Division of Post Audit
08CC03 JUNE 2008

Conclusion ..................page 9

Recommendations ..............page 9

APPENDIX A:  Scope Statement ..............page 11

APPENDIX B:  Agency Responses ..............page 13

This audit was conducted by Allan Foster and Travis Williams. Scott Frank was the audit manager. If you need any additional information about the audit’s findings, please contact Mr. Foster at the Division’s offices. Our address is: Legislative Division of Post Audit, 800 SW Jackson Street, Suite 1200, Topeka, Kansas 66612. You also may call us at (785) 296-3792, or contact us via the Internet at LPA@ipa.state.ks.us.
Under State law, agencies can dispose of outdated computer equipment through the State Surplus Property Program that is operated by the Department of Administration. The equipment is first made available to organizations that are eligible to participate in a similar federal program, and then is offered for sale to the public. Although staff who operate the Surplus Property Program check the computer equipment for information before offering it up for sale, it’s the agency’s responsibility to ensure that all proprietary software and agency data have been removed before it disposes of the equipment.

Over the last several years, numerous audit reports have been released that look at whether federal, state, and local agencies across the country do an adequate job of purging data from computers and other electronic media before disposing of them. In these reports, auditors consistently report finding proprietary software and agency data—often confidential—on computers that were about to be sold to the public. These audit findings raised concerns about how Kansas agencies prepare their surplus computer equipment for disposal.

This performance audit answers the following question:

**Do State agencies effectively purge surplus computers and other electronic media of software and agency data before disposing of them?**

To answer this question, we reviewed a sample of computers that Topeka-based State agencies had turned over to Surplus Property and attempted to recover files from them. When we found data on a computer, we reviewed a sample of documents looking for confidential or sensitive data. For agencies whose computers still had data on them, we reviewed agency disposal policies and interviewed agency officials about how computers ended up at Surplus Property with recoverable files. Finally, we reviewed Information Technology Executive Council (ITEC) policies on disposal of computer equipment and compared them to best practices.

A copy of the complete scope statement for this audit approved by the Legislative Post Audit Committee is included in *Appendix A*.

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.
Question 1: Do State Agencies Effectively Purge Surplus Computers and Other Electronic Media of Software and Agency Data Before Disposing of Them?

**ANSWER IN BRIEF:** Agencies often don’t remove data from computers that are sold to the public through Surplus Property. We obtained computers from Surplus Property that had belonged to at least six Topeka-based State agencies and found data on 10 computers from four of those agencies. Of the 10 computers that still had data, seven had confidential documents, including thousands of Social Security numbers. It appeared that data weren’t properly removed because agencies lacked policies, relied on Surplus Property to remove the data, or did a poor job of keeping track of which computers had been processed and which hadn’t. The State needs to strengthen its policy for removing data from computers and take appropriate steps to ensure that agencies are educated about the policy and are following it. These and other findings are discussed in the sections that follow.

**Agencies Are Responsible for Removing All Data From Their Computers Before They Dispose of Them**

In fiscal year 2008, State agencies owned more than 80,000 computers and servers. All of these computers and servers eventually will become out-of-date and need to be disposed of.

By law, most State agencies located in Shawnee County must send all property—including computers—to State Surplus Property, a group within the Department of Administration that was established to dispose of excess property from State agencies. Agencies located outside Shawnee County, as well as the Department of Transportation, have the authority to dispose of property themselves. We didn’t perform any testwork on any computers that non-Topeka-based agencies owned.

When Surplus Property gets a computer from an agency, a staff member cleans it up, reformats the hard drive, and reinstalls the operating system. Surplus Property sets a price for the computer and holds it for 30 days, during which time State agencies and other organizations that qualify for the federal surplus property program can buy it. After 30 days, the computer is offered for sale to the public. In the 12 months ending April 30, 2008, Surplus Property disposed of approximately 600 computers on behalf of State agencies.

As the custodians of State data, agencies are responsible for removing the data from their computers before they make them available to the public. Many of the records State agencies handle are confidential under either federal or State law. These include Social Security numbers, security information, certain employee personnel records, and medical and income tax records.
Agencies that possess such records are responsible for protecting the confidential data contained in them. That responsibility extends to protecting the data when the computer holding the data is disposed of. In addition, it’s good practice for agencies to avoid needlessly exposing sensitive internal documents that might not be confidential, but that agencies normally wouldn’t make readily available to the public, such as employee phone numbers, evaluations of grant requests, and drafts of policy documents. Therefore, it’s important for each agency to ensure that no computers leave its possession without removing all the data.

**Best practices call for completely removing data from a computer’s hard drive before disposing of it.** Most people don’t realize that data are very persistent on a computer. Although they may be difficult to find, the vast majority of all documents ever stored on a computer remain on the hard drive forever—even documents that have been deleted or lost. Moreover, those documents remain accessible unless someone takes special actions to permanently remove them. The following are examples of things that people commonly think will permanently remove data from a computer, but that really don’t:

- deleting the files and emptying the trash
- reformatting the hard drive
- reinstalling the computer’s operating system

In addition, when a hard drive “crashes” or quits working, the data are still there.

Because data are so persistent, best practices have been developed to help organizations know what to do with hard drives they no longer need. Generally, agencies can use any of the following three methods to completely and securely remove data:

- **Physically destroying the hard drive by shredding or incinerating it.** This is considered the most secure method because it protects against any type of attempt to access the data.

- **Demagnetizing the disk with a powerful magnet ("degaussing").** This makes the hard drive unusable, and prevents the data from being recovered using most tools.

- **Using specialized software to overwrite the hard drive multiple times.** At a minimum, the hard drive should be overwritten three times. This makes it impossible to access the data with standard file recovery software, although very expensive tools, such as electron microscopes, still may be used to recover the data.
In addition, best practices require that agencies clearly document what computers were processed, the date, how they were processed, who did the work, and the final disposition of the computer.

| We Found Recoverable Files On Computers From Four of the Six Agencies We Looked At |

To determine if agencies had completely removed the data from their computers, we picked 15 computers from Surplus Property to review. Nine of the computers hadn’t been processed by Surplus Property staff and were in the condition the original agencies had left them. Six of the computers already had been processed by Surplus Property staff and were ready for sale. We ended up with computers from at least six agencies; we couldn’t tie five of these computers to an agency.

We used three techniques to recover files from each computer:

- First, we tried to start up the computer to see if we could access any files that way.
- Next, we removed the hard drive and tried to read it using another computer.
- Finally, we used file recovery software to see if we could find files that didn’t show up with the other methods. The software we used was readily available over the Internet, inexpensive ($60 per copy), and very simple to use.

Figure 1-1 on page 7 summarizes the results of our review of the 15 computers. As the table shows, data were completely removed on only 5 of those 15 computers. We recovered files from the other 10. Of the six agencies we were able to identify, four had at least one computer with recoverable files.

The types of files we were able to recover generally fell into the following three categories:

- Seven computers contained information that’s confidential under State or federal law. Most of this was personal information, including thousands of Social Security numbers, names of Medicaid beneficiaries, and personnel information about State employees.

  In addition, we were able to recover password files and other network files that would provide valuable information to aid computer hackers.

- Four computers contained sensitive agency files that aren’t confidential, but that agencies likely wouldn’t want to make readily available to the public. These included employee accident reports, a summary of the results of an agency investigation into alleged improprieties by a grant recipient, and architectural drawings of a State office building.

- One computer contained copyrighted music files.
In general, it didn’t appear that much had been done to most of the computers to remove the data. It wasn’t always possible to determine conclusively what steps each agency had taken. As far as we can tell, here’s what had been done to the hard drives:

- **Five computers had been fully overwritten and had all the data removed.** We couldn’t recover anything from these computers.

- **Two computers had been partially overwritten and had most of their data removed.** These computers had many fewer files, but we were able to find a confidential file on one of them.

- **Five computers had been reformatted, which didn’t remove the data.** We couldn’t recover most, if not all, the files from these computers. We couldn’t tell who reformatted the computers—the agencies or Surplus Property.

- **Nothing had been done to three of the computers.** We easily retrieved all the files from these computers, each of which was from the group that Surplus Property staff hadn’t yet processed.

The data weren’t properly removed from the computers because agencies lacked policies, relied on Surplus Property to remove the data, or did a poor job of keeping track of their computers. We looked at policies and talked to officials from the four agencies with recoverable data to find out why data still existed on their surplus computers. We found the following underlying reasons why the data hadn’t been properly removed:

- **The Adjutant General’s Office had no policy for removing data when the computer in our sample was taken out of service in 2002.**

- **Staff at both the Department of Administration and the Sentencing Commission thought that when Surplus Property wiped the hard drives, it would remove the data.** Although staff from Surplus Property do reformat the hard drives before they make the computers available to the public, this technique doesn’t adequately remove the data.

- **Staff at the Kansas Health Policy Authority did a poor job of keeping records on what was done to each computer, allowing one of the computers in our sample to fall through the cracks.** The Authority normally contracts with DISC for all of its information technology work. However, in this case an Authority staff member volunteered to remove the data from several computers, including the ones in our sample. The staff person didn’t keep track of what he’d done to each computer. As a result, while one of the computers in our sample was overwritten properly, the second computer wasn’t overwritten.

The Department of Administration suspended the sale of computers at Surplus Property in early May. As soon as we realized the extent of our findings, we contacted the Department and recommended it stop selling computers at Surplus Property until someone could securely remove all the data from each computer. Department officials agreed and quickly stopped selling computers.
### Figure 1-1
Summary of Results From Review of Computers Obtained From Surplus Property

<table>
<thead>
<tr>
<th>Agency/Computer</th>
<th>Processed by Surplus Property?</th>
<th>Did the computer contain:</th>
<th>What Appeared To Have Been Done To Remove Files?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Recoverable Files</td>
<td>Confidential Files</td>
</tr>
<tr>
<td>Adjutant General's Office</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer #1</td>
<td>Yes</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Department of Administration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer #1</td>
<td>No</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Computer #2</td>
<td>No</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Computer #3</td>
<td>No</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Kansas Health Policy Authority</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer #1</td>
<td>Yes</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Computer #2</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kansas Sentencing Commision</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer #1</td>
<td>Yes</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>AGENCIES WITHOUT RECOVERABLE FILES</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kansas Bureau of Investigation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer #1</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer #2</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insurance Department</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer #1</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AGENCY UNKNOWN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer #1</td>
<td>No</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Computer #2</td>
<td>Yes</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Computer #3</td>
<td>Yes</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Computer #4</td>
<td>Yes</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Computer #5</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOTAL FOR SAMPLE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15 Computers</td>
<td></td>
<td>6</td>
<td>10</td>
</tr>
</tbody>
</table>

Source: LPA review of computers obtained from Surplus Property.
As part of this audit, we evaluated the adequacy of the State’s enterprise-wide policies on removing data from surplus computers. Currently, there’s no stand-alone policy addressing how surplus computers should be handled. However, the State’s Information Technology Executive Council (ITEC) does include requirements for handling surplus computers in its default security policies, which establish minimum security policy requirements for agencies. ITEC currently is developing a more thorough stand-alone policy, but it’s still in draft form. Both policies have shortcomings, as described below:

- **The requirements for handling surplus computers in the default policy are difficult to find, apply only to confidential data, and have inadequate documentation requirements.** The ITEC default policies are contained in a very large document, and the policy on surplus computers is buried in a section on “physical security.” The policy specifies what should be done to remove confidential data from hard drives, but doesn’t address other types of information. It also doesn’t address documentation requirements. Proper documentation would help agencies ensure they’d removed data from all the computers leaving the agency, would allow agency security personnel to better monitor the agency’s security, and would allow officials at Surplus Property to know when they needed to do more work on a computer to ensure it didn’t have data on it when it was sold.

- **The draft stand-alone policy is much stronger, but it lacks requirements on the number of times drives should be overwritten.** The policy appears to have been largely based on current best practice. It is very complete, and includes the recordkeeping requirements that are missing from the current default policy. The draft policy lacks only a requirement on the specific number of times a drive must be overwritten (current best practice is three times), and a requirement that a specific person must sign that the work was done.

While agencies are responsible for taking care of their own data, Surplus Property is in a perfect position to act as a final control to protect data on computers that Topeka-based State agencies dispose of. Because computers from most State agencies in Shawnee County come through Surplus Property, it seems an obvious point of control to prevent any computers from being sold to the public that contain data. Surplus Property could overwrite or demagnetize all computers, unless there was a specific certification from the agency stating that the data had been properly removed.
**Conclusion:**

The fact that we were able to use simple, inexpensive software to retrieve confidential files from almost half of the 15 surplus computers we reviewed is frightening. Our review didn’t include State agencies located outside the Topeka area, but there’s little reason to think that their computer disposal practices are much better. The State has a significant problem with how surplus computers are handled, and is at significant risk of disclosing confidential or sensitive data to the public or even to potential hackers. Should that happen, the State could face both costly and embarrassing consequences.

Solving the problem with surplus computers will require a multi-tiered approach—developing strong State policies on how to remove data from surplus computers, educating agencies about those policies so they can develop their own processes, and ensuring that agencies are following those policies. For Topeka-based agencies, Surplus Property could serve as the final safety net to ensure that all the computers it disposes of have had the data removed properly. On the other hand, agencies outside of Topeka will need to be especially careful with how they handle their surplus computers, because there’s no other agency that can act as the safety net.

**Recommendations For The Information Technology Executive Council (ITEC):**

1. To help ensure that State computers don’t contain any data when they are disposed of, ITEC should adopt the ITEC Security Council’s draft media disposal policy as soon as possible.

2. To strengthen the draft media disposal policy, ITEC should add the following requirements to the policy:
   a. when overwriting a hard drive, agencies must overwrite the drive three times.
   b. in documenting removal of data from a hard drive, the agency must also document the name of the person doing the work.
3. To help ensure that all State agencies understand their responsibilities to protect data in their possession, and understand how to adequately carry out that responsibility, the Executive, Legislative, and Judicial Branch CITOs should communicate the new media disposal policy to all State agencies under their jurisdiction, and should explain the importance to all agencies of following that policy. Each CITO should take special care to ensure that agencies located outside Shawnee County understand that the State’s policy applies to them as well, because these agencies dispose of their computers directly.

4. To help ensure that all data have been removed from computers that are disposed of through Surplus Property, the Department should require that all surplus computers be accompanied by a certificate from the agency stating that all data have been properly removed from the computer. If a computer is delivered without such a certificate, Surplus Property should overwrite, demagnetize, or destroy the hard drive in conformance with best practices.

5. To help ensure that agencies are complying with the policies, the Department should monitor compliance by checking a sample of computers at Surplus Property periodically using methods similar to those we used in this audit.

6. To ensure that they don’t continue to dispose of computers with data on them, these agencies should immediately adopt policies and procedures that, at a minimum, require the following actions when disposing of a computer:

   a. The hard drive must be destroyed, demagnetized, or overwritten
   b. If the drive is overwritten, it must be overwritten at least three times
   c. Staff must document the following to certify that all data were removed:
      i. serial number of the computer
      ii. method used to eliminate the data
      iii. date the work was done
      iv. who did the work
      v. final disposition of the computer
APPENDIX A

Scope Statement

This appendix contains the scope statement for this audit of surplus computers. This audit was conducted as part of the ongoing information system security audit work authorized by the Legislative Post Audit Committee.
SCAPE STATEMENT

Surplus Computer Equipment: Determining Whether State Agencies Effectively Remove Software and Agency Data From Surplus Computers

Under State law, agencies can dispose of outdated computer equipment through the State Surplus Property Program that is operated by the Department of Administration. The equipment is first made available to individuals or entities that are eligible to participate in a similar federal program, and then is offered for sale to the public. Although staff that operate the Surplus Property Program check the computer equipment for information prior to offering it up for sale, it’s the agency’s responsibility to ensure that all proprietary software and agency data have been removed before it disposes of the equipment.

Over the last several years, numerous audit reports have been released that look at whether federal, state, and local agencies across the country do an adequate job of purging data from computers and other electronic media before disposing of them. In these reports, auditors consistently report finding proprietary software and agency data—often confidential—on computers that were about to be sold to the public. These audit findings raise concerns about how Kansas agencies prepare their surplus computer equipment for disposal.

This computer security audit would answer the following question:

1. Do State agencies effectively purge surplus computers and other electronic media of software and agency data before disposing of them? To answer this question, we would review a sample of computers and other electronic media that have been turned over to State Surplus Property to determine if they have readable data on them, including licensed operating system software, licensed application software, and data of a sensitive, personal, or confidential nature. For the computers in the sample, we would review documentation and interview officials from the agency that disposed of the equipment as necessary to understand their policies for disposing of computer equipment. For any computers or media that contain readable data, we would interview officials from the responsible agency and review documentation to determine why the data weren’t properly removed. We would conduct additional test work as necessary.

Estimated Resources: 5-7 weeks
APPENDIX B

Agency Responses

On June 6, 2008, we provided copies of the complete draft audit report to the following agencies and officials:

- the Department of Administration
- the Chair of the Information Technology Executive Council
- the Chief Information Technology Officers of the Executive, Legislative, and Judicial Branches
- the Kansas Sentencing Commission
- the Kansas Health Policy Authority
- the Adjutant General’s Office

These agencies generally concurred with the report's findings, conclusions, and recommendations. All the responses are included in this appendix. The Executive Branch Chief Technology Officer’s response is included in the Department of Administration response.
June 9, 2008

Barbara J. Hinton
Legislative Post Auditor
800 SW Jackson Street, Suite 1200
Topeka, Kansas 66612-2212

Dear Ms. Hinton:

Thank you for the opportunity to respond to the Legislative Post Audit’s report on *Surplus Computer Equipment: Determining Whether State Agencies Effectively Remove Software and Agency Data from Surplus Computers*. The Department of Administration concurs with all the recommendations and is pleased to present the following official response.

**DISC**

1. The Department of Administration Security Policy requires all surplus computers to be submitted to the DISC Bureau of Customer Services for sanitization prior to disposal. This policy has been in effect for more than ten years. A property accountable employee in one of the Divisions was under the mistaken impression that machines submitted directly to Surplus Property would be properly sanitized. Upon notification that machines were being sent directly to Surplus Property, the Bureau of Customer Services contacted division staff to assure compliance with the policy. In addition, software has been provided to Surplus Property that will enable them to perform a 7-pass disk overwrite process in accordance with DOD Standard 5220.22 M.

2. The Department concurs with the recommendation to provide a certificate with each computer stating that all data have been properly removed, in accordance with NIST publication 800-88, Appendix F, *Guidelines for Media Sanitization* (available upon request).

3. The DISC Bureau of Customer Services routinely destroys all hard drives known to have contained sensitive information.

4. The DISC Bureau of Customer Services, in conjunction with Surplus Property, will periodically audit surplus computers to assure that media are either destroyed or properly sanitized.

5. Staff has confirmed the draft ITEC data sanitization policy is on the June agenda for the State Security Council’s consideration. Upon approval, the policy will be submitted to the ITEC for their review and approval process.
June 9, 2008
Page 2

Surplus Property

1. All computers currently in stock have been removed and hard drives have been overwritten per standard set forth by the audit. The State Surplus has been working with DISC and received the DOD disc that overwrites per the standard.

2. The State Surplus will ensure that agencies are complying with the policies of the audit by checking each computer that comes into inventory and overwrite any that comes in that have not been overwritten. The State Surplus will keep records of incoming computer surplus that has not been overwritten and inform the agencies through written communication not in compliance.

3. The State Surplus has the ability for recycling any hard drives through Asset LifeCycle (this company is state and federally certified) that an agency wants destroyed instead of being overwritten.

The State Surplus will comply with all recommendations and with the addition of these policies should ensure that all surplus computers that come into the State Surplus will have all software and agency data removed.

We appreciate the opportunity to review the report and implement the recommendations. Thank you for your time and consideration.

Sincerely,

Carol L. Foreman
Deputy Secretary of Administration

cc: Duane Goossen
    Denise Moore
    Cheryl Buxton
Barbara J. Hinton
Legislative Post Auditor
800 SW Jackson Street
Suite 1200
Topeka, Ks 66612

Re: Surplus Computer Equipment Audit

Dear Ms Hinton:

Thank you for sending me a draft copy of the performance audit entitled “Surplus Computer Equipment: Determining Whether State Agencies Effectively Remove software and Agency Data from Surplus Computers.”

In response to your recommendations for CITO’s to communicate the audit findings within their branch of government, I am scheduling presentations of the audit with the Legislature’s Information Systems Team and the Systems Review Team. All IT staff are on the IS Team and the Division Directors, legislators, and Chamber staff leadership are on the Systems Review Team. In addition, I will notify the chair of the Joint committee on Information Technology about the audit and I will recommend that the committee receive testimony from state agencies, CITO’s, ITEC leadership, and ITEC Security Council senior staff about the audit findings and recommendations.

As you know, the Legislature has a very strong policy on cleansing hard drives prior to disposing computers. The policy is in section 8.7.3 of LCC Policy 51 revised. The policy reads in part: “...when computer equipment is disposed of or de-installed and staged for surplus property, all data must be wiped from the hard drives. This can be accomplished by over writing the hard drive a minimum of 3 times with software approved by the IS team or the degaussing of and physical destruction of drives...”

The policy also requires staff to remove the hard drive from any computer that is sent out for repair or it must be wiped 3 times according to the procedure outlined above. Finally the policy states that if a drive is too damaged to be wiped, then the drive must be destroyed in the presence of an legislative official (Director of Computer Services or LCITO, for example) before it is discarded.
The revised LCC Policy 51 also includes Appendix C which is a full statement of how the IRS protects confidential information. This statement represents "best practice for protecting sensitive and confidential information.

The IS Team has a written procedure for implementing LCC’s policy on cleansing disk drives when computers are sold or discarded. The written procedure is based on Department of Defense best practices and standards. The procedure requires staff to use Symantec GhostG DISK wiping software which is compliant to the DOD 5220.22M standard.

In addition, the procedure requires the filing of a certificate signed by the staff member who performed the cleansing. The certificate includes the ID tag of the machine, the date the machine was cleansed, the method used to cleanse, the name of the person who performed the procedure, and the final disposition of the machine. The procedure is the same procedure you recommend on page 10 of the audit report.

The certificates are filed with the Director of Computer Services. In order to confirm that the procedure has been enforced the Director of Computer Services will implement a confirmation procedure on a sample of all machines that are removed from service. The confirmation will use software similar to the software used in your audit. It is important that our policies and procedures include this final confirmation.

Again thank you for the audit. It is exceptionally well done. Failure to protect sensitive information is a serious breakdown and unacceptable. The IT community and senior managements must take full responsibility for its stewardship of personal and sensitive information.

Respectfully Yours,

Don Heiman
Legislative Chief Information Technology Officer
June 11, 2008

Barbara J. Hinton
Legislative Division of Post Audit
Mercantile Bank Tower
800 SW Jackson Street, Suite 1200
Topeka, Kansas 66612-2212

Dear Ms. Hinton:

I have reviewed the draft document determining whether state agencies effectively remove software and agency data from surplus computers. Thank you for the opportunity to respond to the findings in your audit report.

The report suggests that it would be best for the state to develop a stronger stand-alone policy. I look forward to reviewing and hardening the state policies in light of the results of this audit.

The Judicial Branch is only budgetarily responsible for personnel in the district courts. All operations including the leasing or purchasing of the computers is the responsibility of the county and follow county procedures. We will notify the district courts of the issues that have been raised in this report.

Sincerely,

[Signature]

Kelly O’Brien
CITO, Judicial Branch

KO:mr
June 11, 2008

Ms. Barbara Hinton
Legislative Post Auditor
Legislative Division of Post Audit
800 S. W. Jackson Street, Suite 1200
Topeka, KS  66612-2212

Dear Ms. Hinton:

Thank you for the opportunity to respond to your performance audit, *Surplus Computer Equipment: Determining Whether State Agencies Effectively Remove Software and Agency Data From Surplus Computers.*

Listed below is the recommendation applicable to the Kansas Sentencing Commission and our response.

**RECOMMENDATION:** To ensure that they don’t continue to dispose of computers with data on them, these agencies should immediately adopt policies and procedures that, at a minimum, require the following actions when disposing of a computer:

a. The hard drive must be destroyed, demagnetized, or overwritten
b. If the drive is overwritten, it must be overwritten at least three times
c. Staff must document the following to certify that all data were removed:
   i. serial number of the computer
   ii. method used to eliminate the data
   iii. the date the work was done
   iv. who did the work
   v. final disposition of the computer

**RESPONSE:** The Kansas Sentencing Commission has taken steps to ensure that computers disposed of will not contain data by requiring certification from the Division of Information Systems and Communications (DISC) that hard drive destruction and appropriate disposal has occurred for each hard drive on each computer identified for disposal. Further, the agency has amended its computer inventory to include the items mentioned above, including the date of hard drive destruction as certified by DISC.

Please contact this office if we can assist further.

Sincerely,

Helen J. Pedigo
Executive Director

700 SW Jackson Street, Suite 501, Topeka, KS 66603-3714
June 10, 2008

Ms. Barbara Hinton  
Legislative Post Auditor  
800 SW Jackson Street, Suite 1200  
Topeka, Kansas 66612-2212

Dear Ms. Hinton:

Thank you for the opportunity to respond to audit 08CC03 “Surplus Computer Equipment: Determining Whether State Agencies Effectively Remove Software and Agency Data from Surplus Computers.” We intend to adopt your recommendation to ensure that all data are removed from computers taken out of service to the Kansas Health Policy Authority (KHPA).

The audit identified one computer from KHPA that had recoverable information of a confidential nature and copyrighted files. The audit correctly notes that KHPA contracts for information technology support services through the Division of Information Systems and Communications (DISC). DISC staff members provide desktop support and maintain the inventory of computers owned by KHPA. To implement the recommendation, we are reviewing the process DISC uses to decommission KHPA computers. We will rely more heavily on DISC staff to control the computer inventory and follow the audit’s recommended procedures to eliminate data and document what happens to computers taken out of service.

We plan to implement the recommended procedure as we revise our service level agreement with DISC for FY 2009. Thank you for providing the opportunity to respond to the audit findings and recommendations.

Sincerely,

Dr. Marcia Nielsen  
Executive Director

Rm. 900-N, Landon Building, 900 SW Jackson Street, Topeka, KS 66612-1220  
www.khpa.ks.gov
June 11, 2008

Mr. Allan Foster  
Legislative Division Post Audit  
800 Southwest Jackson Street, Suite 1200  
Topeka, KS 66612-2212  

Dear Mr. Foster:  

In response to your Surplus Computer Equipment audit, I concur with your findings regarding the computer belonging to the Kansas Adjutant General’s Department.  

During the period the machine in question was removed from service and subsequently turned in to surplus, the process for turn and removal of data was insufficient. While most machines were properly configured for disposal, some were not due to incomplete policy and procedures.  

Currently, the process includes turn in to the J6 HelpDesk for inventory control and cleaning. Cleansing of data includes use of a Department of Defense-approved “wipe disk” that overwrites the hard drive a minimum of three times.  

In order to further strengthen our program, we are currently drafting new Standard Operating Procedures to better track and verify this process is occurring. The procedures will entail creating an internal HelpDesk ticket that will include tracking all the information that is included in item 6.c., Recommendations of your audit report. In addition, we will begin placing an easily identifiable colored label on each machine after it is wiped to facilitate identification of machines that have not been cleaned. This will also help State Surplus personnel in that we will ask them to not accept machines that are not so marked.  

Thank you for your evaluation of our procedures and the chance to strengthen the security of our data and network.  

CHRIS A. STRATMANN, Col, JFHQ-KS  
Chief Information Officer/J6