STATE OF
NORTH CAROLINA

INFORMATION SECURITY ASSESSMENT

IMPLEMENTATION OF ENTERPRISE SECURITY STANDARD

PERMANENT REMOVAL OF DATA FROM ELECTRONIC MEDIA

FEBRUARY 2004

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

INFORMATION SECURITY ASSESSMENT

IMPLEMENTATION OF ENTERPRISE SECURITY STANDARD

PERMANENT REMOVAL OF DATA FROM ELECTRONIC MEDIA

FEBRUARY 2004

STATE OF NORTH CAROLINA

Office of the State Auditor

Ralph Campbell, Jr.
State Auditor

2 S. Salisbury Street
20601 Mail Service Center
Raleigh, NC 27699-0601
Telephone: (919) 807-7500
Fax: (919) 807-7647
Internet http://www.osa.state.nc.us

AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Members of the North Carolina General Assembly
Council of State
Cabinet Heads
George Bakolia, State CIO
Chairman and Members IRMC

Ladies and Gentlemen:

We have completed our information security assessment of the implementation of Information Resource Management Commission (IRMC) Enterprise Security Standard Number S003, *Permanent Removal of Data From Electronic Media*. The assessment was conducted in accordance with *Government Auditing Standards* and *Information Systems Audit Standards*.

The objective of this assessment was to test a sample of computers from a variety of state agencies to determine the level of compliance with the IRMC Enterprise Security Standard Number S003, *Permanent Removal of Data From Electronic Media.* The scope of our security assessment included all computers turned in to the Department of Administration's Surplus Property Division between October 16 and November 24, 2003.

This document represents the public report of the general results of our tests and contains an executive summary that highlights the areas where improvements should be made. A separate detailed report disclosing the specific weakness and sensitive information found has be issued to each agency included in the scope of this test as prescribed in G.S. 147-64.6(c)(18).

We wish to express our appreciation to the staff at the Department of Administration's Division of Surplus Property for the courtesy, cooperation and assistance provided to us during this assessment.

North Carolina General Statutes require the State Auditor to make audit reports available to the public. Copies of audit reports issued by the Office of the State Auditor may be obtained through one of the options listed in the back of this report.

Respectfully submitted,

Ralph Campbell, Jr.

Ralph Campbell, Jr.
State Auditor

TABLE OF CONTENTS

PAGE

EXECUTIVE SUMMARY

The Office of the State Auditor conducted an information security assessment of the implementation of Information Resource Management Commission (IRMC) Enterprise Security Standard Number S003, *Permanent Removal of Data From Electronic Media* from October 16, 2003 to November 24, 2003. The primary objective of this assessment was to test a sample of computers from a variety of state agencies to determine the level of compliance with the IRMC Enterprise Security Standard. Based on our objective, we report the following conclusions.

During our test period, we selected 96 machines from a variety of state agencies that had been turned into the Department of Administration's Division of Surplus Property. Of those 96 machines we were able to perform additional tests on 70. We were not able to test 11 machines because they had hard drives that were inoperative, and 15 because the systems were turned in without a hard drive. Of the 70 machines that were actually tested for compliance with the standard, 8 appeared to have destroyed the data and met the criteria as outlined in the IRMC Security Standard. The remaining 62 machines had hard drives that were readable and we were able to gain access to all the files on the system.

For the 62 machines on which we found data, a quick review of documents and spreadsheets revealed 35 drives that contained sensitive or inappropriate data. Sensitive data is defined as any information that is not considered available to the public. The majority of the sensitive information we found on the drives was directly related to the state employee who was using the computer, such as time sheets and other official documents that contain the SSN as an identifying number. Other items we found included, but were not limited to,

- Bank Account information
- National Guard troop class attendance rosters with names and social security numbers
- Employee performance evaluations
- Documentation being kept to terminate an individual
- Loan application
- Legal claim forms
- Unemployment Claim Hearing transcripts
- Letters that included uncleared check information such as the bank, account number, check number, and amount.
- Pornography

In addition, it should be noted that all 62 computers contained information that could be used to compromise the agency network and possibly other networks. Information could be gleaned from the drives such as network identification, required settings, and password files.

Also, the computers that are sent to the Department of Corrections for repair/refurbishing are sent without making any changes to them. Any data left on the machines by the agency surplusing the equipment is available to the inmates repairing/refurbishing the machines. This information could be used for a variety of purposes including identity theft and the compromise of agency network security and data.

[This Page Left Blank Intentionally]

ASSESSMENT OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Under the North Carolina General Statutes Chapter 147-64.6, the State Auditor is responsible for examining and evaluating the adequacy of operating and administrative procedures and practices, systems of accounting, and other elements of State agencies. The objective of this assessment was to test a sample of computers from a variety of state agencies to determine the level of compliance with the IRMC Enterprise Security Standard Number S003, *Permanent Removal of Data From Electronic Media*.

SCOPE

The scope of our assessment included all computers turned in to the Department of Administration's Surplus Property Division between October 16 and November 24, 2003.

METHODOLOGY

On October 16 we took an initial sample of 8 machines already in the Surplus Property warehouse, thereafter we collected 2 or 3 from each delivery until November 24. Once a computer was selected for testing we plugged it into a monitor, mouse and keyboard to determine if the system would boot normally. We noted the results and shut down the computer. The hard drive was removed from the original computer. We then connected the hard drive to our system to analyze the drive further. If the system booted normally, nothing had been done to destroy the data. Based on that, we looked for spreadsheets and documents.

We reviewed any document or spreadsheet found for sensitive information such as Social Security Numbers (SSN), bank account numbers, or any other information that would be considered sensitive in nature. If the computer did not boot up, we would look at information on the drive to make a determination as to what had been done to the drive to prevent it from booting. In some cases the drives had been formatted. In those cases we unformatted the drive and performed the same type of search as described for computers that had been turned in with nothing done to destroy the data. Occasionally we had a computer where the partition had been removed and the drive had been formatted. In those cases we restored the partition, unformatted the drive, and searched for sensitive data. If a drive was inoperative, we did not perform any work to retrieve data.

We conducted our assessment in accordance with the standards applicable to performance audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States and *Information Systems Audit Standards* issued by the Information Systems Audit and Control Association.[1]

[1] In 1992 the State created the Information Resource Management Commission to provide statewide coordination of information technology resources planning. The IRMC provides state enterprise IT leadership including increased emphasis and oversight for strategic information technology planning and management; policy development; technical architecture; and project certification. Pursuant to North Carolina General Statute 147-33.78 numerous state officials serve on the IRMC including four members of the Council of State who are appointed by the Governor. The State Auditor has been appointed a member of the IRMC and elected as chair of the IRMC by its members.

[This Page Left Blank Intentionally]

BACKGROUND INFORMATION

North Carolina spends millions of dollars each year implementing and maintaining security systems to protect sensitive and confidential state information from those not authorized to access the information. But when it comes time to dispose of state computers, much of that concern for security appears to disappear. Instead of risking detection by trying to hack into the State network, a computer thief can just purchase surplus computers turned into the Department of Administration's Division of Surplus Property by state agencies. In most cases, sensitive information, including names, addresses, Social Security numbers and passwords, are available for anyone with relatively simple technical skills and without the risk of getting caught.

On July 9, 2002, the Information Resource Management Commission (IRMC) approved Enterprise Security Standard Number S003, *Permanent Removal of Data From Electronic Media*. This standard was established to reduce the unauthorized access to data and other records stored on electronic media. The standard required each agency to establish a procedure for certifying that data has been properly removed from equipment before it is transferred, donated, or declared surplus. Specifically the standard states that:

> "Whenever electronic storage media are moved from an authorized data user to an unauthorized data user or out of the custody of an agency, the data contained on it must be permanently removed by destroying, reformatting, degaussing, or by using a wipeout utility. The utility must be approved by the National Standards and Technology (NIST) or approved use Department of Defense (DOD) standards so that previously recorded information is not recoverable. The method of data removal will be based on what is reasonable and practical."

The State has a fiduciary responsibility to safeguard the information of its citizens as well as information sensitive in nature to the State. In today's business environment, most information is stored on computer systems where the protection of the information focuses on restricting access to the computer systems that process and store that data. Systems are designed to prevent unauthorized individuals from gaining access to the system and using that information in a manner other than its intended purpose. All of the security controls can be circumvented when an individual takes physical possession of the computer after it has been released to Surplus Property.

When an agency no longer has any use for a computer system, either because the technology of the computer has become outdated, components are no longer functioning, or a variety of other reasons, the equipment is "surplused". Normally, computers are turned over to the Division of Surplus Property, however, some agencies will dispose of their own computer systems without going through the State Surplus System.

An agency will identify all the computers to be surplused and send them to the State Surplus Property Warehouse. Once delivered to the warehouse, the computers are sorted into three categories: those to be recycled, machines to be sold to schools or other state agencies, and those to be sold to the public. The majority of machines are stacked on a pallet to be recycled. There is one recycle contractor that picks up tractor-trailer loads of the computers periodically. The recycle contractor disassembles the machines and sells the components. Those computers that were not recycled are put in two categories. The best machines are sold to schools or other state agencies. The remaining computers are sold to the public through the retail operation of Surplus Property.

If a computer selected for sale to the school program needs repair, it is sent to the Department of Corrections (DOC). DOC has a program that trains inmates to work on computer systems and uses these surplus systems to develop skills in repairing computer systems. Once the inmates have completed the repairs, the computers are returned to Surplus Property and either sold to schools or other state agencies.

ASSESSMENT RESULTS AND RECOMMENDATIONS

During our test period, we selected 96 machines from a variety of state agencies. Of those 96 machines we were able to perform additional tests on 70. We were not able to test 11 machines because they had hard drives that were inoperative, and 15 because the systems were turned in without a hard drive. Of the 70 machines that were actually tested for compliance with the standard, 8 appeared to have destroyed the data and met the criteria as outlined in the IRMC Security Standard. The remaining 62 machines had hard drives that were readable and we were able to gain access to all the files on the system.

The table below shows summary information including the number of computer systems selected by agency, whether the computer system met the IRMC Security Standard, and whether the hard drive was available to be tested.

COMPUTERS SELECTED BY AGENCY

		Security Standard		Hard Drive	
Agency	Selected	Met	Not Met	Removed	Inoperative
Agriculture	3		3		
Administrative Office of the Courts	12	2	8		2
Crime Control & Public Safety	11		6	3	2
Environment and Natural Resources	12	1	8	2	1
Justice	3		1	2	
Administration	3	3			
Commerce	5		4	1	
Corrections	8		8		
Revenue	1		1		
Health and Human Services	8	1	5	1	1
Transportation	6		2	2	2
Employment Security Commission	14	1	10	1	2
General Assembly	3		3		
NC Housing Finance Agency	2		2		
Information Technology Services (ITS)	1			1	
UNC TV	3			2	1
UNKNOWN	1		1		
TOTAL	96	8	62	15	11

We retrieved data from 62 machines. There had been a minimal effort expended to protect the data on 15 of these machines. Twelve (12) of the 15 machines had reformatted hard drives, 2 had the partitions removed, and 1 had the partition removed and had been reformatted. In all cases we were able to rebuild the partition and unformat the drives giving us access to all the data on the machine.

For the 62 machines on which we found data, a quick review of documents and spreadsheets revealed 35 drives contained sensitive data. The majority of the sensitive information we found on the drives was directly related to the state employee who was using the computer, such as time sheets and other official documents that contain the SSN as an identifying number. Other items we found included, but were not limited to,

- Bank account information
- National Guard troop class attendance rosters with names and social security numbers
- Employee performance evaluations
- Documentation being kept to terminate an individual
- Loan application
- Legal claim forms
- Unemployment Claim Hearing transcripts
- Letters that included uncleared check information such as the bank, account number, check number, and amount.
- Pornography

It should be noted that all 62 computers contained information that could be used to compromise the agency network and possibly other networks. Information could be gleaned from the drives such as network identification, required settings, and password files.

The following table shows, by agency, whether the readable data included Sensitive or Non-sensitive information and whether the agency took any efforts to make the hard disk unreadable.

HARD DRIVES NOT MEETING IRMC STANDARD

	Type of Data Found		Agency Action Taken	
Agency	Non-Sensitive	Sensitive	Formatted	Removed Partition
Agriculture	1	2		
AOC	4	4		2
Crime Control & Public Safety	2	4	1	1
DENR	2	6	1	
Dept Justice		1		
Dept of Commerce	1	3		
Dept of Corrections	4	4		
Dept of Revenue		1		
DHHS	2	3	3	
DOT	1	1	1	
ESC	5	5	6	
General Assembly	2	1		
NC Housing Finance Agency	2		2	
UNKNOWN	1			
TOTAL	27	35	13	3

In addition to the documents and spreadsheets we reviewed for sensitive data, we also performed a quick search of the pictures contained on the drives. We found pornography on five computers. Three computers only contained a small number of pictures and we believe those to be incidental contact with a page that contained the inappropriate content. However, two have been referred to the Office of the State Auditor's Investigative Audit Section for further investigation due to the habitual amount of surfing to the inappropriate sites.

COMPUTERS SURPLUSED WITHOUT HARD DRIVES

Several agencies surplus computers after removing the hard drive. Unless these hard drives are properly destroyed, these hard drives continue to contain information. It is not difficult to wipe the information from a hard drive using the proper utility or to destroy the hard drive in such a manner that will render it permanently useless.

COMPUTERS SENT TO DEPARTMENT OF CORRECTIONS

The computers that are sent to the Department of Corrections for repair are sent without making any changes to them. Any data left on the machines by the agency surplusing the equipment is available to the inmates repairing the machines. This information could be used for a variety of purposes including identity theft and the compromise of agency network security and data. If agencies were to comply with the IRMC standard, these security weaknesses would be mitigated.

RECOMMENDATIONS

Based on our review, agencies are not permanently removing the data from hard drives before turning them into Surplus Property as required by IRMC Standard S003 *Permanent Removal of Data From Electronic Media*. All agencies should comply with this standard. The Department of Administration Surplus Property Division should periodical verify that hard drives are being adequately wiped. If the drives still contain data, the computers should be returned to the agency to have the appropriate action taken to comply with the standard.

The standard itself is contradictory when it states that the data should be permanently destroyed; yet lists reformatting the drive as an option. As we exhibited, formatting a drive, as well as removing the partition does not render the data permanently unreadable as required by the standard. The IRMC needs to revisit the list of acceptable procedures for rendering the data permanently removed. The IRMC also needs to review their procedure for notifying agencies of security standards and procedures to improve compliance with the standards.

If a hard drive is removed from a computer, agencies should run a wipe utility that will permanently remove all the data existing on the hard drive and/or agencies should destroy the hard drive in such a manner that will render it permanently useless.

[This Page Left Blank Intentionally]

DISTRIBUTION OF AUDIT REPORT

In accordance with G.S. § 147-64.5 and G.S. § 147-64.6(c)(14), copies of this report have been distributed to the public officials listed below. Additional copies are provided to other legislators, state officials, the press, and the general public upon request.

EXECUTIVE BRANCH

The Honorable Michael F. Easley	Governor of North Carolina
The Honorable Beverly M. Perdue	Lieutenant Governor of North Carolina
The Honorable Richard H. Moore	State Treasurer
The Honorable Roy A. Cooper, III	Attorney General
Mr. David T. McCoy	State Budget Officer
Mr. Robert L. Powell	State Controller
Secretary Gwynn Swinson	Secretary, Department of Administration
Mr. George Bakolia	CIO, Office of the Governor

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

President Pro Tempore
Senator Marc Basnight, Co-Chair
Senator Charles W. Albertson
Senator Patrick J. Ballantine
Senator Daniel G. Clodfelter
Senator Walter H. Dalton
Senator Charlie S. Dannelly
Senator James Forrester
Senator Linda Garrou
Senator Wilbur P. Gulley
Senator Fletcher L. Hartsell, Jr.
Senator David W. Hoyle
Senator Ellie Kinnaird
Senator Jeanne H. Lucas
Senator Stephen M. Metcalf
Senator Anthony E. Rand
Senator Eric M. Reeves
Senator Robert A. Rucho
Senator R. C. Soles, Jr.
Senator Scott Thomas

Speaker of the House
Representative James B. Black, Co-Chair
Representative Richard T. Morgan, Co-Chair
Representative Martha B. Alexander
Representative Rex L. Baker
Representative Bobby H. Barbee, Sr.
Representative Harold J. Brubaker
Representative Debbie A. Clary
Representative E. Nelson Cole
Representative James W. Crawford, Jr.
Representative William T. Culpepper, III
Representative W. Pete Cunningham
Representative W. Robert Grady
Representative Joe Hackney
Representative Julia C. Howard
Representative Joe L. Kiser
Representative Edd Nye
Representative William C. Owens, Jr.
Representative Wilma M. Sherrill
Representative Thomas E. Wright

Other Legislative Officials

Mr. James D. Johnson	Director, Fiscal Research Division

Other Officials

Chairman and Members of the Information Resource Management Commission

Woody Yates	Executive Director, IRMC

ORDERING INFORMATION

Copies of this report may be obtained by contacting the:

Office of the State Auditor
State of North Carolina
2 South Salisbury Street
20601 Mail Service Center
Raleigh, North Carolina 27699-0601

Internet: http://www.ncauditor.net

Telephone: 919/807-7500

Facsimile: 919/807-7647