STATE OF NORTH CAROLINA

INVESTIGATIVE REPORT

EMPLOYMENT SECURITY COMMISSION OF NORTH CAROLINA

RALEIGH, NORTH CAROLINA

AUGUST 2010

OFFICE OF THE STATE AUDITOR

BETH A. WOOD, CPA

STATE AUDITOR

INVESTIGATIVE REPORT

EMPLOYMENT SECURITY COMMISSION OF NORTH CAROLINA

RALEIGH, NORTH CAROLINA

AUGUST 2010

STATE OF NORTH CAROLINA
Office of the State Auditor

Beth A. Wood, CPA
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.ncauditor.net

AUDITOR'S TRANSMITTAL

The Honorable Beverly Perdue, Governor
Lynn Holmes, Chairman, Employment Security Commission of North Carolina
Members of the North Carolina General Assembly

Ladies and Gentlemen:

Pursuant to North Carolina General Statute §147-64.6(c)(16), we have completed an investigation of an allegation concerning employees of the Employment Security Commission of North Carolina. The results of our investigation, along with recommendations for corrective action, are contained in this report.

Copies of this report have been provided to the Governor, the Attorney General and other appropriate officials in accordance with G.S. §147-64.6 (c) (12).

Respectfully submitted,

Beth A. Wood

Beth A. Wood, CPA
State Auditor

August 26, 2010

TABLE OF CONTENTS

INTRODUCTION

The Office of the State Auditor received a complaint through the *State Auditor's Hotline* concerning the improper use of computer equipment by employees assigned to the Information Services Section of the Employment Security Commission of North Carolina (ESC).

To conduct our investigation of this complaint, we performed the following procedures:

- Examination of relevant ESC documents and records
- Interviews with ESC employees and management
- Forensic examination of State-owned computer equipment issued to ESC employees
- Review of applicable North Carolina General Statutes, Federal regulations, and ESC policies and procedures

This report presents the results of our investigation. The investigation was conducted pursuant to North Carolina General Statute § 147-64.6 (c) (16).

[This Page Left Blank Intentionally]

ORGANIZATION OVERVIEW

The Employment Security Commission of North Carolina (ESC) was created as the Unemployment Compensation Commission by the General Assembly in a special session in 1936. The Unemployment Compensation Act provided for the payment of unemployment compensation through local employment offices.

Originally established as a three-member body, ESC was changed to a seven-member commission effective July 1, 1941. The name changed by law to the Employment Security Commission effective April 1, 1947. Currently, ESC is led by a Chairman, two deputy chairmen, two deputy commissioners, and three directors.

ESC's mission is to provide North Carolinians with high quality and accessible workforce-related services. ESC provides employment services, unemployment insurance, and labor market information to the State's workers, employers, and the public. ESC provides these services through four divisions: the Employment Services Division, the Unemployment Insurance Division, the Labor Market Information Division, and the Administrative Division.[1]

The Information Services Section within the Administrative Division is responsible for the overall computer needs for ESC. Information Services is composed of 54 positions organized into three main areas: Operations/Help Desk, Network/Software Technical Support, and Enterprise Applications. In addition, there is a UNIX Systems Administration Solaris/Linux unit within the section.

Each area is overseen by a manager who reports directly to the Information Technology Systems Manager. The Information Technology Systems Manager reports to the Chief Information Officer who leads the entire Information Services Section.

[1] http://www.ncesc.com/pms/aboutesc/history.asp

[This Page Left Blank Intentionally]

1) AN ESC SYSTEMS AND OPERATIONS ANALYST MISUSED THE STATE-OWNED NETWORK AND COMPUTERS BY INSTALLING SOFTWARE TO ILLEGALLY DUPLICATE AND DISTRIBUTE COPYRIGHTED MATERIALS.

Our examination of computers and disk drives assigned to a Systems and Operations Analyst (Systems Analyst) revealed the presence of prohibited software and copyrighted digital media such as movies and computer games. We determined through forensic analysis of the Systems Analyst's computer that software was installed to illegally duplicate copyrighted movies and computer games. The Systems Analyst admitted using his State-owned computer and the ESC telecommunications network to access and duplicate copyrighted movies and games.

United States copyright laws prohibit the unauthorized duplication and distribution of movies, computer games and software, and other digital media. Title 17 of the *United States Code*[2] provides copyright protection to "original works of authorship." Section 1201 of Title 17 specifically prohibits the circumvention of copyright protection such as encryption technology on movies and software. Section 1204 of Title 17 includes criminal penalties for violations of these restrictions. In addition, Title 18 of the *United States Code* provides additional criminal penalties for the unauthorized duplication and distribution of copyrighted works. Thus, in our opinion, by duplicating copyrighted movies and games without authorization, the Systems Analyst violated various provisions of Title 17 of the United States Code.

One of the software applications we discovered on the Systems Analyst's computer was AnyDVD, a software program produced by a company in Antigua. AnyDVD automatically decrypts copyright protection codes on DVDs and removes the FBI warning at the beginning of the movies. The software is illegal in several countries and a number of United States courts have ruled it illegal due to its sole purpose of overriding U.S. copyright protections.

Along with the AnyDVD software, forensic analysis revealed the Systems Analyst's State-owned computer contained the following:

- Eleven copyrighted movies that were stored under a folder named "DVD Rip"
- Four copyrighted movies that had been "ripped"[3]
- Ten computer games
- More than ten software applications pertaining to DVD ripping, copying, or editing. The software applications included tools used to decrypt or "crack" digital copyright protections used by the film industry to prevent illegal duplication.

[2] http://www.copyright.gov/title17/circ92.pdf

[3] Ripping is the process of copying audio or video content to a hard disk, typically from a removable media such as a compact disc.

We also discovered dozens of DVDs stacked around the Systems Analyst's desk. Some of these DVDs appeared to be commercially-obtained while numerous DVDs had the name of copyrighted movies written on the disk with a marker pen. In addition, there were numerous containers of blank DVDs. No other employee in the section had a large collection of blank discs. The Systems Analyst, co-workers, supervisors, and managers could not identify a business purpose for the numerous blank DVDs. Because of the number of movies and games contained on the Systems Analyst's State-owned computer, we believe these activities also affected his performance of official ESC duties.

The Systems Analyst admitted that he had installed various forms of DVD ripping software on his State-owned computer. He said that he purchased the software himself and that he had the license for each program. The Systems Analyst said that the ripping software was on his computer so that he could watch movies "without having to worry about the encryption thing." He also said that he owns approximately 1,200 to 1,500 movies that he has purchased and he uses the ripper programs to make copies to preserve the original and use the copies while at work. The Systems Analyst also admitted that there were video games that he had installed on his State-owned computer. When asked if he thought that this was appropriate, he said "probably not."

The Systems Analyst estimated that he stored "a bunch" of movies on his State-owned computer. When we asked him to clarify, he said "more than one and less than a thousand." He acknowledged that his understanding of the computer use policy was "work only, no personal business. The server is not for storing personal information." He added, "Some people say it is my machine, but the machine is not yours."

The Systems Analyst also said that, a couple of years ago, he maintained a "share drive" on the ESC network. He said that he downloaded movies to the share drive and it was "out there for others to use to pass the time when waiting for vendors." The Systems Analyst said that the share drive was discovered by management when he "inadvertently shared the drive." He said that he was told by his supervisor, "you have movies on your machine and you need to get them off."

The Systems Analyst also admitted that he provided some of the copied movies to other employees including managers in the Information Services Section. The Systems Analyst said that he routinely downloaded movies directly to a specific manager's computer. (See Finding 2)

We asked the Systems Analyst if any other people in his section knew about his activities of downloading and copying movies. He said that "everyone knew about the share drive for months and did nothing about it." He added that his direct supervisor received movies from him and the manager above him knew that he downloaded movies. His supervisor admitted that he received a copy of three un-aired episodes of the Showtime series, "Weeds."

The Systems Analyst said that "I understand the copyright thing; the way I view copyright laws, this is my personal use. If I make copies for friends, then that is my personal use."

In general, it is legal for an individual in the United States to purchase digital media and then make a copy for personal use. However, if the media is protected using effective copyright protection, the Digital Millennium Act (Act) makes it illegal to circumvent that protection. Therefore, the Act makes it illegal to rip most commercial DVDs as they are typically protected by encryption.

United States copyright laws include other specific provisions applicable to ripped copies of digital media. Ripping encrypted digital media for personal use is legal as long as the encryption remains in place. However, in some cases, ripped copies are not made solely for personal use but are provided to others. Some exceptions exist under the "limited fair use" exceptions to copyright laws, but unless those exceptions apply (primarily related to educational materials), distribution of ripped digital media may constitute a violation of United States copyright laws (regardless of whether the material was sold or provided free of charge).

In addition to the violations of United States copyright laws cited above, the Systems Analyst also violated ESC's Computer Use Policy. Each State agency is responsible for developing and enforcing a policy that ensures State-owned computer equipment is only used for conducting official State business. According to the ESC Internal Security Handbook, which every ESC employee must annually certify the receipt and understanding of its contents, the following rules apply:

- Licensed software may not be copied in violation of software licensing agreements for any purpose.
- All software received (purchased or otherwise) by any ESC department must be screened by the Information Utility Group or user.
- Acts of fraud and criminal malfeasance, policy violations, and misconduct will result in disciplinary action up to and including dismissal. Fraud and criminal malfeasance is any deliberate action in violation of federal or state statutes. Violations include misusing state owned property (computer equipment, telephones, real property, vehicles, etc.) for personal gain, using state supplies and equipment for personal use, and unauthorized use of computer programs in violation of copyright laws and license agreements.
- Any department or office directed to purchase or install specific software by its federal or local partners should contact the Help Desk for information. All other software downloaded and/or installed on ESC equipment must be approved by the user's management.[4]

Therefore, the Systems Analyst violated ESC's Computer Use Policy by downloading illegal software and duplicating and distributing copyrighted movies and games.

[4] ESC Internal Security Handbook

RECOMMENDATION

ESC management should take appropriate disciplinary action against the Systems Analyst. In addition, ESC management should educate all ESC employees regarding possession and distribution of copyrighted software and other digital media. Management should reinforce the importance of following State policy relative to personal use of State-owned equipment.

In addition, ESC management should implement an active computer monitoring program to ensure that State-owned systems are used appropriately in accordance with ESC policy. This program should detect instances of non-compliance and also serve as a deterrent for employees considering inappropriate activities.

2) THE ENTERPRISE APPLICATIONS MANAGER'S STATE-OWNED COMPUTER CONTAINED SOFTWARE TO ILLEGALLY DUPLICATE COPYRIGHTED MATERIAL.

The Systems Analyst told us that he regularly downloaded movies onto an Enterprise Applications Manager's (Applications Manager) State-owned computer. We examined the Applications Manager's State-owned computer and discovered that it also contained software to override encryption of copyrighted materials. The presence of this software represents a violation of Title 17 of the United States Code as well as ESC policy.

The Applications Manager's computer contained AnyDVD, a software decryption program. (See Finding 1) In addition, the Applications Manager's State-owned computer contained the following:

- Three software program applications pertaining to DVD ripping, copying or editing
- A file that contained a copyrighted movie that we determined was currently playing in movie theaters and had not been released on DVD
- Nineteen other copyrighted movies and 14 television shows that were ripped and/or stored on the Applications Manager's State-owned computer

Each State agency is responsible for developing and enforcing a policy ensuring that State-owned computer equipment is used only for conducting official State business. The Applications Manager's use of illegal software and copyrighted material violated ESC's computer use policy. According to the ESC Internal Security Handbook which every ESC employee must annually certify receipt and understanding of its contents, the following rules apply:

- Licensed software may not be copied in violation of software licensing agreements for any purpose.
- All software received (purchased or otherwise) by any ESC department must be screened by the Information Utility Group or user.

- Acts of fraud and criminal malfeasance, policy violations, and misconduct will result in disciplinary action up to and including dismissal. Fraud and criminal malfeasance is any deliberate action in violation of federal or state statutes. Violations include misusing state owned property (computer equipment, telephones, real property, vehicles, etc.) for personal gain, using state supplies and equipment for personal use, and unauthorized use of computer programs in violation of copyright laws and license agreements.
- Any department or office directed to purchase or install specific software by its federal or local partners should contact the Help Desk for information. All other software downloaded and/or installed on ESC equipment must be approved by the user's management.[5]

During our initial interview with the Applications Manager and prior to our forensic examination, he said that a review of his computer would only reveal some pictures of cars, his home improvement projects, and some music for his iPod. After we reviewed the Applications Manager's State-owned computer and determined that the computer had the AnyDVD software installed, we spoke to the Applications Manager again. He denied having any knowledge of the software being on his State-owned computer or how it was installed. The Applications Manager said because everyone in the Information Systems Section has administrator rights, anyone could have loaded the software on his computer.

The Applications Manager said that he had no idea how those programs were installed on his computer and added, "I cannot say who put them there." The Applications Manager also said, "If I knew it was there, I would have erased the damn thing. Nobody could ever prove who put it there. We are at a stalemate. I can't prove how it got there and you can't prove who put it there."

The Applications Manager denied that he had obtained and/or shared any movies with the Systems Analyst. We informed the Applications Manager that the Systems Analyst said they shared movies frequently. Again, the Applications Manager denied sharing or copying movies with the System Analyst.

Our forensic examination also determined that the copied movies were stored in an electronic folder named "Stuff2." Although the folder had been deleted, we were able to partially recover the contents to determine that the folder contained 533 files. In addition, we determined that the Applications Manager's user id accessed the folder on the day that our investigation was initiated at ESC. Thus, the folder was deleted *after* our investigation began.

Our forensic examination provided an activity log for the Applications Manager's computer. The log detailed the activity that occurred on the Applications Manager's computer for the days prior to and subsequent to our investigation. The log identified the user id assigned to the Applications Manager as the only user during that period and contained activity within the "Stuff2" folder.

[5] Ibid

According to the ESC User Group Manager, each employee has the ability to log on to any computer in the agency using their own user id and password. However, if an employee logs on using his user id and password, the system creates a log of activity under that user id. To log on to a computer using another employee's id would also require the user's password.

When we attempted to review the Applications Manager's computer, our forensic examiners could not gain access to the computer using an administrator id and password that should have allowed access. The Applications Manager told us that, two weeks prior to our meeting (two weeks into our investigation), he had installed a Windows program that blocked access to his computer. The Applications Manager said that he installed the software to test it for use by the entire agency. The Applications Manager said that he was working on it with two employees that he supervised.

The two employees contradicted the Applications Manager's claims. The first employee said that the Applications Manager had never spoken with him about anything related to blocking software and he doubted that the Applications Manager would know how to configure his computer that way. The second employee said that the Applications Manager had approached him around the time the investigation began because the Applications Manager was concerned that the Systems Analyst might be able to put something on his computer.

The second employee said that he set up the administrator id for the Applications Manager because the Applications Manager did not know how to do it. The second employee said that there was never any discussion about the need to do this for all of the other computers in the agency. He said that the only concern the Applications Manager had was the Systems Analyst's ability to access the Applications Manager's computer.

RECOMMENDATION

ESC management should take appropriate disciplinary action against the Applications Manager. In addition, ESC management should educate all ESC employees regarding possessing copyrighted software and other digital media. Management should reinforce the importance of following State policy relative to personal use of State-owned equipment.

In addition, ESC management should implement an active computer use monitoring program to ensure that State-owned systems are used appropriately in accordance with ESC policy. This program should detect instances of non-compliance and also serve as a deterrent for employees considering inappropriate activities.

3) ESC HAS INADEQUATE CONTROLS OVER THE INSTALLATION AND MONITORING OF SOFTWARE ON STATE-OWNED COMPUTERS.

The ESC Internal Security Handbook, Chapter 2.1.1 indicates that it is a breach of policy to use State–owned property (computer equipment) for personal use and to engage in the unauthorized use of computer programs in violation of copyright laws and license agreements. Our investigation determined that ESC does not actively monitor inappropriate user activity nor does it have a monitoring mechanism for detecting the presence of inappropriate software on its computers and internal telecommunications network. In addition, all ESC employees are granted administrator rights[6] on their computers. This gives individual users the ability to install any software on their computers without restriction.

Inappropriate software installed on ESC computers increases the risk that staff could un-intentionally introduce malicious code, malware, or viruses in the ESC environment and violate copyright laws and license agreements. By not restricting and monitoring software installations on agency computers, the integrity of information maintained on these computers could become vulnerable, thus causing a Personal Identification Information exposure or subjecting ESC to a potential lawsuit because of copyright or license agreement violations.

According to the ESC Chief Information Officer (CIO), ESC policy is "loose" regarding software that employees are allowed to install on their computers. He said, "We do not control the software that lives on the desktops." ESC guidelines state that, with supervisor approval, an end user can install any software. The intent is that the software may assist in the employee's work so the supervisor would be the better judge of its necessity. Further, ESC management believes that it is more efficient to allow the user to have the ability to install the software. The CIO added that he would have no way of knowing if the software was actually needed for an individual user.

The CIO said he is not responsible for finding unauthorized software on computers assigned to employees at ESC. He did not believe there was a specific written policy regarding personal software on ESC computers. The CIO said that "this has been the ESC philosophy for years" dating back to 1978. The CIO said that he would "like to lock down the desktops" for each employee and that the lack of oversight is a problem at ESC. The CIO referenced the recent application controls audit completed by the Office of State Auditor[7] that recommended that ESC install asset management software on their systems to aid in this effort. In addition, that audit found a lack of monitoring for unauthorized software.

[6] An administrator is a local account or a local security group with complete and unrestricted access to create, delete, and modify files, folders, and settings on a particular computer. This is in contrast to other types of accounts that have been granted only specific permissions and levels of access. Administrator rights are permissions granted to users allowing them to make changes such as changing settings and installing software.
[7] http://www.ncauditor.net/EPSWeb/Reports/InfoSystems/ISA-2008-4650.pdf

The Information Technology Services Manager acts as the security liaison between ESC and the North Carolina Office of Information Technology Services. His responsibilities include ensuring the security of the ESC computer network. He said that one of his jobs "should be security; however, I don't have time to do everything I need to do." As a result, he told us that he does not work on security awareness.

The Information Technology Services Manager said that the Deputy CIO brought to his attention the possible misuse of computers assigned to the Systems Analyst two years ago. He said that he addressed it at a staff meeting by conveying to supervisors that downloading software, movies, and games was not legal, was an abuse of State property, and violated copyright laws. However, the Information Technology Services Manager said that he did not feel that information was "substantial" enough to pursue. He said that he does not tend to follow-up on what he believes to be "rumors or gossip." The Information Technology Services Manager said that there were huge liabilities associated with downloading illegal software that should never be brought into a business environment. He said that he does not restrict use more actively because he can not "wear a cop's hat and then be liked by the employees." The Information Technology Services Manager said "the ESC culture leans toward employee rights rather than security."

The ESC User Group Manager said that ESC employees have the ability to load any type of software on their computers. He acknowledged that this was not a good business practice and added that it imposes a great security risk. The User Group Manager said that the Information Services Section developed best practices for computer use but the prior management did not want to implement their recommendations.

The User Group Manager said that not having written, enforced policies in place creates many different kinds of risk including a security risk and a cost-related risk such as the time needed to remove computer viruses. The User Group Manager said that he believes that the agency is getting less and less concerned with security and more concerned with the cost of business. He said, "Security is not on the radar screen, nobody looks at that at all here." Every Information Systems Section employee we interviewed said that they believed that current ESC policy was too loose by allowing administrator rights to all employees and giving employees the freedom to install software programs.

RECOMMENDATION

The Chief Information Officer and other ESC Information Services Section management officials should implement and enforce policies that restrict the ability of employees to download and install software programs. ESC employees should be granted the lowest level of information systems access necessary to perform their jobs. The Information Services Section should have the ability to control and monitor software applications on every networked ESC computer.

The Chief Information Officer and other ESC Information Services Section management officials should establish a monitoring mechanism for detecting the unauthorized

installation of copyrighted or personal software. Managers should investigate and take appropriate action in response to reports of employee misuse of State-owned computers.

The Chairman should ensure that the Chief Information Officer and other ESC Information Services Section management officials take the above recommended actions to protect ESC's networks, equipment, and data. The Chairman should monitor the actions taken to address these concerns. In addition, the Chairman should communicate to all ESC operational units the importance of the increased security and monitoring efforts.

[This Page Left Blank Intentionally]

AUDITOR'S NOTE

In its response to this investigative report, the Employment Security Commission (ESC) notes that the Office of the State Auditor (OSA) "began an investigation in August 2009" and that "ESC received the official report of the investigation on July 13, 2010." Investigations are not conducted within a pre-determined time frame; instead, investigations require enough time to allow investigators to obtain sufficient, appropriate evidence to support all conclusions. Moreover, the ESC response does not acknowledge that OSA provided ESC management significant documentation throughout September, October, and November 2009 that enabled ESC to make decisions regarding disciplinary action. Further, OSA maintained contact with the ESC Human Resources Director, prior Chairman, and current Chairman throughout the investigative process.

In addition, the response notes that ESC "created a proposed report and drafted a procedure" in response to findings from this investigation and an OSA Information Systems audit report released November 13, 2008. The Chairman told us that procedure should become effective September 1, 2010, nearly 22 months after the Information Systems audit report was released. OSA Information Systems auditors confirmed that earlier implementation of their recommendations may have prevented or detected the inappropriate use of the State-owned network and computers as identified in this investigative report.

[This Page Left Blank Intentionally]

Employment Security Commission of North Carolina
Post Office Box 25903, Raleigh, NC 27611 919-733-7546

Beverly Eaves Perdue
Governor

Lynn R. Holmes
Chairman

July 27, 2010

Beth A. Wood, CPA
State of North Carolina
Office of State Auditor
20601 Mail Service Center
Raleigh, NC 27699-0601

RE: Investigative Report

Dear Ms. Wood:

Enclosed please find the Employment Security Commission's (ESC) response to your office's investigation of a complaint made through the State Auditor's Hotline concerning improper use of computer equipment by employees assigned to the Information Services section of ESC. Pursuant to N.C.G.S. §147-64.6(c)(16), your office began an investigation of the matter in August 2009. The ESC received the official report of the investigation on July 13, 2010.

Recommendations: ESC management should take appropriate disciplinary action against the Systems Analyst and the Applications Manager.

ESC management should educate all ESC employees regarding possession and distribution of copyrighted software and other digital media, and reinforce the importance of following State policy relative to personal use of State-owned equipment.

ESC management should implement an active computer monitoring program to ensure that State-owned systems are used appropriately in accordance with ESC policy. This program should detect instances of non-compliance and also serve as a deterrent for employees considering inappropriate activities.

Responses: The Systems Analyst was terminated effective October 16, 2009. The Applications Manager was placed on Disciplinary Suspension without pay for ten (10) work days, effective November 16 through November 27, 2009. Additional disciplinary action is currently under review.

The ESC has updated its Internal Security Handbook and has developed a new Computer Use Policy – pending final management review prior to their release in August 2010. Both documents will require an annual review by all employees along with a signed certification that

the contents have been read and understood as a part of the annual performance review process. ESC will provide periodic security and computer use reminders to all staff.

The ESC will implement and enforce policies that restrict the ability of employees to download and install software programs, as well as adopt other such policies as are deemed necessary and appropriate to enhance and maintain the security and operational integrity of agency automated systems. All such policies will be reviewed in terms of currency, technical adequacy and operational effectiveness on a periodic basis.

In order to emphasize the appropriate use of State-owned computers, software and systems, all ESC networked computers display the following message at login:

> *This is a government computer system operated for authorized state business by the Employment Security Commission of North Carolina. Unauthorized or improper use of this system may result in administrative action and/or civil and criminal penalties. Use of this system constitutes consent to monitoring.*

Recommendation: The Chief Information Officer and other ESC Information Services section management officials should implement and enforce policies that restrict the ability of employees to download and install software programs. ESC employees should be granted the lowest level of information systems access necessary to perform their jobs. The Information Services section should have the ability to control and monitor software applications on every networked ESC computer.

The Chief Information Officer and other ESC Information Services section management officials should establish a monitoring mechanism for detecting the unauthorized installation of copyrighted or personal software. Management should investigate and take appropriate action in response to reports of employee misuse of State-owned computers.

The Chairman should ensure that the Chief Information Officer and other ESC Information Services section management officials take the above-recommended actions to protect ESC's networks, equipment and data. The Chairman should monitor the actions taken to address these concerns. In addition, the Chairman should communicate to all ESC operational units the importance of increased security and monitoring efforts.

Response: In a finding from an earlier audit report, the auditors recommended that the ESC IS section institute a periodic RACF review by data owners of all individuals with access to their data. In response to this recommendation, the ESC IS Division has created a proposed report format and drafted a procedure for the distribution and reconciliation of the information resulting from that report. The draft procedure and a sample data report have been provided to the data owners for review. The procedure is expected to be approved by management in early August 2010 with implementation of the production process following later in August 2010.

The ESC IS Division has prepared a policy to increase security for access by system administrators. Additionally, the ESC IS Division is in the process of drafting the procedures and associated support documentation required for implementation of the policy. The final draft of the policy and all related materials are expected to be approved by management in early August 2010 with implementation of the production process following later in August 2010.

Sincerely,

Lynn R. Holmes T.H.H.Jr.

Lynn R. Holmes
Chairman

[This Page Left Blank Intentionally]

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