STATE OF NORTH CAROLINA

INFORMATION SECURITY VULNERABILITY ASSESSMENT

PRELIMINARY STATEWIDE ASSESSMENT (PHASE I)

COMPREHENSIVE VULNERABILITY ASSESSMENT (PHASE II)

AT

DEPARTMENT OF REVENUE

DEPARTMENT OF STATE TREASURER

OFFICE OF THE STATE CONTROLLER

DEPARTMENT OF HEALTH AND HUMAN SERVICES

DECEMBER 2002

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

INFORMATION SECURITY VULNERABILITY ASSESSMENT

PRELIMINARY STATEWIDE ASSESSMENT (PHASE I)

COMPREHENSIVE VULNERABILITY ASSESSMENT (PHASE II)

AT

DEPARTMENT OF REVENUE

DEPARTMENT OF STATE TREASURER

OFFICE OF THE STATE CONTROLLER

DEPARTMENT OF HEALTH AND HUMAN SERVICES

DECEMBER 2002

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
Secretary E. Norris Tolson
Secretary Carmen Hooker Odom
Treasurer Richard H. Moore
Controller Robert L. Powell
George Bakolia, CIO

Ladies and Gentlemen:

The Office of the State Auditor, in consultation and coordination with Information Technology Services, undertook a series of projects to evaluate the network and computer security in place over computer operations within state government.

In early May 2001, the Office of the State Auditor used a private contractor to attempt to penetrate the network security systems at 22 of the state's computer systems in the Executive, Judicial and Legislative branches of state government. The Office of the State Auditor then initiated a series of information security assessments of the North Carolina Department of Revenue, Department of State Treasurer, Office of the State Controller, and Department of Health and Human Services. These assessments were conducted during the period from December 11, 2001 through September 13, 2002. The assessments were conducted under the authority granted by North Carolina G.S. 147-64.6(c)(18) which states:

> The Auditor shall, after consultation and in coordination with the State Chief Information Officer, assess, confirm, and report on the security practices of information technology systems. If an agency has adopted standards pursuant to G.S. 147-33.82(d)(1) or (2), the audit shall be in accordance with those standards. The Auditor's assessment of information security practices shall include an assessment of network vulnerability. The Auditor may conduct network penetration or any similar procedure as the Auditor may deem necessary. The Auditor may investigate reported information technology security breaches, cyber attacks, and cyber fraud in State Government. The Auditor shall issue public reports on the general results of the reviews undertaken pursuant to this subdivision, but may provide agencies with detailed reports of the security issues identified pursuant to this subdivision which shall not be disclosed as provided in G.S. 132-6.1(c)….

AUDITOR'S TRANSMITTAL (CONCLUDED)

This report represents the **general** results of our assessments. A detailed report containing the conditions found and recommended corrective action was provided to each agency at the conclusion of our fieldwork.

The primary objective of these assessments was to evaluate the security controls over the information network at the Agency. The scope of our assessment included security policies, network architecture, network vulnerability, host vulnerability, and other security areas.

We wish to express our appreciation to the staff at each agency for the courtesy, cooperation and assistance provided to us during this audit.

North Carolina General Statutes require the State Auditor to make reports available to the public. Copies of 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

EXECUTIVE SUMMARY

The Office of the State Auditor, in conjunction with Information Technology Services, undertook a series of projects to evaluate the network and computer security in place over computer operations within state government.

In early May 2001, the Office of the State Auditor used a private contractor to attempt to penetrate the network security systems at 22 of the state's computer systems in the Executive, Judicial and Legislative branches of state government. These penetration tests were performed in the presence of the Agency Head and Information Systems Director. Using a "Pass-Fail" grading formula, 21 of the 22 systems were rated as "Failed" because access to a computer or device identified as owned by the agency was achieved. The contractor employed by the Office of the State Auditor was able to take control of computers on the 21 systems, using programs that are readily available to hackers and the public. One system was not successfully attacked because the vulnerability identified was actually on a computer hosted by a different agency.

To further evaluate the effectiveness of the State's computer security, a comprehensive information security assessment was performed at the Department of Revenue, Department of Treasurer, Office of the State Controller, and Department of Health and Human Services. Funding for these assessments was provided from the Terrorism Defense Fund. The goal of the security assessment was to assist the agencies with achieving a "best practices" level of information security in order to protect agency internal systems, data, and assets.

The comprehensive information security assessment focused on five key areas:

- Security Policy Assessment, which evaluates the implementation of security policies and procedures.
- Network Architecture Assessment, which is a detailed review of a network design.
- Network Vulnerability Assessment, which provides a thorough understanding of security-related weaknesses and exposures in networks.
- Host Vulnerability Assessment, which reviews the current security configuration of mainframes and operating systems.
- Secure Build Review (DOR only), which is a security analysis in a non-production environment for the build procedure for a desktop client computer.

Our assessments identified security controls within each agency that were well defined and effective as well as several controls that posed extreme security risks and exposed the agency to possible internal or external attack. Control weaknesses were classified in relation to the level of risk as High, Medium, or Low. Based on the number and severity of the control weakness identified, the overall risk that the agency or state network could be compromised is High.

[This Page Left Blank Intentionally]

OBJECTIVES AND SCOPE

PHASE I - PRELIMINARY STATE-WIDE ASSESSMENT

The Office of the State Auditor (OSA) contracted with Affiliated Computer Services, Inc. (ACS) to conduct an External Network Penetration Test on the State of North Carolina's (State) networks from May 3, 2001 to May 11, 2001. The purpose of this assessment was to determine the vulnerability of the State's systems from a peripheral attack-ACS Engineers established that the State Network was at a ***high risk for Internet-based attacks.***

OSA identified the following agencies as critical components of the State's information processing system and subject to the external penetration test. These agencies process the critical information systems for the Executive, Legislative, and Judicial branches of state government.

Office of the State Auditor
Administrative Office of the Courts
Department of Administration
Department of Agriculture
Office of Budget and Management
Department of Commerce/Employment Security Commission
Office of the State Controller
Department of Corrections
Department of Crime Control and Public Safety/Highway Patrol
Department of Environment and Natural Resources
Department of Health and Human Services
North Carolina General Assembly
Office of Information Technology Services
Department of Insurance
Department of Justice
Department of Labor
Department of Public Instruction
Department of Revenue
Office of the Secretary of State
Office of State Personnel
Department of Transportation
Department of State Treasurer

The External Network Penetration Test was broken into four separate, relative, phases-they are as follows:

PHASE 1 - INTELLIGENCE GATHERING

In Phase 1 ACS Security Engineers attempted to gather as much data as possible about each Agency in the North Carolina government. The contractors used common communications protocols and applications to determine what information was available to the general public regarding the State's network. This information was reviewed to determine whether it offered potential intruders an adequate view of the network infrastructure from which the intruder could develop a blueprint of the network.

PHASE 2 - ACTIVE RECONNAISSANCE

ACS Security Engineers began Phase 2 by identifying specific hosts and services accessible from the Internet. This was accomplished using a combination of "hacker" utilities, along with ACS's internally developed audit tools. The end state of Phase 2 generated a partial list of accessible hosts, and a list of possible services offered by the hosts.

PHASE 3 - ATTACK AND TOEHOLD

In Phase 3, ACS Security Engineers tested vulnerabilities of popular services offered on various hosts that allow undetected, unauthorized, access to the State's network. The engineers accomplished this task by activating a combination of "hacker" utilities and ACS internally developed auditing tools. In cases where automated scanners did not determine the nature of a specific service, security engineers connected directly to the service verifying security issues on any host. The overall goal of this phase was to gain, using all possible attack methods, user level access to (at least) one host in each state agency.

PHASE 4 - PRIVILEGE ESCALATION

Upon the request of the Auditor's Office, Phase 4 of the External Network Penetration Test was modified allowing for a more controlled approach. The ACS team manually demonstrated their ability to increase their privileges on host sites managed by each Agency in the presence of the Agency Head (or Chief Deputy) and the Information Systems Director. This technique provided a real-time perspective for agency representatives regarding the amount of time required to penetrate the networks and gain control of proprietary agency information. This approach provided an additional buffer (if target machines broke down during the attack-responsible individuals could be notified immediately) for service restoration.

In almost every case, the contractor had full control of an agency computer or device in 30 minutes or less. In some cases, the contractor was able to monitor work being done on the agency computer, while having complete control over that computer. After taking control of the computer, the contractor could monitor network traffic, capture other user ids and passwords, and launch other attacks. These attacks were never detected by either the agency or Information Technology Services. The contractor was successful in penetrating 21 of the 22 agencies identified as part of this test.

One agency was not successfully attacked because the vulnerability that was identified and exploited was actually on a device owned by a different agency. The contractor was only given an hour and 30 minutes to successfully attack an agency and was unable to complete a second attack in the remaining time.

Conclusion

At the time of our testing, the State of North Carolina was at a high risk of having their network compromised by unauthorized users via the Internet. The security posture of the State's network offered little protection from hacker attacks via the Internet. ACS Engineers identified serious vulnerabilities that ultimately may compromise the internal State network. Detailed reports describing the weaknesses identified and recommendations for corrective action were provided to each agency and to Information Technology Services. These security enhancements have been acted upon.

PHASE II - COMPREHENSIVE VULNERA BILITY ASSESSMENT

At the conclusion of the Preliminary Statewide Assessment, several agencies volunteered to have a more comprehensive assessment performed on their agency. Among those agencies were the Department of Revenue, Department of State Treasurer, Office of the State Controller, and Department of Health and Human Services. The consulting firm of @stake, Inc. was selected to perform the assessments at the Department of Revenue, Department of State Treasurer, and Office of the State Controller. The assessment for the Department of Health and Human Services was performed by Affiliated Computer Services, Inc. (ACS).

OBJECTIVES AND SCOPE (CONTINUED)

The comprehensive assessment of the production networks at these agencies included five key areas: Security Policy Assessment, Network Architecture Assessment, Network Vulnerability Assessment, Host Vulnerability Assessment, and Secure Build Review (DOR only). The table below shows the test work that was done at each agency.

AGENCY	Security Policy Assessment	Network Architecture Assessment	Network Vulnerability Assessment	Host Vulnerability Assessment	Secure Build Review
Department of Revenue	X	X	X	X	X
Department of State Treasurer	X	X	X	X	
Office of the State Controller	X	X	X	X	
Department of Health and Human Services			X	X	

Security Policy Assessment

The Security Policy Assessment had the following key objectives:

- Evaluate current security policies and practices - This involved a review of the security policy and its associated procedures for completeness, accuracy, and appropriateness. In addition, current incident response policies and procedures were reviewed.
- Provide recommendations based on best practices and knowledge of client's business objectives and organizational infrastructure.

Network Architecture Assessment

The Network Architecture Assessment focused on the internal network infrastructure, Wide Area Network (WAN) connections to remote locations, and Internet connectivity through the North Carolina Integrated Information Network. During the engagement, the business and technical requirements of the current network infrastructure were examined in order to conduct an analysis to ensure the proper balance among functionality, cost, and security. The engagement had the following key objectives:

- Interview business and technical representatives to gain a solid understanding of business objectives and requirements
- Review technical requirements for the network
- Review required data flows

- Assess security zones and access controls
- High-level review of the host and network management strategy
- High-level review of the enterprise backup strategy
- High-level review of the enterprise virus strategy
- Identify applicable industry best practices
- Identify and validate security issues of immediate consequence
- Develop long-term recommendations to enhance security
- Transfer knowledge

The assessment was divided into the following key areas:

- Network Overview
- Segmentation Model
- IP Routing
- Redundancy
- Encryption
- Remote Access
- Network Management
- Anti-Virus
- Intrusion Detection Systems
- Backups
- Firewalls

Network Vulnerability Assessment

After obtaining an understanding of the network architecture, an assessment of the network vulnerabilities was performed. This part of the engagement examined the configuration of network devices, firewalls, and public web servers to provide a current view of vulnerabilities and threats. The engagement had the following key objectives:

- Perform reconnaissance to develop a picture of the network, including topology, devices and hosts, and services for correlation against provided information and documentation
- Assess network device configuration for vulnerabilities or insecure configurations

- Use active probing to assess network security features such as firewall configuration, intrusion detection systems (IDS), and virtual private networks for vulnerabilities or insecure configuration
- Analyze rule set on the perimeter firewall
- Assess the configuration and architecture of directory services
- Assess security configuration of the mainframe environment
- Identify and validate vulnerabilities in network components, and overall architecture
- Identify quick fixes for vulnerabilities
- Develop long-term recommendations to enhance security

The assessment consisted of a review of devices owned and maintained by each agency and devices owned and maintained by Information Technology Services.

Host Vulnerability Assessment

A Host Vulnerability Assessment of the agency's client services and supporting infrastructure was performed to provide a current view of vulnerabilities and threats. The engagement had the following key objectives:

- Assess server configuration (domain controllers, web servers, application servers, database servers) for vulnerabilities or insecure configurations
- Identify and validate vulnerabilities in network and server components, and overall architecture
- Identify quick fixes for vulnerabilities
- Develop long-term recommendations to enhance security

The assessment consisted of a review of a number of hosts owned and maintained by the agency.

Secure Build Review (Department of Revenue Only)

The Secure Build Review examined the build process created by the Information Technology group (within the Department of Revenue) for building desktop client computers. The engagement had the following key objectives:

- Interview technical and business representatives to gain a solid understanding of the demands placed upon the system and how they impact the host
- Review the intended use of the platform to understand requirements and tailor recommendations

- Establish secure build methodology for evaluating the build
- Examine existing hosts in the production environment for the application of patches and upgrades
- Assess operating system configuration, including: insecure services, permissions, and registry settings as well as unnecessary services and packages
- Identify and validate security issues of immediate consequence
- Develop recommendations to enhance security

Findings

A number of conditions were found at each of the agencies that could be strengthened to improve network security. Some of these weaknesses were significant enough to allow unauthorized access, data manipulation, or data destruction. Each weakness was classified according to its relative risk using the following definitions.

- High-level Risk: Defined as a vulnerability that could cause grave consequences if not addressed and remedied immediately. This type of vulnerability is evident within the most sensitive portions of the network, as identified by the data owner. This vulnerability could cause network functionality to cease or control of the network could be gained by an intruder.
- Medium-level Risk: Defined as a vulnerability that should be addressed within the near future. There is urgency in correcting this type of vulnerability, however; this may be either a more difficult exploit to perform, or of lesser concern to the data owner.
- Low-level Risk: Defined as a vulnerability that should be fixed; however, it is unlikely that this vulnerability alone would allow the network to be exploited and/or it is of little consequence to the data owner.

Department of Revenue

Vulnerabilities identified at the Department of Revenue were summarized into the following categories. The overall risk level was **moderate** based on the controls identified at the Department and the following number of network vulnerabilities:

- High-level Risks: 7 found
- Medium-level Risks: 7 found
- Low-level Risks: 5 found

Department of State Treasurer

Vulnerabilities identified at the Department of State Treasurer were summarized into the following categories. The overall risk level was **high** based on the controls identified at the Department and the following number of network vulnerabilities:

- High-level Risks: 5 found
- Medium-level Risks: 6 found
- Low-level Risks: 2 found

Office of the State Controller

Vulnerabilities identified at the Department of the State Controller were summarized into the following categories. The overall risk level was **moderate** based on the controls identified at the Office and the following number of network vulnerabilities:

- High-level Risks: 4 found
- Medium-level Risks: 2 found
- Low-level Risks: 1 found

Department of Health and Human Services

The vulnerability assessment performed at the Department of Health and Human Services took place at nine divisions within the Department. Each division was evaluated and reported on separately however the results have been consolidated for this report.

The overall risk level is **high** based on the controls identified at the Department and the following number of network vulnerabilities:

- High-level Risks: 23 found
- Medium-level Risks: 6 found
- Low-level Risks: 3 found

Each agency was provided with a detailed report that provided the specifics for the vulnerabilities identified along with specific recommendations for corrective action. In addition, vulnerabilities that effected devices under the control of Information Technology Services were identified in each of the four agency assessments. These vulnerabilities and the details related to each issue were disclosed to ITS for corrective action.

NEXT STEPS

The four agencies that volunteered to participate in this vulnerability assessment should be commended for their concern for information systems security. The results of these tests will assist both the agency and ITS in strengthening network security, however every agency in state government should be subject to the same level of assessment. A thorough vulnerability assessment should be performed at each state agency with follow-up assessments performed on a regular basis.

By participating in these assessments, the Office of the State Auditor's Information Systems Audit Division is developing the skills and testing expertise to perform these tests in the future. To be successful in these efforts, OSA must acquire the testing software necessary to analyze networks for vulnerabilities, establish testing facilities, and continue to receive specialized training in the latest advances in networks and the related vulnerabilities.

[This Page Left Blank Intentionally]

North Carolina Department of Revenue

Michael F. Easley
Governor

E. Norris Tolson
Secretary

August 23, 2002

Mr. Ralph Campbell, State Auditor
2 South Salisbury Street
20601 Mail Service Center
Raleigh, NC 27699-0601

Dear Mr. Campbell:

The Department of Revenue would like to extend our appreciation to the Office of the State Auditor for its assistance with the security vulnerability assessment performed by @stake last fall. We were very pleased with the results of the study and are moving forward with the implementation of the recommendations.

@stake did an excellent job of working with the staff at DOR in a cooperative and effective manner, while thoroughly assessing our operating environment. They demonstrated a comprehensive knowledge of the subject matter and communicated effectively at all levels of the organization.

Thank you for the efforts of the resources from the Office of the State Auditor, as well, in this very successful endeavor.

Sincerely,

E. Norris Tolson
Secretary of Revenue

cc: Reggie Hinton, Deputy Secretary
Randy Barnes, Assistant Secretary-IT
Martin Hefley, Director of Security

NORTH CAROLINA

DEPARTMENT OF STATE TREASURER

RICHARD H. MOORE
STATE TREASURER

325 NORTH SALISBURY STREET
RALEIGH, NORTH CAROLINA 27603-1385

July 25, 2002

The Honorable Ralph Campbell, Jr.
State Auditor of North Carolina
20601 Mail Service Center
Raleigh, NC 27699-0601

Dear Mr. Campbell:

I acknowledge receipt of the Information Technology assessment detailed report that was conducted under the authority granted by North Carolina G.S. 147-64.6(c)(18).

I applaud your efforts to insure the safety of the Department of State Treasurer network by performing the assessment. Conditions were found that require immediate attention. Pursuant to our conversations, it is my understanding that your office will continue to expedite this matter so that appropriate corrective action can be taken as soon as possible.

Thank you, and I look forward to a continued partnership in the future on this very important issue. If you have any questions, please feel free to contact our Chief Information Officer Bill Golden at 715-7516.

Sincerely,

Richard H. Moore

RHM/sls

Fax: (919) 508-5167 Phone: (919) 508-5176 website: www.treasurer.state.nc.us
The Department of State Treasurer includes Local Government Commission Teachers' and State Employees' Retirement System, Local Governmental Employees' Retirement System, Public Employees' Social Security Agency. Legislative Retirement Fund, Escheats Fund, and Tax Review Board.
An Affirmative Action/Equal Opportunity Employer

State of North Carolina
Office of the State Controller

Michael F. Easley, Governor

June 28, 2002

Robert L. Powell, State Controller

The Honorable Ralph Campbell, Jr.
State Auditor
Office of the State Auditor
2 South Salisbury Street
2601 Mail Service Center
Raleigh, North Carolina 27699-0601

Dear Mr. Campbell,

I have reviewed the confidential report, dated June 18, 2002, which resulted from the information security assessment conducted by the Office of the State Auditor and @Stake during the period of April 10, 2002 through May 31, 2002 under the authority granted by North Carolina General Statute §147-64.6(c)(18).

I am pleased to report that several corrective actions have already been taken to ensure compliance with the recommendations. As noted in your report, many of these recommendations were acted upon prior to the completion of the assessment. Other recommendations, some of which will require considerable effort and training on the part of our staff, as well as funding to purchase additional security-related infrastructure services, are also being considered. These recommendations will be prioritized, and implemented, based upon resource availability.

Please be assured that the Office of the State Controller takes an active role in security and is committed to doing their part in protecting the State's investments in technology systems and data by maintaining a secure network. We appreciate the opportunity to have been included in this assessment, as well as the professional manner with which this assessment was conducted.

Sincerely,

Robert L. Powell
State Controller

North Carolina Department of Health and Human Services
2001 Mail Service Center • Raleigh, North Carolina 27699-2001
Tel 919-733-4534 • Fax 919-715-4645

Michael F. Easley, Governor

Carmen Hooker Odom, Secretary

November 13, 2002

TO: Ralph Campbell, State Auditor

FROM: Carmen Hooker Odom

Carmen Hooker Odom

RE: Security Audit

The Department would like to acknowledge the Security Audit and Assessment performed in October 2002. The Office of the State Auditor and the Department of Health and Human Services (DHHS) completed audit as a joint effort.

DHHS has reviewed and discussed the findings with staff from the Office of the State Auditor. DHHS is taking the appropriate actions and steps to correct the identified items from the audit. The Auditor concurs with the steps being taken.

Should other information be needed please let us know.

Location: 101 Blair Drive • Adams Building • Dorothea Dix Hospital Campus • Raleigh, N.C. 27603
An Equal Opportunity / Affirmative Action Employer

State of North Carolina
Office of Information Technology Services

Michael F. Easley, Governor **George Bakolia, State Chief Information Officer**

November 4, 2002

Ralph Campbell, Jr., State Auditor
Office of the State Auditor
2 S Salisbury Street
20601 Mail Service Center
Raleigh, NC 27699-0601

Dear Mr. Campbell:

As part of your efforts to support the state's terrorism preparedness initiatives related to information technology, you conducted vulnerability assessments at the Department of Health and Human Services, Department of Revenue, Department of the State Treasurer, and the Office of the State Controller. The Office of Information Technology Services, ITS, was included within the scope of this effort as it is an information technology service provider to these four agencies.

I want to assure you that ITS has carefully reviewed each condition you identified to me during this process. Whenever possible, corrective actions have been taken to mitigate identified areas of risk and enhance security on the state's network infrastructure. Several suggestions addressed areas that posed no immediate risk but noted that additional measures could be taken over time to improve security. These types of items have also been incorporated into our plans. As soon as I receive a comprehensive list of all your agency findings, I will be proposing statewide standards to improve agency security measures in the areas identified by your vulnerability assessments.

ITS is very supportive of efforts to promote a secure information technology operational environment in state government. Information security matters are one of my top priorities. Please contact me or Ann Garrett, ITS Chief Security Officer, if you have any questions regarding this matter.

Yours truly,

George Bakolia

George Bakolia

Cc: Ann Garrett

[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 Carmen Hooker Odom	Department of Health and Human Services
Secretary E. Norris Tolson	Department of Revenue
Mr. George Bakolia	State Chief Information Officer

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

Senator Marc Basnight, Co-Chairman
Senator Charlie Albertson
Senator Frank W. Ballance, Jr.
Senator Charles Carter
Senator Kever Clark
Senator Daniel G. Clodfelter
Senator Walter H. Dalton
Senator James Forrester
Senator Linda Garrou
Senator Wilbur P. Gulley
Senator Kay R. Hogan
Senator David W. Hoyle
Senator Ellie Kinnaird
Senator Howard N. Lee
Senator Jeanne H. Lucas
Senator R. L. Martin
Senator William N. Martin
Senator Stephen M. Metcalf
Senator Fountain Odom
Senator Aaron W. Plyler
Senator Eric Miller Reeves
Senator Dan Robinson
Senator Larry Shaw
Senator Robert G. Shaw
Senator R. C. Soles, Jr.
Senator Ed N. Warren
Senator David F. Weinstein
Senator Allen H. Wellons

Representative James B. Black, Co-Chairman
Representative Martha B. Alexander
Representative Flossie Boyd-McIntyre
Representative E. Nelson Cole
Representative James W. Crawford, Jr.
Representative William T. Culpepper, III
Representative W. Pete Cunningham
Representative Beverly M. Earle
Representative Ruth M. Easterling
Representative Stanley H. Fox
Representative R. Phillip Haire
Representative Dewey L. Hill
Representative Mary L. Jarrell
Representative Maggie Jeffus
Representative Carolyn Justus
Representative Edd Nye
Representative Warren C. Oldham
Representative William C. Owens, Jr.
Representative E. David Redwine
Representative R. Eugene Rogers
Representative Drew P. Saunders
Representative Wilma M. Sherrill
Representative Ronald L. Smith
Representative Gregg Thompson
Representative Joe P. Tolson
Representative Russell E. Tucker
Representative Thomas E. Wright
Representative Douglas Y. Yongue

Other Legislative Officials

Representative Philip A. Baddour, Jr.	Majority Leader of the N.C. House of Representatives
Senator Anthony E. Rand	Majority Leader of the N.C. Senate
Senator Patrick J. Ballantine	Minority Leader of the N.C. Senate
Representative N. Leo Daughtry	Minority Leader of the N.C. House of Representatives
Representative Joe Hackney	N.C. House Speaker Pro-Tem
Mr. James D. Johnson	Director, Fiscal Research Division

Other Officials

Chairman and Members of the Information Resource Management Commission

December 13, 2002

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