



STATE OF NORTH CAROLINA

INFORMATION SECURITY VULNERABILITY ASSESSMENT

NORTH CAROLINA OFFICE OF THE STATE AUDITOR

RALEIGH, NORTH CAROLINA

OCTOBER 2006

OFFICE OF THE STATE AUDITOR

LESLIE W. MERRITT, JR., CPA, CFP

STATE AUDITOR

INFORMATION SECURITY VULNERABILITY ASSESSMENT

NORTH CAROLINA OFFICE OF THE STATE AUDITOR

RALEIGH, NORTH CAROLINA

OCTOBER 2006



STATE OF NORTH CAROLINA
Office of the State Auditor

Leslie W. Merritt, Jr., CPA, CFP
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 Michael F. Easley, Governor
Members of the North Carolina General Assembly
N. C. Office of the State Auditor
Leslie W. Merritt, Jr., State Auditor
George Bakolia, CIO, Information Technology Services

Ladies and Gentlemen:

The Office of the State Auditor, in consultation and coordination with Information Technology Services, undertook a project to evaluate the network and computer security in place over computer operations at the Office of the State Auditor.

In April and May 2006 the Office of the State Auditor used a private contractor to perform a comprehensive vulnerability assessment of the network and computer security at the Office of the State Auditor.

This report represents the general results of our assessment. A detailed report containing the conditions found and recommended corrective action was provided to the Office of the State Auditor 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, secure build review, and wireless site 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,

A handwritten signature in cursive script that reads "Leslie W. Merritt, Jr.".

Leslie W. Merritt, Jr., CPA, CFP
State Auditor

OBJECTIVES AND SCOPE

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

In April and May 2006, the Office of the State Auditor used a private contractor to perform a comprehensive information security assessment of the Office of the State Auditor. The goal of the security assessment was to assist the Office of State Auditor with achieving and maintaining a “best practices” level of information security in order to protect agency internal systems, data, and assets.

The comprehensive information security assessment focused on six key areas:

- **Security Policy Review.** The Security Policy Review evaluates the existing and proposed security policies and procedures and provides guidelines for future development.
- **Network Architecture Assessment.** The Network Architecture Assessment is a detailed review of a network design from an information security perspective.
- **Network Vulnerability Assessment.** The Network Vulnerability Assessment provides a thorough understanding of security-related weaknesses and exposures in networks.
- **Host Vulnerability Assessment.** A Host Vulnerability Assessment reviews the current security configuration of deployed hosts.
- **Secure Build Review.** A Secure Build Review is a security analysis in a non-production environment of the build procedure for a host.
- **Wireless Site Assessment.** A Wireless Site Assessment reviews the current security configuration of deployed wireless infrastructure.

Our assessment identified security controls within each area above that were well defined and effective as well as controls that posed 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. Our assessment identified twelve high level weaknesses, eighteen medium level weaknesses, and twelve low level weaknesses.

Due to the sensitive nature of the conditions found in these weaknesses, we have conveyed these findings to management in a separate report pursuant to the provision of the North Carolina General Statute 147-64.6(c)(18).

OBJECTIVES AND SCOPE (CONCLUDED)

Auditee's Response: The OSA MIS division has carefully reviewed the assessment and has either taken action to secure existing weaknesses, or where appropriate, is in the process of evaluating solutions to identified weaknesses. The MIS Division is committed to addressing and strengthening all identified weaknesses. In addition, the MIS Division continually strives to improve the level of information security in order to protect agency internal systems, data, and assets.

[This Page Left Blank Intentionally]

ORDERING INFORMATION

Audit reports issued by the Office of the State Auditor can be obtained from the web site at www.ncauditor.net. Also, parties may register on the web site to receive automatic email notification whenever reports of interest are issued. Otherwise, copies of audit reports 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

Telephone: 919/807-7500

Facsimile: 919/807-7647