STATE OF NORTH CAROLINA

INFORMATION SECURITY VULNERABILITY ASSESSMENT

NORTH CAROLINA OFFICE OF THE STATE CONTROLLER

RALEIGH, NORTH CAROLINA

OCTOBER 2008

OFFICE OF THE STATE AUDITOR

LESLIE W. MERRITT, JR., CPA, CFP

STATE AUDITOR

INFORMATION SECURITY VULNERABILITY ASSESSMENT

NORTH CAROLINA OFFICE OF THE STATE CONTROLLER

RALEIGH, NORTH CAROLINA

OCTOBER 2008

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
Mr. David McKoy, State Controller
Mr. George Bakolia, State CIO

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 North Carolina Office of the State Controller.

In September 2008, the Office of the State Auditor used a private contractor to perform an application penetration test of one application at the North Carolina Office of the State Controller. This assessment was conducted under the authority granted by North Carolina G.S. 147-64.6(c)(18).

This report represents the general results of our assessment. A detailed report containing the conditions found and recommended corrective action was provided to the North Carolina Office of the State Controller at the conclusion of our fieldwork.

The primary objective of this assessment was to evaluate the Payment Card Industry (PCI) compliance security controls over the application reviewed at the Agency. The scope of our assessment was limited to the application penetration test.

We wish to express our sincere appreciation to the staff of the North Carolina Office of the State Controller for the exceptional courtesy, cooperation, and assistance provided to us during this audit.

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,

Leslie W. Merritt, Jr.

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

OBJECTIVES AND SCOPE

The Office of the State Auditor, in consultation and coordination with Information Technology Services, undertook a project to evaluate the PCI compliance security of an application within the North Carolina Office of the State Controller.

In September 2008, the Office of the State Auditor used a private contractor to perform an application penetration test of one application at the North Carolina Office of the State Controller. The goal of the security assessment was to assist the North Carolina Office of the State Controller with achieving and maintaining PCI compliance with the application reviewed.

The comprehensive information security assessment focused on one key area:

- **Application Penetration Assessment.** The Application Penetration Assessment provides a thorough understanding of security-related weaknesses and exposures in an application.

Our assessment identified security controls within the application 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 2 high level weaknesses, 2 medium level weaknesses, and 5 low level weaknesses. Compensating controls in place at the North Carolina Information Technology Services (the host provider for the application) and the Office of the State Controller mitigated the severity of these weaknesses. This provides the North Carolina Office of the State Controller with a benchmark for future assessments.

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).

Auditee's Response: We have reviewed the confidential report, dated September 3, which resulted from the information security assessment of the Office of the State Controller's application, conducted by the Office of the State Auditor and the private vendor during the period of August 20, 2008 through September 3, 2008 under the authority granted by North Carolina General Statute §147-64.6(c)(18). As noted in the report, the primary focus of this assessment was to fulfill the Payment Card Industry's Data Security Standard Requirement 11.3.

We are pleased that the vendor's assessment revealed that the Office of Information Technology Services (our host service provider) "had adequately planned and executed a secure deployment of the application reviewed" …and that "overall, the mechanisms protecting the target application infrastructure from internal and external threats were highly effective". The Office of the State Controller has always worked diligently to build a strong and secure foundation by achieving a "best practices" level of information security in order to protect our systems and data.

The Office of Information Technology Services is currently reviewing the impact and remediation effort associated with the recommendations noted in the report. For some of the recommendations, appropriate measures to implement corrective action have already been taken. The remaining recommendations will be prioritized, and implemented, based upon resource availability.

Please be assured that the Office of the State Controller, along with our business partner, the Office of Information Technology Services, takes an active role in security and we are committed to doing our part in protecting the State's investment in technology systems, as well as protecting our citizens' personally identifiable or confidential data. We appreciate the opportunity to have been included in this assessment, as well as the professional manner with which this assessment was conducted.

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