STATE OF
NORTH CAROLINA

OFFICE OF THE INFORMATION TECHNOLOGY SERVICES

INFORMATION TECHNOLOGY GENERAL CONTROLS

JULY 2013

PERFORMANCE AUDIT

OFFICE OF THE STATE AUDITOR

BETH A. WOOD, CPA

STATE AUDITOR

EXECUTIVE SUMMARY

PURPOSE

This audit was conducted to determine the effectiveness of information technology general controls for the overall organization and operation of the North Carolina Office of Information Technology Services (ITS).

BACKGROUND

ITS is the leading provider of IT services to state agencies, local governments, and educational institutions across North Carolina. ITS services include hosting, network and video services, telecommunications, and enterprise services such as email and calendaring.

KEY FINDINGS

- The ITS Education and Training policy for employees is general in nature and inadequate for key personnel, such as system administrators and information security officers.

- The ITS policy requiring contractors to acknowledge understanding of ITS policies is not enforced.

KEY RECOMMENDATIONS

- ITS should update the Education and Training policy to ensure that system administrators and information security personnel obtain annual training pertinent to their roles and responsibilities.

- ITS should enforce its policy and maintain on file a signed *ITS Policy Manual Acknowledgement Statement* from all third-party contractors.

ADDITIONAL INFORMATION

Items regarding access controls, due to their sensitivity, were reported to the agency by separate letter and should be kept confidential as provided in *North Carolina G.S. 132-6.1(c).*

STATE OF NORTH CAROLINA

Office of the 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

Beth A. Wood, CPA
State Auditor

July 30, 2013

The Honorable Pat McCrory, Governor
Members of the North Carolina General Assembly
Mr. Chris Estes, State Chief Information Officer

Ladies and Gentlemen:

This report presents the results of our performance audit of information technology general controls at the State of North Carolina Office of Information Technology Services (ITS). Our audit was performed by authority of Article 5A of Chapter 147 of the *North Carolina General Statutes* and was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States.

The objective of this audit was to determine the effectiveness of general controls for the overall organization and operation of ITS. The results of our audit disclosed deficiencies that are considered reportable under *Government Auditing Standards*. Items regarding access controls, due to their sensitivity, are reported to the agency by separate letter and should be kept confidential as provided in *North Carolina G.S. 132-6.1(c)*.

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.

Beth A. Wood

Beth A. Wood, CPA
State Auditor

TABLE OF CONTENTS

PAGE

BACKGROUND

The General Assembly, "in recognition of the need to better manage the acquisition and use of information technology in general state government" created the Office of Information Technology Services in 1983 (at the time called State Information Processing Services) by consolidating the State Computer Center and similar operations at the Department of Transportation, the Department of Correction, and the Employment Security Commission. Originally placed within the Department of Administration, the Office of Information Technology Services (ITS) was later moved by executive order to the Office of State Controller and the Department of Commerce on March 1, 1987, and April 14, 1997, respectively. Effective November 1, 2000, Senate Bill 1345 of the 1999 Session of the General Assembly transferred ITS from the Department of Commerce to the Office of the Governor as well as expanded its responsibilities to include enterprise management of information technology (IT) assets.

General Statutes (GS) §147-33.83 stipulates, among other things, that ITS shall provide cities, counties, and other local governmental units with access to ITS information resource centers and services. These services are provided through use of mainframe computers, distributed computing servers, and statewide voice, data, and video networks. ITS operates as an internal service fund and, as such, the costs of providing services are recovered through direct billings to clients.

General Statutes (GS) §147-33.76, State Information Technology Management, stipulates the State Chief Information Officer (CIO) shall be responsible for developing and administering a comprehensive long-range plan to ensure the proper management of the State's information technology resources. The State CIO shall set technical standards for information technology, review and approve major information technology projects, review and approve State agency information technology budget requests, establish information technology security standards, provide for the procurement of information technology resources, and develop a schedule for the replacement or modification of major systems. The State CIO is authorized to adopt rules to implement this Article.

OBJECTIVES, SCOPE, AND METHODOLOGY

As authorized by Article 5A of Chapter 147 of the *North Carolina General Statutes*, a performance audit at the State of North Carolina Office of Information Technology Services (ITS) was conducted. The objective of this audit was to determine the effectiveness of information technology (IT) general controls for the overall organization and operation of ITS. The audit was conducted between July 1, 2012, and April 30, 2013.

The scope of the audit included the following IT general controls categories: general security, access controls, program maintenance, systems software, systems development, physical security, operations procedures, and disaster recovery, which directly affect ITS' computer operations. The audit evaluated general controls for financial applications hosted by ITS, which are critical to the State of North Carolina Comprehensive Annual Financial Report (CAFR) and the federal single audit.

To accomplish the audit objective, the auditors gained an understanding of ITS' policies and procedures, interviewed key ITS administrators and other personnel, examined system configurations, tested on-line system controls, reviewed appropriate technical literature, and reviewed computer-generated reports.

As a basis for evaluating general controls, auditors applied the guidance contained in *The State of North Carolina Statewide Information Security Manual*. It sets out the standards required by *General Statute §147-33.110*, which directs the State Chief Information Officer (State CIO) to establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the State's distributed information technology assets.

Additionally, auditors applied the guidance contained in the *Control Objectives for Information and Related Technology* (COBIT) framework issued by ISACA. COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance and helps organizations increase the value attained from IT. COBIT standards state that management should implement controls to ensure that the organization's policies and procedures are designed to adequately protect critical and sensitive data from unauthorized access from both internal and external users.

ITS management, pursuant to *North Carolina General Statute §143D-7*, bears full responsibility for establishing and maintaining a proper system of internal control, which includes IT general controls. A proper system of internal control is designed to provide reasonable, rather than absolute, assurance that relevant objectives are achieved. Because of inherent limitations in internal controls, unauthorized access to data, for example, may nevertheless occur and not be detected. Also, projections of the auditors' evaluation in this report of general controls to future periods are subject to the risk that, for example, conditions at ITS may change or compliance with ITS' policies and procedures may deteriorate.

This performance audit was conducted in accordance with generally accepted government auditing standards. Those standards require that the auditors plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. The auditors believe that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objectives.

The results of this audit disclosed internal control deficiencies that are considered reportable under *Government Auditing Standards*. The deficiencies noted result from a failure to implement adequate access controls and IT governance practices.

Details about the failure to implement adequate access controls, due to their sensitive nature, were communicated to ITS management in a separate letter pursuant to *North Carolina G.S. 132-6.1(c).*

The auditors found deficiencies related to IT governance practices that could increase the risk of inadequate information system security by employees and contractors. Specifically, auditors found:

ITS EDUCATION AND TRAINING POLICY NOT ADEQUATE FOR KEY PERSONNEL

The ITS Education and Training[1] policy for employees is general in nature and does not require formal and regular training for the system administrators or information security officer. The ITS policy states "Ultimately, all ITS employees are responsible for their own development and education. Employees are expected to advance their own careers through appropriate self-education and self-improvement."

This approach by ITS does not take reasonable actions to ensure the authorized and acceptable use of data, networks, and communications transiting the ITS systems or network. *The State of North Carolina Statewide Information Security Manual* states agencies must clearly define security responsibilities for system administrators and "must also provide appropriate training for their system administrators."[2]

POLICY REQUIRING CONTRACTORS TO ACKNOWLEDGE UNDERSTANDING OF POLICY NOT ENFORCED

Signed statements are not filed and maintained for all contractors acknowledging that that they have read and understand the policies within the *ITS Policy Manual*. *The Office of Information Technology Service Policy Manual* states:

> "Managers shall give new employees and contractors adequate time to read the *ITS Policy Manual* and to ask any questions they might have during the employees' and contractors' first two weeks of work at ITS. At the end of the two week period, the employees and contractors will sign the *ITS Policy Manual Acknowledgement Statement*, acknowledging that they have been given the opportunity to read, understand and ask questions about the *ITS Policy Manual*."[3]

According to the State Chief Security & Risk Officer, ITS employees and third-party contractors have a continuing responsibility to stay current on the *ITS Policy Manual,* and they are notified of revisions by the IT Policy and Programs Office or by their managers.

---

[1] *ITS Policy Manual,* Section 2.09, Education and Training
[2] Section 030202, Administering Systems
[3] Section 19.31, *ITS Policy Manual* Review

Recommendations:

- ITS should update the Education and Training policy to ensure that system administrators and information security personnel obtain annual training pertinent to their roles and responsibilities.

- ITS should enforce its policy and maintain on file a signed *ITS Policy Manual Acknowledgement Statement* from all third-party contractors.

Agency Response:

NO POLICY FOR FORMAL ANNUAL TRAINING FOR KEY PERSONNEL
ITS has revised the ITS Education and Training Policy in order to confirm that system administrators and security personnel obtain annual training pertinent to their roles and responsibilities. The policy revision will be adopted after review and approval by senior management.

POLICY REQUIRING CONTRACTORS TO ACKNOWLEDGE UNDERSTANDING OF POLICY NOT ENFORCED
An agency trainer who will begin work by mid-August will help managers consistently obtain and file signed statements of third party contractors acknowledging that they have read and understood the ITS Policy Manual.

State of North Carolina
Office of Information Technology Services

Pat McCrory
Governor

Chris Estes
State Chief Information Officer

July 22, 2013

The Honorable Beth A. Wood
Office of the State Auditor
20601 Mail Service Center
Raleigh, North Carolina 27699-0601

Dear Ms. Wood:

We have reviewed the draft of the Information Technology General Controls performance audit dated July, 2013 for performance between July, 2012 and April, 2013. We have responded to the State's recommendations as follows:

NO POLICY FOR FORMAL ANNUAL TRAINING FOR KEY PERSONNEL
ITS has revised the ITS Education and Training Policy in order to confirm that system administrators and security personnel obtain annual training pertinent to their roles and responsibilities. The policy revision will be adopted after review and approval by senior management.

POLICY REQUIRING CONTRACTORS TO ACKNOWLEDGE UNDERSTANDING OF POLICY NOT ENFORCED
An agency trainer who will begin work by mid-August will help managers consistently obtain and file signed statements of third party contractors acknowledging that they have read and understood the ITS Policy Manual.

Thank you again for the opportunity to respond to the draft audit.

Sincerely,

Chris Estes

P.O. Box 17209, Raleigh, NC 27619-7209
4101 Mail Service Center, Raleigh, NC 27699-4101
Telephone: 919-754-6100
An Equal Opportunity/Affirmative Action Employer

6

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

Telephone: 919-807-7500

Facsimile: 919-807-7647

Internet: http://www.ncauditor.net

To report alleged incidents of fraud, waste or abuse in state government contact the:

Office of the State Auditor Fraud Hotline: 1-800-730-8477

or download our free app

https://play.google.com/store/apps/details?id=net.ncauditor.ncauditor

https://itunes.apple.com/us/app/nc-state-auditor-hotline/id567315745

For additional information contact:
Bill Holmes
Director of External Affairs
919-807-7513