

# STATE OF NORTH CAROLINA

OFFICE OF THE STATE AUDITOR

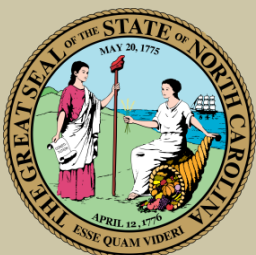
BETH A. WOOD, CPA



## ADMINISTRATIVE OFFICE OF THE COURTS

INFORMATION TECHNOLOGY  
GOVERNANCE AND SECURITY MANAGEMENT

INFORMATION SYSTEMS AUDIT  
APRIL 2020



**NCOSA**  
The Taxpayers' Watchdog

# EXECUTIVE SUMMARY

---

## **PURPOSE**

The purpose of this audit was to determine whether the Administrative Office of the Courts (AOC) has established and implemented key objectives of information technology (IT) governance and security management in accordance with state policies and best practices.

## **BACKGROUND**

AOC provides statewide support services for the courts, including court programs and management, IT, human resources, financial, legal, legislative support, and purchasing.

By state law<sup>1</sup>, the Director is responsible for prescribing policies and procedures and establishing and operating systems for the exchange of criminal and civil information from and to the Judicial Branch and local, state, and federal governments and the Eastern Band of Cherokee Indians.

## **KEY FINDINGS**

- AOC did not ensure that more than half of its security management policies and programs were approved and implemented.
- AOC did not develop and implement an access control policy to establish requirements for controlled logical access to information assets.
- AOC did not implement a security awareness program to ensure security is considered consistently throughout the organization.

## **KEY RECOMMENDATIONS**

- The Director should ensure security management policies and programs are approved and implemented to help protect against security risks associated with citizen information, judicial data, and IT systems.
- AOC management should develop and implement an access control policy for the existing environment to ensure access to sensitive data and IT systems is appropriately protected against unauthorized modification, loss, or disclosure.
- AOC management should implement a security awareness program to ensure all employees and contractors are aware of their security responsibilities and threats that target human behavior.
- AOC Management should monitor compliance with its security awareness program requirements after implementation.

---

<sup>1</sup> N.C. Gen. Stat. Section 7A-343(13), Duties of Director

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 27699-0600  
Telephone: (919) 807-7500  
Fax: (919) 807-7647  
[www.auditor.nc.gov](http://www.auditor.nc.gov)

## AUDITOR'S TRANSMITTAL

---

The Honorable Roy Cooper, Governor  
Members of the North Carolina General Assembly  
The Honorable Cheri Beasley, Chief Justice Supreme Court  
McKinley Wooten, Director, Administrative Office of the Courts

Ladies and Gentlemen:

We are pleased to submit this information systems audit report titled *Information Technology Governance and Security Management*.

The purpose of this audit was to determine whether the Administrative Office of the Courts has established and implemented key objectives of information technology governance and security management in accordance with state policies and best practices.

The Director reviewed a draft copy of this report. His written comments are included starting on page 9.

This audit was conducted in accordance with Chapter 147, Article 5A of the *North Carolina General Statutes*.

We appreciate the courtesy and cooperation received from management and the employees of the Administrative Office of the Courts during our audit.

Respectfully submitted,

A handwritten signature in black ink that reads 'Beth A. Wood'.

Beth A. Wood, CPA  
State Auditor

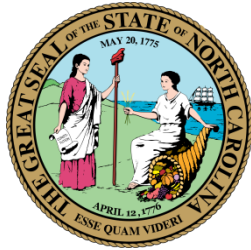


**Beth A. Wood, CPA  
State Auditor**

# TABLE OF CONTENTS

---

	<b>PAGE</b>
BACKGROUND.....	1
OBJECTIVE, SCOPE, AND METHODOLOGY .....	3
RESULTS AND CONCLUSIONS.....	5
FINDINGS AND RECOMMENDATIONS.....	6
RESPONSE FROM THE ADMINISTRATIVE OFFICE OF THE COURTS .....	9
ORDERING INFORMATION.....	14



# BACKGROUND

## **Administrative Office of the Courts**

The Administrative Office of the Courts (AOC) operates under the leadership of the Director, as appointed by the Chief Justice of the Judicial Branch. The Director has wide authority over the governance of AOC including its systems and services for electronic filing, electronic transaction processing, and access to court information systems. A full list of the powers and duties of the Director can be found in *North Carolina General Statutes Chapter 7A, Article 29, Section 343*.

The AOC provides administrative services to North Carolina's unified court system to help it operate more efficiently and effectively<sup>2</sup>. The Technology Services Division, within AOC, provides information technology services and solutions to support the day-to-day work of the Judicial Branch.

## **Services Provided by the Technology Services Division**

The Technology Services Division operates a complex information technology (IT) environment consisting of more than 25 thousand components<sup>3</sup>, which support thousands of Judicial Branch employees across the state. The IT network spans more than 49 thousand square miles, and supports court users in every county and more than 32 thousand law enforcement personnel statewide<sup>4</sup>. Users include judges, district attorneys, magistrates, public defenders, private attorneys, clerks of court, law enforcement organizations, and various state institutions<sup>2</sup>.

More than 50 enterprise applications track over 50 million criminal and infraction cases, 20 million civil cases, and 138 million pages of discovery documents, and process more than a million daily transactions and 700 thousand annual payments. Nine of these applications are more than 20 years old. Court information subsystems are tailored to the unique needs of North Carolina's unified court system, which is one of the few truly unified court information systems in the nation<sup>4</sup>. The AOC incurred approximately \$64 million in IT expenditures during state fiscal year 2019<sup>5</sup>.

## **Importance of Information Technology Governance and Security Management**

By state law<sup>6</sup>, the Director is responsible for prescribing policies and procedures and establishing operating systems for the exchange of criminal and civil information between the Judicial Branch, local, state, and federal governments, and the Eastern Band of Cherokee Indians.

To ensure the public has confidence in state services, the Director must implement and maintain governance processes that protect citizen information, judicial data, and IT systems. IT governance requires formalized processes and programs to ensure security activities are consistently performed, responsive to risk, and auditable.

---

<sup>2</sup> North Carolina Administrative Office of the Courts 2014 - 2017 Information Technology Plan

<sup>3</sup> Supported computer components include computers, peripherals, telephones, servers, faxes, and routers.

<sup>4</sup> <https://www.nccourts.gov/assets/documents/publications/Technology-Services-Fact-Sheet-2018-19.pdf>

<sup>5</sup> <https://www.osc.nc.gov/public-information/reports/it-expenditures-report>

<sup>6</sup> N.C. Gen. Stat. Section 7A-343(13), Duties of Director

Proper IT governance over North Carolina's unified court system means:

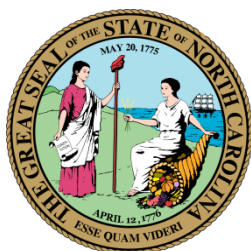
- AOC management ensures a security program is implemented through policies and procedures that ensure that IT systems are protected.
- The enterprise IT function ensures that resource owners, system administrators, and users are aware of security policies.

According to best practice framework *ISO 27002 – Information Technology – Security Techniques – Code of Practice for Information Security Controls*<sup>7</sup>, key information security activities include incident response, vulnerability management, information handling, access control, and security awareness training.

Establishing plans and policies for key information security activities improves an organization's ability to respond to security incidents, manage known vulnerabilities, and protect data. Information security governance also requires an organization to establish and implement rules and guidelines for use of its information resources and data. Controlling access to data reduces the risk of unauthorized data modification, loss, or disclosure. Lastly, security awareness processes ensure that resource owners, system administrators, and users are aware of the security policies. Security awareness training is important because people are the weakest link in an organization's security posture. Technology can be used to implement many IT controls. However, untrained employees can diminish the effectiveness of those controls. In turn, this can result in data being mishandled, inappropriately used, or shared with unauthorized people.

---

<sup>7</sup> ISO 27002 is a reference for organizations to use as guidance while designing an information security management system or while implementing commonly accepted information security controls.



# **OBJECTIVE, SCOPE, AND METHODOLOGY**



We conducted this information systems audit in accordance with *Generally Accepted Government Auditing Standards*. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The purpose of this audit was to determine whether the Administrative Office of the Courts (AOC) has established and implemented key objectives of information technology (IT) governance and security management in accordance with state policies and best practices. In planning the audit, we considered IT control objectives as follows:

1) Governance

- Assess the use of IT in enabling the achievement of AOC's goals and objectives;
- Ensure controls are in place to identify and manage enterprise IT risk;
- Assess the value measurement process to ensure that IT costs align with business goals;
- Assess the IT strategy to ensure that IT aligns with the business direction; and
- Assess knowledge management to ensure proper alignment of IT knowledge and experience with governance decision making.

2) Security Management

- Assess the security management program to ensure that IT systems are protected;
- Assess the security awareness process to ensure that resource owners, system administrators, and users are aware of security policies;
- Ensure controls are in place to periodically monitor and assess the effectiveness of security over IT systems and data;
- Ensure controls are in place to identify vulnerabilities and effectively remediate IT security weaknesses; and
- Assess the vendor management process to ensure that third-party activities are secured, documented, and monitored.

After evaluating the IT control objectives, we identified risks in AOC's internal controls over security management that expanded our audit scope related to three key objectives:

- 1) Determine whether AOC implemented a security governance program to ensure that IT systems are protected in accordance with best practices.
- 2) Determine whether AOC implemented an access control policy to ensure requirements for controlled logical access to information assets are established in accordance with best practices.
- 3) Determine whether AOC implemented a security awareness process to ensure that resource owners, system administrators, and users are aware of security policies in accordance with best practices.

We performed the following procedures to accomplish those audit objectives:

- Interviewed key AOC managers and staff.
- Reviewed policies and best practices.
- Reviewed state laws.
- Observed system and process controls related to the control objectives.
- Examined documentation supporting AOC's policies and procedures.
- Evaluated system processes and documentation against policy requirements and best practices.

Our audit scope covered the period between March 2019 through December 2019.

Because of the test nature and other inherent limitations of an audit, together with limitations of any system of internal and management controls, this audit would not necessarily disclose all performance weaknesses or lack of compliance.

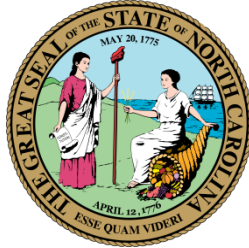
As a basis for evaluating controls, auditors applied the guidance contained in *ISO 27002 – Information Technology – Security Techniques – Code of Practice for Information Security Controls*<sup>8</sup>. During the audit period, this framework was the basis under which AOC aligned IT security requirements for the Judicial Branch of state government and managed information security risk.

Additionally, auditors applied the guidance contained in the COBIT framework issued by ISACA<sup>9</sup>. COBIT is a comprehensive framework that helps enterprises in achieving their objectives for the governance and management of enterprise information and technology assets.

---

<sup>8</sup> This framework was developed by the International Organization for Standardization (ISO), an international standard-setting body that promotes worldwide proprietary, industrial, and commercial standards.

<sup>9</sup> ISACA is a non-profit and independent leading global provider of knowledge, certifications, community, advocacy, and education on information systems assurance and security, enterprise governance and management of IT, and IT-related risk and compliance.

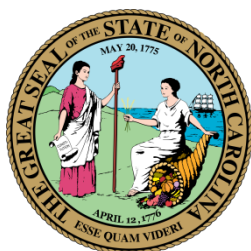


# RESULTS AND CONCLUSIONS

Based on the results of audit procedures described in the *Objective, Scope, and Methodology* section of this report, we identified deficiencies in the Administrative Office of the Court's (AOC) controls over governance and security management that are considered reportable under *Government Auditing Standards* as follows:

- AOC did not ensure that more than half of its security management policies and programs were approved and implemented.
- AOC did not develop and implement an access control policy to establish requirements for controlled logical access to information assets.
- AOC did not implement a security awareness program to ensure security is considered consistently throughout the organization.

These deficiencies are described in more detail in the *Findings and Recommendations* section of this report. Management's response is presented in the *Response from the Administrative Office of the Courts* section of this report. We did not audit the responses, and accordingly, we express no opinion on them.



# **FINDINGS AND RECOMMENDATIONS**

---

## 1. INSUFFICIENT SECURITY GOVERNANCE PROGRAM

---

The Administrative Office of the Courts (AOC) did not ensure that more than half of its security management policies and programs were approved and implemented. Select policies and programs were in draft form since 2016.

Auditors found that 12 out of 20 (60%) of the information security policy and program documents were still in draft and had not been formally implemented. These documents included:

- North Carolina Judicial Branch Information Security – This policy provides a secure foundation for the protection of the Judicial Branch’s information assets.
- Information Handling – This policy requires appropriate controls to be in place and operating effectively to manage risk to the confidentiality, integrity, and availability of sensitive data in any form, and creates a minimum standard for data protection within the organization.
- Vulnerability Management – This program is designed to mitigate inherent security weaknesses created by software vulnerabilities.
- Incident Management Response – This policy ensures that disruptions to business operations, security, information technology (IT) systems, and vital business functions are managed through an established process.
- Use of Removable Media<sup>10</sup> – This policy communicates the requirement to protect the confidentiality and integrity of sensitive information as it relates to removable media, and to prevent deliberate or inadvertent exfiltration<sup>11</sup> of data from the organization.

Without fully implementing information security policy and program documents, AOC cannot ensure that:

- Information security activities will be coordinated, efficient, and meet the State’s needs.
- Personnel will not unintentionally jeopardize the confidentiality, integrity, and/or availability of sensitive data.
- Vulnerabilities are managed and mitigated to protect against unauthorized access to, or theft of, sensitive data.
- Unplanned situations or events do not negatively impact or interrupt services.
- Information assets are protected against risk of data loss, data exposure, or network-based attacks.

According to AOC management, previous directors did not prioritize the approval and implementation of security management policies and programs. Current management focused efforts on the implementation of new technologies.

---

<sup>10</sup> Portable device that can be connected to an information system, computer, or network to provide data storage, such as a USB flash drives or external hard drive.

<sup>11</sup> Data exfiltration is the unauthorized copying, transfer or retrieval of data from a computer or server.

However, AOC management should ensure that security management policies and programs are in place for existing citizen information, judicial data, and IT systems, as the implementation of new technologies could take several years.

Best practices identified by the International Organization for Standardization<sup>12</sup> state that a set of policies for information security should be defined, approved by management, published, and communicated to employees and relevant external parties.

By state law, the Director is responsible for prescribing policies over the organization's systems of information exchange. *North Carolina General Statutes* Section 7A-343(13) states that the Director's duties include:

“Prescribe policies and procedures and establish and operate systems for the exchange of criminal and civil information from and to the Judicial Department and local, state, and federal governments and the Eastern Band of Cherokee Indians.”

### RECOMMENDATION

The Director should ensure security management policies and programs are approved and implemented to help protect against security risks associated with citizen information, judicial data, and IT systems.

---

## 2. ACCESS CONTROL POLICY NOT IMPLEMENTED

---

The Administrative Office of the Courts (AOC) did not develop and implement an access control policy to establish requirements for controlled logical access to information assets. An access control policy establishes requirements for managing access to information resources and determining who may be granted access.

The lack of an access control policy increases the risk that system users could gain inappropriate access to sensitive data and maliciously or inadvertently modify data or information technology (IT) systems.

According to AOC management, previous directors did not prioritize the creation and implementation of an access control policy. Current management focused IT management efforts on the implementation of new technologies.

However, AOC management should ensure that an access control policy is in place to control logical access to existing information assets, as the implementation of new technologies could take several years.

Best practices identified by the International Organization for Standardization<sup>13</sup> state that an access control policy should be established, documented, and reviewed based on business and information security requirements.

---

<sup>12</sup> ISO 27002 (2013), §5.1.1. Policies for information security

<sup>13</sup> ISO 27002 (2013), §9.1.1. Access control policy

**RECOMMENDATION**

AOC management should develop and implement an access control policy for the existing environment to ensure access to sensitive data and IT systems is appropriately protected against unauthorized modification, loss, or disclosure.

---

**3. SECURITY AWARENESS PROGRAM NOT IMPLEMENTED**

---

The Administrative Office of the Courts (AOC) did not implement a security awareness program to ensure security is considered consistently throughout the organization<sup>14</sup>. Security awareness is a formal process for educating employees about the protection of an organization's physical and information assets.

Auditors found that AOC management had drafted an information security program definition document that included a section on security awareness, but this document had not been approved. Therefore, security awareness activities have not been formally implemented, mandated, or monitored for participation and compliance.

The lack of a security awareness program increases the risk that employees will be unaware of security responsibilities and will fall victim to emerging cyber threats.

According to AOC management, previous directors did not prioritize the approval and endorsement of a security awareness program. Current management focused IT management efforts on the implementation of new technologies.

However, AOC management should ensure that a security awareness program is in place to ascertain that existing information assets remain confidential, as the implementation of new technologies could take several years.

Best practices identified by the International Organization for Standardization<sup>15</sup> state that all employees, and contractors where relevant, receive security awareness training relevant to their job role.

**RECOMMENDATION**

AOC management should implement a security awareness program to ensure all employees and contractors are aware of their security responsibilities and threats that target human behavior.

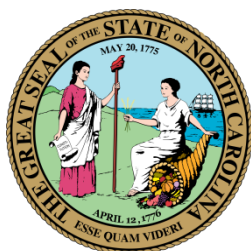
AOC management should monitor compliance with its security awareness program requirements after implementation.

---

<sup>14</sup> The Administrative Office of the Courts employees and contractors

<sup>15</sup> ISO 27002 (2013), §7.2.2. Information security awareness, education, and training





# **RESPONSE FROM THE ADMINISTRATIVE OFFICE OF THE COURTS**



ADMINISTRATIVE OFFICE OF THE COURTS

MCKINLEY WOOTEN, JR.  
DIRECTOR

PO BOX 2448, RALEIGH, NC 27602  
O 919-890-1000  
F 919-890-1915  
MCKINLEY.WOOTEN@NCCOURTS.ORG

April 8, 2020

The Honorable Beth A. Wood, State Auditor  
Office of the State Auditor  
2 Salisbury Street  
20601 Mail Service Center  
Raleigh, NC 27699-0601

Dear State Auditor Wood:

The North Carolina Administrative Office of the Courts (AOC) provides support services for the Judicial Branch, including: court programs and management services; financial, legal, and legislative support services; information technology (IT) services; human resources services; training; and purchasing services.

The AOC delivers IT services to the Judicial Branch through its Technical Services Division (TSD). TSD's services include application development and hosting, local and wide area networking, telecommunications, desktop computing, quality control and testing, information security, project management, and unified communications such as email and calendaring. TSD supports and maintains mainframe computers, distributed computing servers, and statewide voice, data, cloud services and video networks to provide these services.

The scope, breadth, and reach of AOC information technology is quite vast. TSD provides computer hardware and software in more than 250 locations statewide, including 541 district and superior courtrooms in all 100 North Carolina counties. TSD also maintains and operates a statewide communication network including data and network operations centers in Raleigh with disaster recovery centers in Asheville and Research Triangle Park.

The Judicial Branch technology user community comprises approximately 6,500 staff including over 530 elected court officials and over 690 appointed officials. More than 33,000 law enforcement officers also utilize computer applications created and supported by AOC and federal, state, and local government agencies exchange information with AOC systems daily. Likewise, many of the 10 million North Carolina citizens interact with the court system through these applications and services. The AOC utilizes industry standards and best practices and takes all reasonable efforts to safeguard Judicial Branch information assets against unauthorized disclosure, modification, damage and loss.

**Finding # 1: *Insufficient Security Governance Program***

The Administrative Office of the Courts (AOC) did not ensure that more than half of its security management policies and programs were approved and implemented. Select policies and programs were in draft form since 2016.

**Recommendation:**

The Director should ensure security management policies and program are approved and implemented to help protect against security risk associated with citizen information, judicial data and IT systems.

**NCAOC Response:** NCAOC agrees with the finding and has provided remediation efforts below.

To put an increased focus on the NCAOC information security program, including the development and maintenance of Information Security policy, NCAOC hired a new Chief Information Security Officer (August 2019), Risk Management Officer (October 2019), and Privacy Officer (March 2020) with responsibilities developing a formal information security program for NCAOC. In addition, two other FTEs are dedicated to supporting security functions. Additional staff has been requested and plan to be added to the security program to support various security initiatives.

At the CISO's Office recommendation, in September 2019, the NCAOC eCourts Steering committee formally adopted the NIST 800-53 r4 family of control objectives as the basis of the NCAOC Information Security Program. NCAOC has completed, formally accepted and implemented nine of the eighteen control family policies in NIST 800-53 r4. Even as NCAOC builds out essential foundational controls needed to support the security program, NCAOC continues to focus on the remaining nine control families to ensure that all the policy families have been addressed, formally accepted and implemented.

To define and build out supporting key foundational controls and mitigate immediate cybersecurity risk, the CISO's Office developed the NCAOC 2020 Security and Risk Strategic Plan which was approved by the CTO and then communicated to the NCAOC IT managers in January 2020. Since the security program has been reestablished, NCAOC has made significant investments in cybersecurity tools/services and cybersecurity initiatives in support of initiatives identified in the strategic plan. Currently, NCAOC is procuring Governance, Risk and Compliance (GRC) software to further support the NCAOC Governance program and the various associated risk mitigation efforts underway.

**Finding # 2: Access Control Policy Not Implemented**

The Administrative Office of the Courts (AOC) did not develop and implement an access control policy to establish requirements for controlled logical access to information assets. An access control policy established requirements for managing access to information resources and determining who may be granted access.

**Recommendation:**

AOC management should develop and implement an access control policy for the existing environment to ensure access to sensitive data and IT systems is appropriately protected against unauthorized modification, loss, or disclosure.

**NCAOC Response:** NCAOC agrees with the finding and has provided remediation efforts below.

In April 2020, NCAOC implemented a new Access Control policy based on the adopted NIST 800-53 r4 control family guidance. Information Security policies will be reviewed at least annually and updated as necessary to manage risk taking in consideration organizational change and control enhancements. As a result, this policy is expected to continue to be refined over time as NCAOC moves more applications to the cloud and makes additional investments in supporting IAM (Identity and Access Management) Governance software.

**Finding # 3: Security Awareness Program Not Implemented**

The Administrative Office of the Courts (AOC) did not implement a security awareness program to ensure security is considered consistently throughout the organization. Security awareness is a formal process for educating employees about the protection of an organization's physical and information assets.

**Recommendation:**

AOC management should implement a security awareness program to ensure all employees and contractors are aware of their security responsibilities and threats that target human behavior.

**NCAOC Response:** NCAOC agrees with the finding and has provided remediation efforts below.

This gap was also identified by the NCAOC CISO Office in August of 2019. To meet this need, new Security Awareness training modules were selected that cover key areas of risk where end users are most often targeted and would also benefit the most from the provided security

awareness training. The selected security awareness modules include: “Understanding and Protecting PII”, “Phishing Fundamentals”, “Social Engineering Basics”, and “Ransomware”.

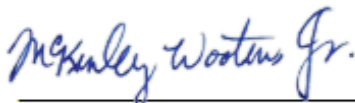
In December 2019, the Chief Justice and the NCAOC Director approved the Security Awareness Policy and mandated that the new security awareness training be taken by all NCAOC staff. In January 2020, NCAOC formally rolled out the new security awareness training that aligns with NIST 800-53 r4 control family (AT – Training and Awareness). The required online training is provided annually to full-time and temporary staff, interns and contractors. In addition to the online security awareness training, monthly security awareness articles are also sent out by the Information Security Office to NCAOC staff via email and are also posted to the NCAOC Intranet.

Thank you for the opportunity to review and comment on the draft report, *Information Technology and Security Management, Information Systems Audit April 2020*. The NCAOC continues to strive to ensure IT resources and data are managed properly in all areas, especially in the areas of governance and security.

The NCAOC greatly appreciates the State Auditor’s Office providing this report and looks forward to our continued partnership in the future.

Please do not hesitate to reach out if you have any further questions.

Sincerely,




---

McKinley Wooten Jr., Director  
Administrative Office of the Courts

# ORDERING INFORMATION

---

COPIES OF THIS REPORT MAY BE OBTAINED BY CONTACTING:

Office of the State Auditor  
State of North Carolina  
2 South Salisbury Street  
20601 Mail Service Center  
Raleigh, North Carolina 27699-0600

Telephone: 919-807-7500  
Facsimile: 919-807-7647  
Internet: <https://www.auditor.nc.gov>

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.ncstateauditor.ncauditor&hl=en\\_US](https://play.google.com/store/apps/details?id=net.ncstateauditor.ncauditor&hl=en_US)



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

For additional information contact  
North Carolina Office of the State Auditor at **919-807-7666**



---

This audit was conducted in 2,248.5 hours at an approximate cost of \$233,844.