**GENERAL ASSEMBLY OF NORTH CAROLINA**

**SESSION 2005**

**H** **1**

# HOUSE BILL 51

| | | |
|---|---|---|
| Short Title: | IT Security Assessments. | (Public) |
| Sponsors: | Representatives Michaux, Tolson (Primary Sponsors); Alexander, Farmer-Butterfield, Jones, and McAllister. | |
| Referred to: | Science and Technology. | |

February 3, 2005

A BILL TO BE ENTITLED

AN ACT MAKING THE STATE CHIEF INFORMATION OFFICER RESPONSIBLE FOR INFORMATION TECHNOLOGY SECURITY ASSESSMENTS AND RELIEVING THE STATE AUDITOR OF THE DUTY TO PERFORM SIMILAR ASSESSMENTS.

The General Assembly of North Carolina enacts:

**SECTION 1.** G.S. 147-64.6(c) reads as rewritten:

"**§ 147-64.6. Duties and responsibilities.**

(c) The Auditor shall be responsible for the following acts and activities:

(1) Audits made or caused to be made by the Auditor shall be conducted in accordance with generally accepted auditing standards as prescribed by the American Institute of Certified Public Accountants, the United States General Accounting Office, or other professionally recognized accounting standards-setting bodies.

(2) Financial and compliance audits may be made at the discretion of the Auditor without advance notice to the organization being audited. Audits of economy and efficiency and program results shall be discussed in advance with the prospective auditee unless an unannounced visit is essential to the audit.

(3) The Auditor, on his own initiative and as often as he deems necessary, or as requested by the Governor or the General Assembly, shall, to the extent deemed practicable and consistent with his overall responsibility as contained in this act, make or cause to be made audits of all or any part of the activities of the State ~~agencies.~~agencies, except that the Auditor may not make information technology security assessments.

(4) The Auditor, at his own discretion, may, in selecting audit areas and in evaluating current audit activity, consider and utilize, in whole or in

part, the relevant audit coverage and applicable reports of the audit staffs of the various State agencies, independent contractors, and federal agencies. He shall coordinate, to the extent deemed practicable, the auditing conducted within the State to meet the needs of all governmental bodies. The discretion granted by this subdivision does not authorize the Auditor to select information technology security assessment as an audit area.

(5) The Auditor is authorized to contract with federal audit agencies, or any governmental agency, on a cost reimbursable basis, for the Auditor to perform audits of federal grants and programs administered by the State Departments and institutions in accordance with agreements negotiated between the Auditor and the contracting federal audit agencies or any governmental agency. In instances where the grantee State agency shall subgrant these federal funds to local governments, regional councils of government and other local groups or private or semiprivate institutions or agencies, the Auditor shall have the authority to examine the books and records of these subgrantees to the extent necessary to determine eligibility and proper use in accordance with State and federal laws and regulations.

The Auditor shall charge and collect from the contracting federal audit agencies, or any governmental agencies, the actual cost of all the audits of the grants and programs contracted by him to do. Amounts collected under these arrangements shall be deposited in the State Treasury and be budgeted in the Department of State Auditor and shall be available to hire sufficient personnel to perform these contracted audits and to pay for related travel, supplies and other necessary expenses.

(6) The Auditor is authorized and directed in his reports of audits or reports of special investigations to make any comments, suggestions, or recommendations he deems appropriate concerning any aspect of such agency's activities and operations.

(7) The Auditor shall charge and collect from each examining and licensing board the actual cost of each audit of such board. Costs collected under this subdivision shall be based on the actual expense incurred by the Auditor's office in making such audit and the affected agency shall be entitled to an itemized statement of such costs. Amounts collected under this subdivision shall be deposited into the general fund as nontax revenue.

(8) The Auditor shall examine as often as may be deemed necessary the accounts kept by the Treasurer, and if he discovers any irregularity or deficiency therein, unless the same be rectified or explained to his satisfaction, report the same forthwith in writing to the General Assembly, with copy of such report to the Governor and Attorney General. In addition to regular audits, the Auditor shall check the

treasury records at the time a Treasurer assumes office (not to succeed himself), and therein charge him with the balance in the treasury, and shall check the Treasurer's records at the time he leaves office to determine that the accounts are in order.

(9) The Auditor may examine the accounts and records of any bank or financial institution relating to transactions with the State Treasurer, or with any State agency, or he may require banks doing business with the State to furnish him information relating to transactions with the State or State agencies.

(10) The Auditor may, as often as he deems advisable, conduct a detailed review of the bookkeeping and accounting systems in use in the various State agencies which are supported partially or entirely from State funds. Such examinations will be for the purpose of evaluating the adequacy of systems in use by these agencies and institutions. In instances where the Auditor determines that existing systems are outmoded, inefficient, or otherwise inadequate, he shall recommend changes to the State Controller. The State Controller shall prescribe and supervise the installation of such changes, as provided in G.S. 143B-426.39(2).

(11) The Auditor shall, through appropriate tests, satisfy himself concerning the propriety of the data presented in the Comprehensive Annual Financial Report and shall express the appropriate auditor's opinion in accordance with generally accepted auditing standards.

(12) The Auditor shall provide a report to the Governor and Attorney General, and other appropriate officials, of such facts as are in his possession which pertain to the apparent violation of penal statutes or apparent instances of malfeasance, misfeasance, or nonfeasance by an officer or employee.

(13) At the conclusion of an audit, the Auditor or his designated representative shall discuss the audit with the official whose office is subject to audit and submit necessary underlying facts developed for all findings and recommendations which may be included in the audit report. On audits of economy and efficiency and program results, the auditee's written response shall be included in the final report if received within 30 days from receipt of the draft report.

(14) The Auditor shall notify the General Assembly, the Governor, the Chief Executive Officer of each agency audited, and other persons as the Auditor deems appropriate that an audit report has been published, its subject and title, and the locations, including State libraries, at which the report is available. The Auditor shall then distribute copies of the report only to those who request a report. The copies shall be in written or electronic form, as requested. He shall also file a copy of the audit report in the Auditor's office, which will be a permanent public record; Provided, nothing in this subsection shall be construed as

authorizing or permitting the publication of information whose disclosure is otherwise prohibited by law.

(15) It is not the intent of the audit function, nor shall it be so construed, to infringe upon or deprive the General Assembly and the executive or judicial branches of State government of any rights, powers, or duties vested in or imposed upon them by statute or the Constitution.

(16) The Auditor shall be responsible for receiving reports of allegations of the improper governmental activities set forth in G.S. 126-84. The Auditor shall provide a telephone hotline to receive such allegations and informant may choose whether to remain anonymous. The Auditor shall implement the necessary policies and procedures to investigate hotline allegations and recommend appropriate action. When the allegation involves issues of substantial and specific danger to the public health and safety, the Auditor shall notify the appropriate agency immediately. In addition, the Auditor shall publicize the hotline number periodically and shall report findings to the agencies involved. The Auditor shall refer allegations concerning information technology security to the State Chief Information Officer.

All records maintained by the State Auditor which involve unsubstantiated allegations of improper governmental activities set forth in G.S. 126-84 shall be destroyed within four years from the date such allegation was received.

(17) The Auditor or the Auditor's designee, in conjunction with the State Controller and the State Budget Officer or their designees, shall handle the resolution of fee disputes between the Office of Information Technology Services and the State agencies receiving information technology services from the Office.

~~(18) 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. 147-33.111(a), 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 enter into a contract with a State agency under G.S. 147-33.111(c) for an assessment of network vulnerability, including network penetration or any similar procedure. Any contract with the Auditor for the assessment and testing shall be on a cost-reimbursement basis. 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). The Auditor shall provide the State Chief Information Officer with detailed reports of the security issues identified pursuant to this subdivision. For the purposes of this subdivision only, the Auditor is exempt from the provisions of Article 3 of Chapter 143 of the General Statutes in retaining contractors.~~"

**SECTION 2.** G.S. 147-64.7(a) reads as rewritten:

"(a) Access to Persons and Records. –

(1) The Auditor and his authorized representatives shall have ready access to persons and may examine and copy all books, records, reports, vouchers, correspondence, files, personnel files, investments, and any other documentation of any State agency. The review of State tax returns shall be limited to matters of official business and the Auditor's report shall not violate the confidentiality provisions of tax laws.

(2) The Auditor and his duly authorized representatives shall have such access to persons, records, papers, reports, vouchers, correspondence, books, and any other documentation which is in the possession of any individual, private corporation, institution, association, board, or other organization which pertain to:

a. Amounts received pursuant to a grant or contract from the federal government, the State, or its political subdivisions.

b. Amounts received, disbursed, or otherwise handled on behalf of the federal government or the State. In order to determine that payments to providers of social and medical services are legal and proper, the providers of such services will give the Auditor, or his authorized representatives, access to the records of recipients who receive such services.

(3) The Auditor shall, for the purpose of examination and audit authorized by this act, have the authority, and will be provided ready access, to examine and inspect all property, equipment, and facilities in the possession of any State agency or any individual, private corporation, institution, association, board, or other organization which were furnished or otherwise provided through grant, contract, or any other type of funding by the State of North Carolina, or the federal government.

(4) All contracts or grants entered into by State agencies or political subdivisions shall include, as a necessary part, a clause providing access as intended by this section.

(5) The Auditor and his authorized agents are authorized to examine all books and accounts of any individual, firm, or corporation only insofar as they relate to transactions with any agency of the State.

(6) Notwithstanding the other provisions of this section, the Auditor and his authorized representatives and agents may only have access to the staff, equipment, reports, records, or other documentation of the State

Chief Information Officer and the Office of Information Technology Services upon the express written permission of the State Chief Information Officer."

**SECTION 3.** G.S. 147-33.83(b) reads as rewritten:

"(b) No data of a confidential nature, as defined in the General Statutes or federal law, may be entered into or processed through any cost-sharing information resource center or network established under this section until safeguards for the data's security satisfactory to the department head and the State Chief Information Officer have been designed and installed and are fully operational. Nothing in this section may be construed to prescribe what programs to satisfy a department's objectives are to be undertaken, nor to remove from the control and administration of the departments the responsibility for program efforts, regardless whether these efforts are specifically required by statute or are administered under the general program authority and responsibility of the department. This section does not affect the provisions of ~~G.S. 147-64.6, 147-64.7, or 147-33.91.~~G.S. 147-33.91."

**SECTION 4.** G.S. 147-33.111(c) reads as rewritten:

"(c) ~~Before a State agency~~ The State Chief Information Officer may enter into ~~any~~ a contract with another party for an assessment of network vulnerability, including network penetration or any similar ~~procedure, the State agency shall notify the State Chief Information Officer and obtain approval of the request. The State Chief Information Officer shall refer the request to the State Auditor for a determination of whether the Auditor's office can perform the assessment and testing. If the State Auditor determines that the Auditor's office can perform the assessment and testing, then the State Chief Information Officer shall authorize the assessment and testing by the Auditor. If the State Auditor determines that the Auditor's office cannot perform the assessment and testing, then with the approval of the State Chief Information Officer and State Auditor, the State agency may enter into a contract with another party for the assessment and testing. If the State agency enters into a contract with another party for assessment and testing, the State agency shall issue public reports on the general results of the reviews. The contractor shall provide the State agency with detailed reports of the security issues identified that shall not be disclosed as provided in G.S. 132-6.1(c). The State agency shall provide the State Chief Information Officer and the State Auditor with copies~~ procedure. Copies of the detailed reports that are provided to the State Chief Information Officer by the contractor shall not be disclosed as provided in G.S. 132-6.1(c)."

**SECTION 5.** G.S. 147-33.113(a)(4) reads as rewritten:

"(4) Designating an agency liaison in the information technology area to coordinate with the State Chief Information Officer. The liaison shall be subject to a criminal background report from the State Repository of Criminal Histories, which shall be provided by the State Bureau of Investigation upon its receiving fingerprints from the liaison. If the liaison has been a resident of this State for less than five years, the background report shall include a review of criminal information from both the State and National Repositories of Criminal Histories. The

criminal background report shall be provided to the State Chief Information Officer and the head of the agency. ~~In addition, all personnel in the Office of State Auditor who are responsible for information technology security reviews pursuant to G.S. 147-64.6(c)(18) shall be subject to a criminal background report from the State Repository of Criminal Histories, which shall be provided by the State Bureau of Investigation upon receiving fingerprints from the personnel designated by the State Auditor.~~ For designated personnel who have been residents of this State for less than five years, the background report shall include a review of criminal information from both the State and National Repositories of Criminal Histories. ~~The criminal background reports shall be provided to the State Auditor.~~"

**SECTION 6.** All (i) statutory authority, powers, duties, and functions, including rule making, budgeting, and purchasing, (ii) records, (iii) personnel, personnel positions, and salaries, (iv) property, and (v) unexpended balances of appropriations, allocations, reserves, support costs, and other funds of the Department of State Auditor relating to information technology security assessment and computer systems auditing are transferred to and vested in the Office of Information Technology Services within the Office of the Governor. This transfer has all the elements of a Type I transfer, as defined in G.S. 143A-6.

**SECTION 7.** This act is effective when it becomes law.