GENERAL ASSEMBLY OF NORTH CAROLINA
SESSION 2003

SESSION LAW 2003-153
HOUSE BILL 1003

AN ACT RELATING TO STATE GOVERNMENT INFORMATION TECHNOLOGY SECURITY.

The General Assembly of North Carolina enacts:

SECTION 1.(a) G.S. 147-33.82 is amended by adding a new section to read:

"(e1) The State Chief Information Officer shall assess the ability of each agency to comply with the current security enterprise-wide set of standards established pursuant to this section. The assessment shall include, at a minimum, the rate of compliance with the standards in each agency and an assessment of each agency's security organization, network security architecture, and current expenditures for information technology security. The assessment shall also estimate the cost to implement the security measures needed for agencies to fully comply with the standards. Each agency subject to the standards shall submit information required by the State Chief Information Officer for purposes of this assessment. Not later than May 4, 2004, the Information Resources Management Commission and the State Chief Information Officer shall submit a public report that summarizes the status of the assessment, including the available estimates of additional funding needed to bring agencies into compliance, to the Joint Legislative Commission on Governmental Operations and shall provide updated assessment information by January 15 of each subsequent year."

SECTION 1.(b) G.S. 147-33.82(f) reads as rewritten:

"(f) The head of each State agency shall cooperate with the State Chief Information Officer in the discharge of his or her duties by:

(1) Providing the full details of the agency's information technology and operational ~~requirements.~~requirements and of all the agency's information technology security incidents within 24 hours of confirmation.

(2) Providing comprehensive information concerning the information technology security employed to protect the agency's information technology.

(3) Forecasting the parameters of the agency's projected future information technology security needs and capabilities.

(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.

The information provided by State agencies to the State Chief Information Officer under this subsection is protected from public disclosure pursuant to G.S. 132-6.1(c)."

SECTION 2. Article 3D of Chapter 147 of the General Statutes is amended by adding a new section to read:

"**§ 147-33.89. Business continuity planning.**

(a) Each State agency shall develop and continually review and update as necessary a business and disaster recovery plan with respect to information technology. Each agency shall establish a disaster recovery planning team to develop the disaster recovery plan and to administer implementation of the plan. In developing the plan, the disaster recovery planning team shall do all of the following:

(1) Consider the organizational, managerial, and technical environments in which the disaster recovery plan must be implemented.

(2) Assess the types and likely parameters of disasters most likely to occur and the resultant impacts on the agency's ability to perform its mission.

(3) List protective measures to be implemented in anticipation of a natural or man-made disaster.

(b) Each State agency shall submit its disaster recovery plan on an annual basis to the Information Resource Management Commission and the State Chief Information Officer."

SECTION 3. This act is effective when it becomes law.

In the General Assembly read three times and ratified this the 28th day of May, 2003.

s/ Beverly E. Perdue
President of the Senate

s/ James B. Black
Speaker of the House of Representatives

s/ Michael F. Easley
Governor

Approved 11:45 p.m. this 4th day of June, 2003