GENERAL ASSEMBLY OF NORTH CAROLINA

SESSION 2003

H **2**

HOUSE BILL 1003
Committee Substitute Favorable 4/22/03

Short Title: IT Security Changes. (Public)

Sponsors:

Referred to:

April 10, 2003

A BILL TO BE ENTITLED

AN ACT RELATING TO STATE GOVERNMENT INFORMATION TECHNOLOGY SECURITY.

The General Assembly of North Carolina enacts:

SECTION 1. 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.

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.