

GENERAL ASSEMBLY OF NORTH CAROLINA
SESSION 2001

S

1

SENATE BILL 1096

Short Title: Security Standards for State IT.

(Public)

Sponsors: Senators Reeves; and Gulley.

Referred to: Information Technology.

April 5, 2001

A BILL TO BE ENTITLED

AN ACT PROVIDING FOR THE ADOPTION OF ENTERPRISE-WIDE SECURITY
AND ENCRYPTION STANDARDS FOR STATE GOVERNMENT
INFORMATION TECHNOLOGY.

The General Assembly of North Carolina enacts:

SECTION 1. Article 3D of Chapter 147 of the General Statutes is amended
by adding a new section to read:

"§ 147-33.89. State security and encryption standards.

(a) Notwithstanding G.S. 143-48.3, or any other provision of law, every
information technology security feature purchased using State funds, or for use by a
State agency or in a State facility, shall be subject to approval by the State Chief
Information Officer in accordance with security standards adopted under this section,
except that:

(1) If the legislative branch or the judicial branch develops security
standards that exceed those set by the State Chief Information Officer
under this section, then the legislative branch and the judicial branch
may elect to be governed by their own respective security standards,
and approval of the State Chief Information Officer shall not be
required before the purchase of information technology security
features. The State Chief Information Officer shall consult with the
legislative branch and the judicial branch in reviewing their standards.
The State Auditor shall mediate any disputes arising under this
subdivision.

(2) If the Governor certifies that a State agency has developed security
standards that exceed those set by the State Chief Information Officer
under this section, then the agency may elect to be governed by its
own security standards, and approval of the State Chief Information

1 Officer shall not be required before the purchase of information
2 technology security features.

3 The State Chief Information Officer may assume the direct responsibility of
4 providing for the information technology security of any State agency that fails to
5 adhere to security standards adopted pursuant to this section.

6 (b) The State Chief Information Officer shall establish an enterprise-wide set of
7 standards for information security to maximize the functionality, security, and
8 interoperability of the State's distributed information technology assets, including
9 communications and encryption technologies. As part of this function, the State Chief
10 Information Officer shall review existing security standards and practices in place
11 among the various State agencies to determine whether those standards and practices
12 meet enterprise-wide security and encryption requirements.

13 (c) The State Chief Information Officer shall consult the Information Technology
14 Management Advisory Council in the development of the enterprise-wide set of
15 standards for the State's information security. After approval by the Information
16 Technology Management Advisory Council, the Information Resources Management
17 Commission shall consider the standards and report approval of the standards to the
18 Joint Legislative Commission on Governmental Operations prior to implementation of
19 the standards. The State Chief Information Officer shall review and revise the standards
20 at least annually, and the revisions shall be subject to approval by the Information
21 Resources Management Commission, with the Commission reporting to the Joint
22 Legislative Commission on Governmental Operations on the revisions.

23 (d) The head of each State agency shall cooperate with the State Chief
24 Information Officer in the discharge of his or her duties under this section by:

25 (1) Providing the full details of the agency's information technology and
26 operational requirements.

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

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

31 (4) Designating an agency liaison in the information technology area to
32 coordinate with the State Chief Information Officer.

33 (e) Notwithstanding G.S. 147-33.80, the provisions of this section apply to every
34 State agency, to the General Assembly, to the Judicial Department, and to The
35 University of North Carolina and its constituent institutions. The term 'State agency'
36 means every State agency, institution, board, commission, council, member of the
37 Council of State, or officer of the State government."

38 **SECTION 2.** G.S. 147-64.6(c) is amended by adding a new subdivision to
39 read:

40 "(17) The State Auditor shall investigate reported information technology
41 security breaches, cyber attacks, and cyber fraud in State government."

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