FILED SENATE
Mar 27, 2017
S.B. 394
PRINCIPAL CLERK

GENERAL ASSEMBLY OF NORTH CAROLINA
SESSION 2017

S **D**

SENATE BILL DRS45272-MQ-54A (03/02)

Short Title:	Legislative Cybersecurity Committee.	(Public)
Sponsors:	Senators Tarte, Brock, and Hise (Primary Sponsors).	
Referred to:		

A BILL TO BE ENTITLED

AN ACT ESTABLISHING THE LEGISLATIVE CYBERSECURITY COMMITTEE.

The General Assembly of North Carolina enacts:

SECTION 1. Article 26 of Chapter 120 of the General Statutes reads as rewritten:

"Article 26.

"Joint Legislative Oversight Committee on Information ~~Technology.~~Technology and the Legislative Cybersecurity Committee.

"Part 1. Joint Legislative Oversight Committee on Information Technology.

…

"Part 2. Legislative Cybersecurity Committee.

"**§ 120-238. Definitions.**

The following definitions apply in this Part:

(1) Committee. – Legislative Cybersecurity Committee, also known as the LCC.

(2) Information resources. – Data and the means for storing, retrieving, connecting, or using data, including, but not limited to, records, files, databases, documents, software, equipment, and facilities that a State agency owns or leases.

(3) Information security assessment. – An (i) organized method to determine a risk to or a vulnerability of a State agency's information system or a third-party information service to which a State agency subscribes and (ii) independent examination and review of records, logs, policies, activities, and practices used to do the following:

a. Assess whether a State agency's information system is vulnerable to an information security incident.

b. Ensure compliance with rules, policies, standards, and procedures that the State Chief Information Officer or a State agency, under the State agency's independent authority, adopts or otherwise promulgates.

c. Recommend necessary changes to a State agency's rules, policies, standards, and procedures to ensure compliance and prevent information security incidents.

(4) Information technology or IT. – As defined by G.S. 143B-1320(a)(11).

(5) Information technology security incident. – As defined by G.S. 143B-1320(a)(12). The term also includes any incident that creates a risk of harm to a State agency or the State agency's operations and in which any of the following occurs:

a. Access to, or viewing, copying, transmission, theft, or usage of, a State agency's sensitive, protected, or confidential information occurs without authorization from the State agency.

b. A failure of compliance with a State agency's security or acceptable use policies or practices occurs that results in access to a State agency's information system or information resources for viewing, copying, transmission, theft, or use without the State agency's authorization.

c. A State agency's information system or information resources or a third party information service to which a State agency subscribes becomes unavailable in a reliable and timely manner to authorized individuals or organizations, or is modified or deleted under circumstances that the State agency does not intend, plan, or initiate.

(6) Security incident. – As defined by G.S. 143B-1320(a)(15).

(7) State agency. – As defined by G.S. 143C-1-1(d)(24).

"**§ 120-238.1. Creation, membership, and organization of Legislative Cybersecurity Committee.**

(a) The Legislative Cybersecurity Committee is established. The Committee consists of 12 members as follows:

(1) Six members of the Senate appointed by the President Pro Tempore of the Senate.

(2) Six members of the House of Representatives appointed by the Speaker of the House of Representatives.

(b) Terms on the Committee are for two years and begin on the convening of the General Assembly in each odd-numbered year. Members may complete a term of service on the Committee even if they do not seek reelection or are not reelected to the General Assembly, but resignation or removal from service in the General Assembly constitutes resignation or removal from service on the Committee. A member continues to serve until a successor is appointed. A vacancy shall be filled within 30 days by the officer who made the original appointment. A member shall be subject to the provisions of G.S. 120-238.3.

(c) The President Pro Tempore of the Senate and the Speaker of the House of Representatives shall each designate a cochair of the Joint Legislative Oversight Committee on Cybersecurity. The Committee shall meet upon the joint call of the cochairs.

(d) A quorum of the Committee is eight members. No action may be taken except by a majority vote at a meeting at which a quorum is present. While in the discharge of its official duties, the Committee has the powers of a joint committee under G.S. 120-19 and G.S. 120-19.1 through G.S. 120-19.4. Members of the Committee shall receive subsistence and travel expenses as provided in G.S. 120-3.1. The Committee may contract for consultants or hire employees in accordance with G.S. 120-32.02. The Legislative Services Commission, through the Legislative Services Officer, shall assign professional staff to assist the Committee in its work. Upon the direction of the Legislative Services Commission, the Directors of Legislative Assistants of the Senate and of the House of Representatives shall assign clerical staff to the Committee. The expenses for clerical employees shall be borne by the Committee.

"**§ 120-238.2. Purpose and powers of Committee.**

(a) The Committee is charged with examining, on a continuing basis, the cybersecurity practices of State agencies in order to make ongoing recommendations to the General Assembly on ways to improve the effectiveness, efficiency, and quality of the State's cybersecurity and data loss prevention practices and measures. The Committee has the following powers and duties in order to carry out its charge:

(1) Monitoring State agency and Department of Information Technology cybersecurity and data loss prevention activities. This function includes

receiving timely notification from State agencies regarding all information technology security incidents and a description of the actions the State agency has taken or must reasonably take to prevent, mitigate, or recover from damage to, unauthorized access to, unauthorized modifications or deletions of, or other impairments of the integrity of the State agency's information system or information resources.

(2) Reviewing and monitoring State agency compliance with budgetary and other directives of the General Assembly relating to State agency cybersecurity and data loss prevention and monitoring State agency expenditures, deviations, and changes to the certified budget related to cybersecurity and data loss prevention.

(3) Requesting and receiving presentations and reports from State agencies on security incidents and information security assessments as well as audits, studies, and other reports as directed by law.

(4) Identifying opportunities for agencies to coordinate and collaborate to eliminate duplicative cybersecurity functions.

(5) Reviewing, in its discretion, any issues that affect State agency information resources that arise during the interim period between sessions of the General Assembly.

(b) The Committee shall make periodic reports to the General Assembly. A report to the General Assembly may contain legislative proposals to implement its recommendations.

"**§ 120-238.3. Nondisclosure requirements.**

(a) Each member of the Committee shall execute a nondisclosure agreement upon appointment to the Committee and any subsequent nondisclosure agreements, as appropriate. The nondisclosure agreement shall be provided by the Committee and shall contain at least all of the following provisions:

(1) A description of the parties to the agreement.

(2) A definition of the types of information covered by the agreement.

(3) The period of nondisclosure.

(4) Exclusions from the agreement.

(5) Description of how to handle information covered by the agreement that is received by the member.

(6) Types of permissible disclosure, such as those required by a court order.

(b) Disclosure of information covered by the nondisclosure agreement described in this section constitutes grounds for removal from the Committee by the appointing official.

(c) Willful or intentional disclosure of information covered by the nondisclosure agreement described in this section shall constitute a Class I felony.

"**§ 120-238.4. Closed session permitted; records of closed proceedings not public records.**

(a) In addition to the permitted purposes provided in G.S. 143-318.11(a), the LCC may conduct its business in closed session and exclude the public under G.S. 143-318.11 when required to do any of the following:

(1) Receive reports, audits, studies, or testimony that could provide sensitive information relating to the State agency cybersecurity, data loss prevention measures, protocols, or related budgetary expenditures.

(2) Discuss information technology security incidents affecting State agencies.

(3) Discuss the provision or status of measures taken to prevent information technology security incidents by the departments and agencies of this State.

(4) Discuss budgetary items and requests relating to the prevention and mitigation of security incidents.

(b) All minutes, documents, testimony, or other records relating to Committee proceedings occurring during a closed session held pursuant to this section are subject to the

nondisclosure provisions of G.S. 120-283.3 and are not public records within the meaning of Chapter 132 of the General Statutes.

(c) The Committee may, in its discretion and upon unanimous vote of the members, release information it has received pursuant to this Part. In exercising its discretion, the Committee shall consider the potential impact upon private and proprietary interests."

SECTION 2.(a) G.S. 143B-1322(c) is amended by adding a new subdivision to read:

"(22) Enter into nondisclosure agreements with the Legislative Cybersecurity Committee and the Chief Information Officers and department heads of participating agencies relating to the sharing of information on cybersecurity and data loss prevention practices and measures used by the Department and participating agencies."

SECTION 2.(b) G.S. 143B-1322(d) reads as rewritten:

"(d) Budgetary Matters. – The Department's budget shall incorporate information technology costs and anticipated expenditures of State agencies identified as participating agencies, together with all divisions, boards, commissions, or other State entities for which the principal departments have budgetary authority. The Office of State Budget and Management and the Office of State Controller shall cooperate with the Department in the assignment of budget codes in a manner that protects the security of the State's information technology assets."

SECTION 3. Part 7 of Article 15 of Chapter 143B of the General Statutes is amended by adding a new section to read:

"**§ 143B-1380. Incident reporting.**

(a) At least quarterly thereafter, the State CIO shall report to the Legislative Cybersecurity Committee on all of the following:

(1) Known instances of and attempts at cyber attack or data breach within the Department or participating agencies.

(2) Quantifiable data on losses stemming from instances of cyber attack or data breach.

(3) Identification of issues surrounding cybersecurity and data loss prevention practices and measures in place at the time of the cyber attack or data breach.

(4) Steps taken to prevent future cyber attacks and data breaches of a similar nature.

(5) Recommendations to the Committee on potential legislative action.

(b) The report required by this section is not a public record within the meaning of Chapter 132 of the General Statutes. Reports submitted to the Legislative Cybersecurity Committee are subject to the provisions of G.S. 120-238.3 and G.S. 120-238.4."

SECTION 4.(a) With the support of the staff of the Legislative Services Office and assistance from the State Chief Information Officer, the chairs of the Legislative Cybersecurity Committee created by Section 1 of this act shall determine the requirements and provisions of the nondisclosure agreement described by G.S. 120-238.3, as enacted by Section 1 of this act.

SECTION 4.(b) Notwithstanding any provision to the contrary in G.S. 120-238.1(b) and (c), as enacted by Section 1 of this act, the initial appointment of members to the Legislative Cybersecurity Committee shall be made on or before January 1, 2018, and the initial members shall serve for one year, during the 2018 Regular Session of the 2017 General Assembly, unless reappointed by the appointing official.

SECTION 5. This act is effective when it becomes law.