

GENERAL ASSEMBLY OF NORTH CAROLINA
SESSION 2017

S

1

SENATE BILL 394

Short Title: Legislative Cybersecurity Committee. (Public)

Sponsors: Senators Tarte, Brock, and Hise (Primary Sponsors).

Referred to: Rules and Operations of the Senate

March 28, 2017

1 A BILL TO BE ENTITLED
2 AN ACT ESTABLISHING THE LEGISLATIVE CYBERSECURITY COMMITTEE.
3 The General Assembly of North Carolina enacts:

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

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

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

9 ...

10 "Part 2. Legislative Cybersecurity Committee.

11 "§ 120-238. Definitions.

12 The following definitions apply in this Part:

- 13 (1) Committee. – Legislative Cybersecurity Committee, also known as the LCC.
14 (2) Information resources. – Data and the means for storing, retrieving,
15 connecting, or using data, including, but not limited to, records, files,
16 databases, documents, software, equipment, and facilities that a State agency
17 owns or leases.
18 (3) Information security assessment. – An (i) organized method to determine a
19 risk to or a vulnerability of a State agency's information system or a
20 third-party information service to which a State agency subscribes and (ii)
21 independent examination and review of records, logs, policies, activities, and
22 practices used to do the following:
23 a. Assess whether a State agency's information system is vulnerable to
24 an information security incident.
25 b. Ensure compliance with rules, policies, standards, and procedures
26 that the State Chief Information Officer or a State agency, under the
27 State agency's independent authority, adopts or otherwise
28 promulgates.
29 c. Recommend necessary changes to a State agency's rules, policies,
30 standards, and procedures to ensure compliance and prevent
31 information security incidents.
32 (4) Information technology or IT. – As defined by G.S. 143B-1320(a)(11).
33 (5) Information technology security incident. – As defined by
34 G.S. 143B-1320(a)(12). The term also includes any incident that creates a
35 risk of harm to a State agency or the State agency's operations and in which
36 any of the following occurs:



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

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

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

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

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

16 **§ 120-238.1. Creation, membership, and organization of Legislative Cybersecurity**
17 **Committee.**

18 (a) The Legislative Cybersecurity Committee is established. The Committee consists of
19 12 members as follows:

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

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

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

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

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

44 **§ 120-238.2. Purpose and powers of Committee.**

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

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

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

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

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

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

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

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

22 **"§ 120-238.3. Nondisclosure requirements.**

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

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

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

29 (3) The period of nondisclosure.

30 (4) Exclusions from the agreement.

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

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

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

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

38 **"§ 120-238.4. Closed session permitted; records of closed proceedings not public records.**

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

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

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

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

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

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

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

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

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

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

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

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

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

23 **§ 143B-1380. Incident reporting.**

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

- 26 (1) Known instances of and attempts at cyber attack or data breach within the
27 Department or participating agencies.
- 28 (2) Quantifiable data on losses stemming from instances of cyber attack or data
29 breach.
- 30 (3) Identification of issues surrounding cybersecurity and data loss prevention
31 practices and measures in place at the time of the cyber attack or data
32 breach.
- 33 (4) Steps taken to prevent future cyber attacks and data breaches of a similar
34 nature.
- 35 (5) Recommendations to the Committee on potential legislative action.

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

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

43 **SECTION 4.(b)** Notwithstanding any provision to the contrary in
44 G.S. 120-238.1(b) and (c), as enacted by Section 1 of this act, the initial appointment of
45 members to the Legislative Cybersecurity Committee shall be made on or before January 1,
46 2018, and the initial members shall serve for one year, during the 2018 Regular Session of the
47 2017 General Assembly, unless reappointed by the appointing official.

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