**South Carolina General Assembly**

121st Session, 2015-2016

**H. 3226**

**STATUS INFORMATION**

General Bill

Sponsors: Rep. M.S. McLeod

Document Path: l:\council\bills\bbm\9128dg15.docx

Introduced in the House on January 13, 2015

Currently residing in the House Committee on **Judiciary**

Summary: Department of Information Security

**HISTORY OF LEGISLATIVE ACTIONS**

Date Body Action Description with journal page number

12/18/2014 House Prefiled

12/18/2014 House Referred to Committee on **Judiciary**

1/13/2015 House Introduced and read first time ([House Journal‑page 156](file:///h:\HJ%20Archive\2015\01-13-15.docx))

1/13/2015 House Referred to Committee on **Judiciary** ([House Journal‑page 156](file:///h:\HJ%20Archive\2015\01-13-15.docx))

View the latest [legislative information](http://www.scstatehouse.gov/billsearch.php?billnumbers=3226&session=121&summary=B) at the website

**VERSIONS OF THIS BILL**

[12/18/2014](file:///p:\pprever\2015-16\3226_20141218.docx)

**A** **BILL**

TO AMEND THE CODE OF LAWS OF SOUTH CAROLINA, 1976, BY ADDING CHAPTER 38 TO TITLE 1 SO AS TO CREATE THE DEPARTMENT OF INFORMATION SECURITY TO PROVIDE A COMPREHENSIVE FRAMEWORK FOR ENSURING THE EFFECTIVENESS OF INFORMATION SECURITY CONTROLS OVER INFORMATION RESOURCES THAT SUPPORT STATE OPERATIONS AND ASSETS, TO PROVIDE THAT THE DEPARTMENT OF INFORMATION SECURITY’S DIRECTOR IS THE CHIEF INFORMATION SECURITY OFFICER, TO PROVIDE THAT THE DEPARTMENT SHALL OVERSEE AGENCY INFORMATION SECURITY POLICIES AND PRACTICES, TO PROVIDE THAT THE DEPARTMENT MAY PROMULGATE BINDING REGULATIONS REGARDING MINIMUM INFORMATION SECURITY REQUIREMENTS, TO PROVIDE STEPS EACH STATE AGENCY MUST TAKE REGARDING INFORMATION SECURITY, TO PROVIDE FOR AN ANNUAL INDEPENDENT EXTERNAL AUDIT OF EACH AGENCY’S INFORMATION SECURITY PROGRAM, AND TO PROVIDE FOR THE OPERATION OF A CENTRAL INFORMATION SECURITY INCIDENT CENTER; AND TO AMEND SECTION 1‑30‑10, AS AMENDED, RELATING TO DEPARTMENTS WITHIN THE EXECUTIVE BRANCH OF STATE GOVERNMENT, SO AS TO ADD THE DEPARTMENT OF INFORMATION SECURITY.

Be it enacted by the General Assembly of the State of South Carolina:

SECTION 1. The General Assembly finds that:

(1) in 2012, a cyber criminal gained access to South Carolina Department of Revenue computer systems utilizing malicious software, leading to the ultimate theft of more than six million of the State’s taxpayers’ personally identifying information that were not encrypted;

(2) under the State’s current decentralized approach to information security, each agency, the breach at the Department of Revenue could have occurred at any state agency;

(3) an agency cannot be allowed to decide its own risk tolerance for data loss and create its own information security plan, absent statewide oversight and standards; and

(4) the creation of a centralized Department of Information Security is necessary to provide statewide oversight and standards to all South Carolina State government to protect the personally identifiable information of all citizens and taxpayers of this State.

SECTION 2. A. Title 1 of the 1976 Code is amended by adding:

“CHAPTER 38

Department of Information Security

Section 1‑38‑10. For purposes of this chapter:

(1) ‘Agency’ means all state agencies, departments, boards, commissions, institutions, and authorities.

(2) ‘Information security’ means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

(a) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(b) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;

(c) availability, which means ensuring timely and reliable access to and use of information; and

(d) authentication, which means utilizing digital credentials to assure the identity of users and validate their access.

(3) ‘Information system’ means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information, and includes:

(a) computers and computer networks;

(b) ancillary equipment;

(c) software, firmware, and related procedures;

(d) services, including support services; and

(e) related resources.

(4) ‘Information technology’ means:

(a) with respect to an agency, any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the agency that requires the use:

( i) of that equipment; or

(ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product; and

(b) includes computers, ancillary equipment, including imaging peripherals, input, output, and storage devices necessary for security and surveillance, peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services, including support services, and related resources.

‘Information technology’ does not include any equipment acquired by a federal or state contractor incidental to a federal or state contract.

(5) ‘Personally identifiable information’ means information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual, including, but not limited to, social security numbers, debit card numbers, credit card numbers, and bank account numbers.

Section 1‑38‑20. (A) There is hereby established the Department of Information Security. The department shall:

(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support state operations and assets;

(2) recognize the highly networked nature of the current state computing environment and provide effective governmentwide management and oversight of the related information security risks, including the coordination of information security efforts;

(3) provide for development and maintenance of minimum controls required to protect state information and information systems;

(4) provide a mechanism for improved oversight of state agency information security programs;

(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures; and

(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

(B) The department shall consist of the Chief Information Security Officer, who is the director of the department, and a staff employed by the Chief Information Security Officer as necessary to carry out the duties of the department and as are authorized by law.

(C) The Governor shall appoint the Chief Information Security Officer with the advice and consent of the Senate. The Chief Information Security Officer shall serve a term coterminous with the Governor.

Section 1‑38‑30. The Chief Information Security Officer shall oversee agency information security policies and practices, including:

(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, by ensuring timely agency adoption of and compliance with standards promulgated pursuant to this chapter;

(2) requiring agencies, consistent with the standards promulgated pursuant to this chapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of:

(a) information collected or maintained by or on behalf of an agency; or

(b) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(3) overseeing agency compliance with the requirements of this chapter, including through any authorized action to enforce accountability for compliance with such requirements;

(4) reviewing at least annually, and approving or disapproving, agency information security programs;

(5) coordinating information security policies and procedures with related information resources management policies and procedures;

(6) overseeing the operation of the Federal information security incident center required by this chapter;

(7) ensuring that all personally identifiable information electronically or digitally maintained by an agency is encrypted; and

(8) reporting to the General Assembly by March first of each year on agency compliance with the requirements of this chapter, including:

(a) a summary of the findings of evaluations;

(b) significant deficiencies in agency information security practices; and

(c) planned remedial action to address such deficiencies.

Section 1‑38‑40. (A) The department may promulgate regulations necessary to implement the provisions of this chapter and to accomplish the objectives set forth in Sections 1‑38‑20 and 1‑38‑30. The regulations may include penalties for any agency in violation of this chapter.

(B) In promulgating regulations relating to the objectives set forth in Sections 1‑38‑20 and 1‑38‑30, the standards must provide minimum information security requirements that are necessary to improve the efficiency of operation or security of state information systems. These regulations are compulsory and binding.

(C) The head of an agency may employ standards for the cost‑effective information security for all operations and assets within or under the supervision of that agency that are more stringent than the standards promulgated by the department, if such standards:

(1) contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the department; and

(2) are otherwise consistent with policies and guidelines set forth by the Chief Information Security Officer.

Section 1‑38‑50. (A) The head of each agency shall:

(1) be responsible for:

(a) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of:

( i) information collected or maintained by or on behalf of the agency; and

(ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(b) complying with the requirements of this chapter and related policies, procedures, standards, and guidelines;

(c) ensuring that information security management processes are integrated with agency strategic and operational planning processes; and

(d) ensuring that all personally identifiable information electronically or digitally maintained by the agency is encrypted;

(2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through:

(a) assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

(b) determining the levels of information security appropriate to protect such information and information systems in accordance with standards set forth in this chapter;

(c) implementing policies and procedures to cost‑effectively reduce risks to an acceptable level; and

(d) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented; and

(3) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this chapter and related policies, procedures, standards, and guidelines.

(B) Each agency shall develop, document, and implement an agencywide information security program, approved by the Chief Information Security Officer, to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes:

(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;

(2) policies and procedures that:

(a) are based on the risk assessments required by item (1);

(b) cost‑effectively reduce information security risks to an acceptable level;

(c) ensure that information security is addressed throughout the life cycle of each agency information system; and

(d) ensure compliance with:

( i) the requirements of this chapter;

(ii) policies and procedures as may be prescribed by the Chief Information Security Officer; and

(iii) minimally acceptable system configuration requirements, as determined by the agency;

(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of:

(a) information security risks associated with their activities; and

(b) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually;

(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

(7) procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to this chapter, including:

(a) mitigating risks associated with such incidents before substantial damage is done;

(b) notifying and consulting with the Chief Information Security Officer; and

(c) notifying and consulting with law enforcement agencies, as appropriate; and

(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

(C) By March first of each year, each agency shall submit a report to the General Assembly detailing the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of this chapter. Also, the report shall include any significant deficiency in a policy, procedure, or practice identified.

(D) Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

Section 1‑38‑60. (A)(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices. The evaluation must be conducted by an independent external auditor. The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

(2) Each evaluation under this section shall include:

(a) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency’s information systems;

(b) an assessment, made on the basis of the results of the testing, of compliance with:

( i) the requirements of this chapter; and

(ii) related information security policies, procedures, standards, and guidelines; and

(c) separate presentations, as appropriate, regarding information security relating to national security systems.

(B) Each year, not later than such date established by the Chief Information Security Officer, the head of each agency shall submit to the Chief Information Security Officer the results of the evaluation required under this section.

Section 1‑38‑70. The Chief Information Security Officer shall ensure the operation of a central information security incident center to:

(1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;

(2) compile and analyze information about incidents that threaten information security; and

(3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities.

Section 1‑38‑80. (A) All agencies must adopt and implement the policies, guidelines, and standards developed by the Chief Information Security Officer.

(B) Upon request of the Chief Information Security Officer for information or data, all agencies must fully cooperate with and furnish the Chief Information Security Officer with all documents, reports, answers, records, accounts, papers, and other necessary data and documentary information to perform the mission of the department and to exercise the functions, powers, and duties of the department.”

B. Section 1‑30‑10(A) of the 1976 Code, as last amended by Act 121 of 2014, is further amended by adding an appropriately numbered item at the end to read:

“ . Department of Information Security”

SECTION 3. This act takes effect July 1, 2015.

‑‑‑‑XX‑‑‑‑