S E N A T E A M E N D M E N T

AMENDMENT NO. _____

Good/Lee
February 27, 2013

ADOPTED	TABLED	CARRIED OVER	FAILED	RECONSIDERED

Clerk of the Senate

ADOPTION NO. _____

BILL NO: S. 334 (Reference is to the original version.)

Senator proposed the following amendment (031313 AMENDMENT TO S334 FULL SFC (334C004.NL.DG13)))):

Amend the bill, by striking all after the title and inserting:

/ Whereas, between August 13, 2012 and September 15, 2012, a cyber criminal gained unprecedented access to forty-four South Carolina Department of Revenue computer systems utilizing thirty-three unique and undetected pieces of malicious software, leading to the ultimate theft of more than six million of the State's taxpayers' most sensitive pieces of personal identifying information that were not encrypted, including social security numbers, bank account information, and credit card numbers; and

Whereas, at no time during this extended period did the Department of Revenue prevent, mitigate, or detect the presence of the cyber criminal, who ultimately uploaded nearly seventy-five gigabytes of data containing millions of pieces of the State's citizens' personal and financial information; and

Whereas, the Department of Revenue did not discover this unprecedented crime until October 10, 2012, almost two months after the attack began, when a law enforcement agency contacted the Department of Revenue with evidence that a cyber security breach had occurred; and

Whereas, the public was notified by the Governor of South Carolina of the cyber security breach at the Department of Revenue, the largest to date in United States history, on October 26, 2012, at which time the public was informed of the initial steps that were being taken by the Governor and the Department of Revenue to mitigate the damaging effects of the cyber security breach; and

Whereas, at a cost of more than twenty million dollars to date, the Governor and the Department of Revenue have utilized emergency procurement laws of this State, to both investigate and close the unprecedented breach, as well as to provide victims of this breach, identity theft protection and resolution services; and

Whereas, the contract negotiated by the Governor and the Department of Revenue under emergency procurement laws of this State, include differing levels of credit report access, monitoring, alerts and identity theft insurance for free, for the initial year, after which time taxpayers would have to purchase the credit report access, monitoring, alerts and identity theft insurance portions of their current coverage at their own expense; and

Whereas, taxpayers whose personally identifiable information was stolen as a result of this unprecedented cyber security breach were victims through no fault of their own, and trusted the Department of Revenue to protect their most personal and valuable financial information from criminal attacks that could expose them, and their children, to long-term identity theft vulnerabilities; and

Whereas, the failure of the Department of Revenue to adequately protect taxpayers from this cyber security breach, warrants the provision of identity theft protection and resolution services to eligible persons beyond the initial year, free of charge; and

Whereas, the Department of Revenue declined technology services, including cyber security services, that had been offered free of charge by another entity of state government; and

Whereas, the Department of Revenue determined that the encryption of taxpayers' personally identifiable information was too costly and cumbersome to pursue; and

Whereas, security techniques were known and available but the Department of Revenue decided that the risk of such a breach was small enough to warrant inaction regarding the application of such security techniques; and

Whereas, this cyber security breach at the Department of Revenue was not primarily about the failure of technology, but was about the failure to deploy even the most basic technology and a failure of organizational structure; and

Whereas, under the State's current decentralized approach to information security, each agency, decides its own risk tolerance for data loss and creates its own information security plan, absent statewide oversight and standards, thereby undermining the State's overall cyber security posture and creating unacceptable risks for data breaches throughout all of state government; and

Whereas, the creation of a centralized Department of Information Security is necessary to provide statewide oversight and standards to all South Carolina State and local governments to protect the personally identifiable information of all citizens and taxpayers of this State; and

Whereas, the development and implementation of a single, common, statewide technology direction is fundamental to every aspect of state government, and that the creation of the Department of Information Security will best support the State in this endeavor to unify its technology strategies while identifying those solutions which best improve the protection of the personally identifiable information of the State's citizens. Now, therefore,

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

SECTION 1. A. Article 3, Chapter 4, Title 12 of the 1976 Code is amended by adding:

"Section 12-4-352. (A) As used in this section:

(1) 'Eligible person' means a taxpayer that filed a return with the department for any taxable year after 1997 and before 2013, whether by paper or electronic transmission, or any taxpayer whose personally identifiable information was contained on the return of another eligible person, including minor dependents.

(2) 'Identity theft protection' means identity fraud and protection products and services that attempt to proactively detect, notify, or prevent unauthorized access or misuse of a person's identifying information or financial information to fraudulently obtain resources, credit, government documents or benefits, phone or other utility services, bank or savings accounts, loans, or other benefits in the person's name.

(3) 'Identity theft resolution services' means products and services that attempt to mitigate the effects of identity fraud after personally identifiable information has been fraudulently obtained by a third party, including, but not limited to, identity theft insurance and other identity theft resolution services that are designed to resolve actual and potential identity theft and related matters.

(4) 'Person' means an individual, corporation, firm, association, joint venture, partnership, limited liability corporation, or any other business entity.

(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.

(B)(1) The Governor shall develop a protection plan to minimize the actual and potential costs and effects of identity theft perpetrated upon all eligible persons by providing identity theft protection and identity theft resolution services. The identity theft protection and identity theft resolution services must be free of charge to each eligible person.

(2) The Governor shall develop and implement a policy that is designed to ensure the safety of all personally identifiable information in possession of the Department of Revenue. The policy shall include, but is not limited to, the encryption of personally identifiable information both during transmission and at rest.

(3) The protection plan and policy implemented pursuant to items (1) and (2) may include assistance from or services provided by any executive branch agency of state government, including the Department of Consumer Affairs.

(C)(1) The protection plan implemented pursuant to subsection (B)(1) must include procurement by the Governor of one or more contracts for identity theft protection and identity theft resolution services for all eligible persons, including,

but not limited to, credit monitoring and alerts. In implementing the protection plan, the Governor must also consider including protections against government documents and benefits fraud, phone and other utilities fraud, bank fraud and loan fraud. The procurement of identity theft protection shall be governed by the South Carolina Consolidated Procurement Code and conducted in compliance with the following additional requirements. Any contract for identity theft protection or identity theft resolution services entered into by the Governor must be solicited through the Materials Management Office using the process set forth in Section 11-35-1530. Prior to issuance, the Governor's request for proposals must be reviewed and approved by an advisory panel composed of three members appointed by the Governor, Chairman of the Senate Finance Committee, and Chairman of the House Ways and Means Committee. The evaluation and ranking required by Section 11-35-1530 must be conducted by an evaluation panel composed of at least three members. The advisory panel must approve anyone selected to serve or otherwise participate with the evaluation panel and anyone authorized by the procurement officer to participate, directly or indirectly, in the selection process.

(2) Any contract entered into pursuant to subsection (B)(1) must be for a term of no more than five years. Upon the expiration of a contract or contracts, the Governor shall issue a report to the General Assembly containing findings and recommendations concerning the ongoing risk of identity theft to eligible persons, the services the contract or contracts provided, and the need, if any, for extending the period for the contracted services, including the levels of service required if such a need exists. Based on the findings of the report, the Governor may extend the provision of one or more services offered pursuant to subsection (B)(1) for one additional term of up to five years; however, the provisions of item (1) of this subsection must be complied with in procuring another contract.

(3) No service provided pursuant to subsection (B)(1) may be procured for a cost if the same service is available to eligible persons for free under state or federal law.

(D)(1) In order to ensure that every eligible person obtains identity theft protection and identity theft resolution services pursuant to subsection (B)(1), to the extent allowed by federal or state law, including Section 30-2-320, the Governor and the Department of Revenue must develop and implement a policy to make enrollment as simple as possible for each eligible person. The policy may include, but is not limited to, automatic enrollment, provided that there is an opt-out mechanism for otherwise eligible persons, enrollment authorization on a tax return filed in this State, and enrollment authorization through a secure protected server on the department's website.

(2) By March fifteenth of each year, the Department of Revenue shall issue a report to the Governor and the General Assembly detailing the number of eligible persons that enrolled in the identity theft protection and identity theft resolution services program procured by the Governor pursuant to subsection (B)(1) in the most recent tax year for which there is an accurate figure and the number of people eligible to enroll. The report also must detail the efforts of the Governor and the Department of Revenue to increase enrollment in the programs.

(E) The Governor must include the estimated costs of implementing this section when submitting the executive budget pursuant to Article 1, Chapter 11, Title 11. Also, if the department, or an executive branch of state government, including the Department of Consumer Affairs, anticipate funds are necessary to implement the provisions of this section, they must account specifically for such estimated costs in making their annual budget request to the Office of State Budget pursuant to Article 1, Chapter 11, Title 11.

(F) Nothing in this section creates a private right of action or an expenditure of funds."

B. Article 9, Chapter 6, Title 12 of the 1976 Code is amended by adding:

"Section 12-6-1141. (A) In addition to the deductions allowed in Section 12-6-1140, there is allowed a deduction in computing South Carolina taxable income of an individual the actual costs, but not exceeding three hundred dollars for an individual taxpayer, and not exceeding one thousand dollars for a joint return or a return claiming dependents, incurred by a taxpayer in the taxable year to purchase a monthly or annual contract or subscription for identity theft protection and identity theft resolution services. The deduction allowed by this item may not be claimed by an individual if the individual deducted the same actual costs as a business expense or if the taxpayer is enrolled in the identity theft protection and identity theft resolution services program pursuant to Section 12-4-352(B)(1). For purposes of this item, 'identity theft protection' and 'identity theft resolution services' have the same meaning as provided in Section 12-4-352.

(B) By March fifteenth of each year, the department shall issue a report to the Governor and the General Assembly detailing the number of taxpayers claiming the deduction allowed by this item in the most recent tax year for which there is an accurate figure, and the total monetary value of the deductions claimed pursuant to this item in that same year.

(C) The department shall prescribe the necessary forms to claim the deduction allowed by this section. The department may require the taxpayer to provide proof of the actual costs and the taxpayer's eligibility.

C. Unless reauthorized by the General Assembly, SECTION 1B, as contained in this act, is repealed on January 1, 2018, and only applies to tax years beginning after 2012 and ending before 2018.

SECTION 2. A. Chapter 6, Title 37 of the 1976 Code is amended by adding:

"Part 7

Identity Theft Unit

Section 37-6-701. There is created within the Department of Consumer Affairs the Identity Theft Unit with duties and organizations as provided in this part.

Section 37-6-702. The Identity Theft Unit must be staffed and equipped to perform the functions prescribed in Section 37-6-703.

Section 37-6-703. The purpose of the Identity Theft Unit is to promote the protection of individuals' personal information, establish programs to inform the public with respect to identity theft, identity fraud and related unlawful conduct or practices, and provide identity theft and fraud resolution services to victims. The unit shall:

(1) receive complaints concerning identity theft, identity fraud, and related crimes;

(2) provide information and advice to the public on effective ways of handling complaints that involve identity theft, identity fraud, and related crimes;

(3) assist victims of identity theft, identity fraud, and related crimes in rectifying the effects of the theft or fraud through personalized assistance;

(4) refer complaints where appropriate to local, State, or federal agencies that are available to assist the public with identity theft, identity fraud, and related crimes;

(5) develop information and educational programs and materials to foster public understanding and recognition of the issues related to identity theft, identity fraud, and other unlawful conduct or practices;

(6) identify consumer problems in, and promote and facilitate the development and use of best practices in the protection of the privacy of personal information;

(7) promote voluntary and mutually agreed upon non-binding mediation of identity theft and identity fraud disputes where appropriate;

(8) cooperate and assist local, State, and federal law enforcement agencies in carrying out their legal enforcement responsibilities related to identity theft and identity fraud;

(9) assist and coordinate in the training of local, State, and federal law enforcement agencies regarding identity theft, identity fraud, and other privacy related crimes; and

(10) provide a centralized location where information related to incidents of identity theft may be securely stored and accessed for the benefit of victims of identity theft.

Section 37-6-704. By March fifteenth of each year, the division shall issue a report to the Governor, the General Assembly, and the Joint Information Security Oversight Committee with recommendations, including the text of an amendment effectuating the recommendations, to State and federal law, including the Consumer Protection Code, regarding identity theft that would reduce the occurrence of identity theft and the costs, monetary and otherwise, of identity theft."

B. Notwithstanding the general effective date of this act, this SECTION takes effect October 1, 2013.

SECTION 3. A. Title 1 of the 1976 Code is amended by adding:

"CHAPTER 36

Information Security

Article 1

Section 1-36-10. (A) There is hereby established within the Budget and Control Board the Division of Information Security that is dedicated to the protection of the State's information and cyber security infrastructure, including, but not limited to, the identification and mitigation of vulnerabilities, deterring and responding to cyber events, and promoting cyber security awareness within the State. The division also shall be responsible for statewide policies, standards, programs and services relating to cyber security and information systems, including the statewide coordination of critical infrastructure information. The divison shall consist of the Chief Information Security Officer, who is the director of the divison, and a staff employed by the Chief Information Security Officer as necessary to carry out the duties of the division and as are authorized by law. The Chief Information Security Officer, with advice and assistance of the Office of Human Resources of the Budget and Control Board, shall fix the salaries of all staff subject to the funds authorized in the annual general appropriations act. Subject to funding, the salaries of the staff involved with information technology must be competitive with the private sector. The compensation plan must be unique to information technology employees working at the Division of Information Security and consider all factors including areas requiring specialized skill sets, and should include components necessary to recruit and retain highly qualified information technology professionals to the State.

(B) After consulting with the Division of State Information Technology of the Budget and Control Board, the Governor shall appoint the Chief Information Security Officer with the advice and consent of the Senate for a term of four years, except that the initial appointment shall expire June 30, 2017. The Governor may reappoint the Chief Information Security Officer for additional terms. The Chief Information Security Officer's compensation must not be reduced during the Chief Information Security Officer's uninterrupted continued tenure in office.

(C) The Chief Information Security Officer may be removed from office only by the Governor as provided in Section 1-3-240(C).

Section 1-36-20.(A) In consultation with appropriate agency heads, the Chief Information Security Officer shall develop cyber security policies, guidelines, and standards. The Chief Information Security Officer shall oversee the implementation of and compliance with established standards. Each agency or agency head shall, under the management

of the Division of State Information Technology, install and administer state data security systems on its computer facilities consistent with these policies, guidelines, standards, and state law to ensure the integrity of computer-based and other data and to ensure applicable limitations on access to data. In furtherance of and in addition to these duties, the Chief Information Security Officer shall:

(1) include the identification and routine assessment of security risks at the agency level in the information security plan developed;

(2) regularly audit agencies to monitor compliance with established standards;

(3) require in the information security plan developed that agencies ensure service contractors follow established procedures when providing contracted services;

(4) coordinate all incident responses to agency cyber security breaches; and

(5) offer security services to agencies.

(B) The Chief Information Security Officer is responsible for overall security of state agency networks connected to the Internet as a component of the overall information technology function. Information technology remains the responsibility of the director of the Division of State Information Technology. Each agency or agency head is responsible for the security of the agency's data within the guidelines of the policy established by the Chief Information Security Officer.

Section 1-36-30. (A) In developing policies, guidelines, and standards, the Chief Information Security Officer must consider:

(1) developing an information technology governance structure that is inclusive of all agencies;

(2) adopting control objectives to manage, implement, and maintain information technology systems;

(3) developing security metrics that accurately measure unwanted intrusions, security breaches, penetrations, and vulnerabilities;

(4) developing security standards based on a full risk assessment of critical infrastructure vulnerabilities; and

(5) developing a method for the sharing of security information sharing and analysis.

(B) The Chief Information Security Officer and the director of the Division of State Information Technology shall collaborate with each other in developing policies, guidelines and standards required by each office.

Section 1-36-40. (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 division's mission and to exercise the division's functions, powers, and duties.

(C) The Chief Information Security Officer shall coordinate at least one training conference annually for state agency information security officers and shall receive an appropriation for the conference in an amount sufficient to attract the top cyber security professionals in the country to speak and to produce training materials for attendees.

Section 1-36-50. For purposes of this chapter, 'Agency' means all state agencies, departments, boards, commissions, institutions, and authorities, except the legislative and judicial departments of state government, that collect or maintain personally identifiable information as defined in Section 12-4-352. 'Agency' also includes all political subdivisions of this State, including school districts, and public authorities that collect or maintain personally identifiable information as defined in Section 12-4-352.

Section 1-36-60. The Division of Information Security may promulgate regulations necessary to implement the provisions of this chapter and to accomplish the objectives set forth in Section 1-36-20. The regulations may include penalties for any agency in violation of Section 1-36-40.

Article 3

Technology Investment Council

Section 1-36-310. There is hereby established a Technology Investment Council. The council shall consist of seven members, appointed as follows:

(1) the Director of the Budget and Control Board, Division of State Information Technology, who shall serve as chairman;

(2) the Chief Information Security Officer;

(3) five members, with one appointment made by each: the Governor, President Pro Tempore of the Senate, Speaker of the House of Representatives, Chairman of the Senate Finance Committee, and Chairman of the House Ways and Means Committee.

Section 1-36-320. The duties of the council are as follows:

(1) adopt policies and procedures used to develop, review, and annually update a statewide technology plan and provide it to the Governor, Office of State Budget, and the General Assembly;

(2) by October 1, 2013, and each October first thereafter, the council shall provide the Governor, the Legislative Fiscal Office, the Executive Budget and Strategic Planning Office, and the General Assembly with a statewide technology plan. The plan shall discuss the State's overall technology needs over a multiyear period and the potential budgetary implications of meeting those needs;

(3) by November fifteenth of each year, the council shall make recommendations to the Governor and General Assembly regarding the funding of technology for the next fiscal year;

(4) enforce active project management, review the progress of current projects to determine if they are on budget and have met their project milestones, and when necessary, recommend the termination of projects; and

(5) develop minimum technical standards, guidelines, and architectures as required for state technology projects.

Section 1-36-330. To assist the council and Division of Information Security in fulfilling its duties, each agency shall name an individual to act as that agency's 'information security officer'. It is the intent of this section that such information security officers will act as the primary points of contact for appropriate communications between the council and the Division of Information Security."

B. Section 1-3-240(C)(1) of the 1976 Code, as last amended by Act 105 of 2012, is further amended by adding an appropriately numbered subitem at the end to read:

"( ) Chief Information Security Officer."

C. Notwithstanding the general effective date of this act, this SECTION takes effect July 1, 2013.

SECTION 4. Title 2 of the 1976 Code is amended by adding:

"CHAPTER 79

Joint Information Security Oversight Committee

Section 2-79-10. The General Assembly finds that:

(1) a need exists for the protection of the State's information and cyber security infrastructure;

(2) a need exists for statewide policies, standards, programs and services relating to cyber security and information systems; and

(3) it is necessary that the General Assembly be kept apprised of statewide efforts to improve cyber security, including any barriers to improved cyber security.

Section 2-79-20. There is created the Joint Information Security Oversight Committee to conduct a continuing study of the laws of this State affecting cyber security, including the receipt of information from the Department of Information Security regarding impediments to improved cyber security. The committee is composed of nine members appointed as follows:

(1) two members appointed by the Chairman of the Senate Finance Committee;

(2) two members appointed by the Chairman of the House Ways and Means Committee;

(3) one member appointed by the President Pro Tempore of the Senate;

(4) one member appointed by the Speaker of the House of Representatives;

(5) two members appointed by the Governor; and

(6) the Chief Information Security Officer who shall serve ex officio.

At its first meeting the committee shall organize by selecting from its membership a chairman, vice chairman, secretary, and other officers the committee may determine. The committee shall meet on the call of the chairman or a majority of the members. A quorum consists of five members. Terms of appointed committee members are coterminous with that of the appointing authority. The committee shall report its initial findings and recommendations to the General Assembly on March 15, 2014, and shall make a report to the General Assembly each year thereafter. The report shall include the text of an amendment that effectuates the recommendations.

Section 2-79-30. The committee shall make a continuous study and investigation of all facets of the laws and practices relating to cyber security, so as to recommend appropriate modifications. The committee and its subcommittees may hold hearings and act at the times and places within the State the chairman designates and require the appearance of witnesses and the production of documents as provided for in Chapter 69, Title 2.

Section 2-79-40. (A) The members of the committee are ineligible for compensation but shall receive the usual mileage, per diem, and subsistence as is provided by law for members of state boards, commissions, and committees. The allowed mileage, per diem, and subsistence must be paid from approved accounts of the Senate for the Senate appointees, from approved accounts of the House for the House appointees, from funds appropriated to the Office of the Governor for gubernatorial appointees, and from funds appropriated to the Department of Information Security for the Chief Information Security Officer.

(B) Upon funding from the General Assembly, the committee may engage or employ staff or consultants as may be necessary and prudent to assist the commission in the performance of its duties and responsibilities.

(C) Staffs of the Senate, the House of Representatives, and the Department of Information Security must be available to assist the commission in its work. Any other expenses incurred by the commission shall be paid equally from each respective house's approved account subject to the approval of the Senate Operations and Management Committee and the Speaker of the House."

SECTION 5. Except as otherwise provided, this act takes effect upon approval by the Governor.

/

Renumber sections to conform.
Amend title to conform.