Thomas R. Carper

AMENDMENT NO._____ Calendar No._____

Purpose: In the nature of a substitute.

IN THE SENATE OF THE UNITED STATES—113th Cong., 2d Sess.

S. 2519

To codify an existing operations center for cybersecurity.

Referred to the Committee on _____ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended to be proposed by Mr. CARPER

Viz:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "National Cybersecurity Protection Act of 2014".

SEC. 2. DEFINITIONS.

In this Act—

(1) the term "Center" means the national cybersecurity and communications integration center under section 226 of the Homeland Security Act of 2002, as added by section 3;

(2) the term "critical infrastructure" has the meaning given that term in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101);

(3) the term "cybersecurity risk" has the meaning given that term in section 226 of the Homeland Security Act of 2002, as added by section 3;

(4) the term "information sharing and analysis organization" has the meaning given that term in section 212(5) of the Homeland Security Act of 2002 (6 U.S.C. 131(5));

(5) the term "information system" has the meaning given that term in section 3502(8) of title 44, United States Code; and

(6) the term "Secretary" means the Secretary of Homeland Security.

SEC. 3. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

(a) IN GENERAL.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.) is amended by adding at the end the following:

"SEC. 226. NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.

"(a) DEFINITIONS.—In this section—

"(1) the term 'cybersecurity risk' means threats to and vulnerabilities of information or information

systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of information or information systems, including such related consequences caused by an act of terrorism;

"(2) the term 'incident' means an occurrence that—

"(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system; or

"(B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies;

"(3) the term 'information sharing and analysis organization' has the meaning given that term in section 212(5); and

"(4) the term 'information system' has the meaning given that term in section 3502(8) of title 44, United States Code.

"(b) CENTER.—There is in the Department a national cybersecurity and communications integration center (referred to in this section as the 'Center') to carry

out certain responsibilities of the Under Secretary appointed under section 103(a)(1)(H).

"(c) FUNCTIONS.—The cybersecurity functions of the Center shall include—

"(1) being a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities;

"(2) providing shared situational awareness to enable real-time, integrated, and operational actions across the Federal Government and non-Federal entities to address cybersecurity risks and incidents to Federal and non-Federal entities;

"(3) coordinating the sharing of information related to cybersecurity risks and incidents across the Federal Government;

"(4) facilitating cross-sector coordination to address cybersecurity risks and incidents, including cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors;

"(5)(A) conducting integration and analysis, including cross-sector integration and analysis, of cybersecurity risks and incidents; and

"(B) sharing the analysis conducted under subparagraph (A) with Federal and non-Federal entities;

"(6) upon request, providing timely technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to cybersecurity risks and incidents, which may include attribution, mitigation, and remediation; and

"(7) providing information and recommendations on security and resilience measures to Federal and non-Federal entities, including information and recommendations to—

"(A) facilitate information security; and

"(B) strengthen information systems against cybersecurity risks and incidents.

"(d) COMPOSITION.—

"(1) IN GENERAL.—The Center shall be composed of—

"(A) appropriate representatives of Federal entities, such as—

"(i) sector-specific agencies;

"(ii) civilian and law enforcement agencies; and

"(iii) elements of the intelligence community, as that term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4));

"(B) appropriate representatives of non-Federal entities, such as—

"(i) State and local governments;

"(ii) information sharing and analysis organizations; and

"(iii) owners and operators of critical information systems;

"(C) components within the Center that carry out cybersecurity and communications activities;

"(D) a designated Federal official for operational coordination with and across each sector; and

"(E) other appropriate representatives or entities, as determined by the Secretary.

"(2) INCIDENTS.—In the event of an incident, during exigent circumstances the Secretary may grant a Federal or non-Federal entity immediate temporary access to the Center.

"(e) PRINCIPLES.—In carrying out the functions under subsection (c), the Center shall ensure—

"(1) to the extent practicable, that—

"(A) timely, actionable, and relevant information related to cybersecurity risks, incidents, and analysis is shared;

"(B) when appropriate, information related to cybersecurity risks, incidents, and analysis is integrated with other relevant information and tailored to the specific characteristics of a sector;

"(C) activities are prioritized and conducted based on the level of risk;

"(D) industry sector-specific, academic, and national laboratory expertise is sought and receives appropriate consideration;

"(E) continuous, collaborative, and inclusive coordination occurs—

"(i) across sectors; and

"(ii) with—

"(I) sector coordinating councils;

"(II) information sharing and analysis organizations; and

"(III) other appropriate non-Federal partners;

"(F) as appropriate, the Center works to develop and use mechanisms for sharing infor-

mation related to cybersecurity risks and incidents that are technology-neutral, interoperable, real-time, cost-effective, and resilient; and

"(G) the Center works with other agencies to reduce unnecessarily duplicative sharing of information related to cybersecurity risks and incidents;

"(2) that information related to cybersecurity risks and incidents is appropriately safeguarded against unauthorized access; and

"(3) that activities conducted by the Center comply with all policies, regulations, and laws that protect the privacy and civil liberties of United States persons.

"(f) NO RIGHT OR BENEFIT.—

"(1) IN GENERAL.—The provision of assistance or information to, and inclusion in the Center of, governmental or private entities under this section shall be at the sole and unreviewable discretion of the Under Secretary appointed under section 103(a)(1)(H).

"(2) CERTAIN ASSISTANCE OR INFORMATION.—The provision of certain assistance or information to, or inclusion in the Center of, one governmental or private entity pursuant to this section shall not

create a right or benefit, substantive or procedural, to similar assistance or information for any other governmental or private entity.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 note) is amended by inserting after the item relating to section 225 the following:

''Sec. 226. National cybersecurity and communications integration center.''.

SEC. 4. RECOMMENDATIONS REGARDING NEW AGREEMENTS.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Secretary shall submit recommendations on how to expedite the implementation of information-sharing agreements for cybersecurity purposes between the Center and non-Federal entities (referred to in this section as ''cybersecurity information-sharing agreements'') to—

(1) the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate; and

(2) the Committee on Homeland Security and the Committee on the Judiciary of the House of Representatives.

(b) CONTENTS.—In submitting recommendations under subsection (a), the Secretary shall—

(1) address the development and utilization of a scalable form that retains all privacy and other protections in cybersecurity information-sharing agreements that are in effect as of the date on which the Secretary submits the recommendations, including Cooperative Research and Development Agreements; and

(2) include in the recommendations any additional authorities or resources that may be needed to carry out the implementation of any new cybersecurity information-sharing agreements.

SEC. 5. ANNUAL REPORT.

Not later than 1 year after the date of enactment of this Act, and every year thereafter for 3 years, the Secretary shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate, the Committee on Homeland Security and the Committee on the Judiciary of the House of Representatives, and the Comptroller General of the United States a report on the Center, which shall include—

(a) information on the Center, including—

(1) an assessment of the capability and capacity of the Center to carry out its cybersecurity mission under this Act;

(2) the number of representatives from non-Federal entities that are participating in the Center, including the number of representatives from States, nonprofit organizations, and private sector entities, respectively;

(3) the number of requests from non-Federal entities to participate in the Center and the response to such requests;

(4) the average length of time taken to resolve requests described in paragraph (3);

(5) the identification of—

(A) any delay in resolving requests described in paragraph (3) involving security clearance processing; and

(B) the agency involved with a delay described in subparagraph (A);

(6) a description of any other obstacles or challenges to resolving requests described in paragraph (3) and a summary of the reasons for denials of any such requests;

(7) the extent to which the Department is engaged in information sharing with each critical infrastructure sector, including—

(A) the extent to which each sector has representatives at the Center;

(B) the extent to which owners and operators of critical infrastructure in each critical infrastructure sector participate in information sharing at the Center; and

(C) the volume and range of activities with respect to which the Secretary has collaborated with the sector coordinating councils and the sector-specific agencies to promote greater engagement with the Center; and

(8) the policies and procedures established by the Center to safeguard privacy and civil liberties.

SEC. 6. GAO REPORT.

Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the effectiveness of the Center in carrying out its cybersecurity mission.

SEC. 7. CYBER INCIDENT RESPONSE PLAN; CLEARANCES; BREACHES.

(a) CYBER INCIDENT RESPONSE PLAN; CLEARANCES.—Subtitle C of title II of the Homeland Security Act of 2002 (6 U.S.C. 141 et seq.), as amended by section 3, is amended by adding at the end the following:

"SEC. 227. CYBER INCIDENT RESPONSE PLAN.

"The Under Secretary appointed under section 103(a)(1)(H) shall, in coordination with appropriate Federal departments and agencies, State and local governments, sector coordinating councils, information sharing and analysis organizations (as defined in section 212(5)), owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, regularly update, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks (as defined in section 226) to critical infrastructure.

"SEC. 228. CLEARANCES.

"The Secretary shall make available the process of application for security clearances under Executive Order 13549 (75 Fed. Reg. 162; relating to a classified national security information program) or any successor Executive Order to appropriate representatives of sector coordinating councils, sector information sharing and analysis organizations (as defined in section 212(5)), owners and operators of critical infrastructure, and any other person that the Secretary determines appropriate.".

(b) BREACHES.—

(1) REQUIREMENTS.—The Director of the Office of Management and Budget shall ensure that data breach notification policies and guidelines are updated periodically and require—

(A) except as provided in paragraph (4), notice by the affected agency to each committee of Congress described in section 3544(c)(1) of title 44, United States Code, the Committee on the Judiciary of the Senate, and the Committee on Homeland Security and the Committee on the Judiciary of the House of Representatives, which shall—

(i) be provided expeditiously and not later than 30 days after the date on which the agency discovered the unauthorized acquisition or access; and

(ii) include—

(I) information about the breach, including a summary of any information that the agency knows on the date on which notification is provided about how the breach occurred;

(II) an estimate of the number of individuals affected by the breach, based on information that the agency knows on the date on which notification is provided, including an assessment of the risk of harm to affected individuals;

(III) a description of any circumstances necessitating a delay in providing notice to affected individuals; and

(IV) an estimate of whether and when the agency will provide notice to affected individuals; and

(B) notice by the affected agency to affected individuals, pursuant to data breach notification policies and guidelines, which shall be provided as expeditiously as practicable and without unreasonable delay after the agency discovers the unauthorized acquisition or access.

(2) NATIONAL SECURITY; LAW ENFORCEMENT; REMEDIATION.—The Attorney General, the head of an element of the intelligence community (as such term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)), or the Secretary may delay the notice to affected individuals under paragraph (1)(B) if the notice would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions.

(3) OMB REPORT.—During the first 2 years beginning after the date of enactment of this Act, the Director of the Office of Management and Budget shall, on an annual basis—

(A) assess agency implementation of data breach notification policies and guidelines in aggregate; and

(B) include the assessment described in clause (i) in the report required under section 3543(a)(8) of title 44, United States Code.

(4) EXCEPTION.—Any element of the intelligence community (as such term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)) that is required to provide notice under paragraph (1)(A) shall only provide such notice to appropriate committees of Congress.

(c) RULE OF CONSTRUCTION.—Nothing in the amendment made by subsection (a) or in subsection (b)(1) shall be construed to alter any authority of a Federal agency or department.

(d) TECHNICAL AND CONFORMING AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 note), as amended by section 3, is amended by inserting after the item relating to section 226 the following:

SEC. 8. RULES OF CONSTRUCTION.

(a) PROHIBITION ON NEW REGULATORY AUTHORITY.—Nothing in this Act or the amendments made by this Act shall be construed to grant the Secretary any authority to promulgate regulations or set standards relating to the cybersecurity of private sector critical infrastructure that was not in effect on the day before the date of enactment of this Act.

(b) PRIVATE ENTITIES.—Nothing in this Act or the amendments made by this Act shall be construed to require any private entity—

(1) to request assistance from the Secretary; or

(2) that requested such assistance from the Secretary to implement any measure or recommendation suggested by the Secretary.