SA 2760. Mr. JOHNSON of South Dakota submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2761. Mr. JOHNSON of South Dakota submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2762. Mr. JOHNSON of South Dakota submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2763. Ms. LANDRIEU submitted an amendment intended to be proposed by her to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2764. Mr. COCHRAN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2765. Mr. COCHRAN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2766. Mr. COCHRAN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2767. Mr. COCHRAN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2768. Mr. COCHRAN submitted an amendment intended to be proposed by him to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2769. Mr. LEAHY submitted an amendment intended to be proposed to amendment SA 2579 submitted by Mr. LEAHY and intended to be proposed to the bill S. 3414, supra; which was ordered to lie on the table.

SA 2770. Mr. REID (for Mr. CARPER (for himself, Ms. COLLINS, Mr. BROWN of Massachusetts, and Mr. COBURN)) proposed an amendment to the bill S. 1409, to intensify efforts to identify, prevent, and recover payment error, waste, fraud, and abuse within Federal spending.

## TEXT OF AMENDMENTS

**SA 2743.** Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of section 604, add the following:

(__) CONSTRUCTION.—

(1) IN GENERAL.—Nothing in this Act may be construed as—

(A) an authorization for any person, entity, or element of the Federal Government, or any person or entity acting on behalf of an element of the Federal Government, to take, authorize, or direct any offensive cyber-related action against a foreign country or an entity owned or controlled by a foreign country; or

(B) an authorization for any person, entity, or element of the Federal Government, or any person or entity acting on behalf of an element of the Federal Government, to take, authorize, or direct any cyber-related action if such action is likely to cause death or serious bodily harm to any person outside of the jurisdiction of the United States,

unless Congress has declared war or otherwise specifically authorized such action pursuant to Article I, section 8, of the Constitution.

(2) CYBER-RELATED ACTIONS.—For purposes of this subsection, a cyber-related action includes, but is not limited to, any action by cyber means as follows:

(A) An action to disable a power grid or power source that will result in temporary or permanent loss of electricity to a civilian area.

(B) An action to disable or to cause a temporary or permanent malfunction of a civilian water supply, reservoir, or water source.

(C) An action to disable or otherwise cause a temporary or permanent loss of a civilian communication system, including telephone, electronic mail, or Internet services for a civilian population.

(D) An action to disrupt or disable a civilian transportation network, including, but not limited to—

(i) a transportation hub;

(ii) a railroad or train;

(iii) motor vehicles;

(iv) airplanes; and

(v) traffic signals, including motor vehicle and railroad traffic signals.

(3) DEFENSIVE ACTIONS.—Nothing in this subsection shall be construed to limit the ability of the President to respond to an imminent cyber threat to the extent that such response is solely defensive in nature and intended to terminate an ongoing cyber action that is causing, or is likely to cause, significant damage, injury, or loss of life.

**SA 2744.** Mr. HOEVEN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of the bill, add the following:

**TITLE VIII—MISCELLANEOUS**

**SEC. 801. PILOT PROJECT OFFICES OF FEDERAL PERMIT STREAMLINING PILOT PROJECT.**

Section 365 of the Energy Policy Act of 2005 (42 U.S.C. 15924) is striking subsection (d) and inserting the following:

''(d) PILOT PROJECT OFFICES.—The following Bureau of Land Management Offices shall serve as the Pilot Project offices:

''(1) Rawlins Field Office, Wyoming.

''(2) Buffalo Field Office, Wyoming.

''(3) Eastern Montana/Dakotas District, Montana.

''(4) Farmington Field Office, New Mexico.

''(5) Carlsbad Field Office, New Mexico.

''(6) Grand Junction/Glenwood Springs Field Office, Colorado.

''(7) Vernal Field Office, Utah.''.

**SA 2745.** Mr. BROWN of Massachusetts submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 51, line 23, insert '', including through the use of security analytics whenever possible,'' after ''awareness''.

On page 53, line 9, insert '', including security analytics,'' after ''capabilities''.

On page 67, line 3, insert ''the use of real-time security analytics for'' before ''reporting''.

On page 72, line 1, insert '', real-time or near real-time analysis,'' after ''security testing''.

**SA 2746.** Ms. LANDRIEU submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 154, strike line 9, and insert the following:

**SEC. 415. REPORT ON NATIONAL GUARD CYBER-SECURITY CAPABILITIES.**

Not later than 180 days after the date of enactment of this Act, the Secretary, in consultation with the Secretary of Defense, shall submit to the appropriate committees of Congress a report on—

(1) the current cybersecurity defensive, offensive, and training capabilities within the National Guard;

(2) the current balance of cybersecurity defensive, offensive, and training capabilities across the Active and Reserve components of the Armed Forces and whether it achieves the appropriate balance between capability and cost; and

(3) the number of Federal cyber security civilian employees who are currently serving as members of the National Guard, including the States and units to which such National Guard members are assigned.

**SEC. 416. MARKETPLACE INFORMATION.**

**SA 2747.** Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 185, line 7, insert ''if a warrant has been obtained and'' after ''(A)''.

**SA 2748.** Mr. AKAKA (for himself, Mr. BLUMENTHAL, Mr. COONS, Mr. FRANKEN, Mr. SANDERS, Mr. UDALL of New Mexico, Mr. WYDEN, Mr. DURBIN, and Mrs. SHAHEEN) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 105, after the end of the matter between lines 11 and 12, insert the following:

**SEC. 205. PRIVACY BREACH REQUIREMENTS.**

(a) IN GENERAL.—Subchapter II of chapter 35 of title 44, United States Code, as amended by section 201 of this Act, is amended by adding at the end the following:

**''§ 3559. Privacy breach requirements**

''(a) POLICIES AND PROCEDURES.—The Director of the Office of Management and Budget shall establish and oversee policies and procedures for agencies to follow in the event of a breach of information security involving the disclosure of personally identifiable information, including requirements for—

''(1) timely notice to the individuals whose personally identifiable information could be compromised as a result of such breach;

''(2) timely reporting to a Federal cybersecurity center (as defined in section 708 of the Cybersecurity Act of 2012), as designated by the Director of the Office of Management and Budget; and

''(3) additional actions as necessary and appropriate, including data breach analysis, fraud resolution services, identity theft insurance, and credit protection or monitoring services.

''(b) REQUIRED AGENCY ACTION.—The head of each agency shall ensure that actions taken in response to a breach of information security involving the disclosure of personally identifiable information under the authority or control of the agency comply with policies and procedures established by the Director of the Office of Management and Budget under subsection (a).

''(c) REPORT.—Not later than March 1 of each year, the Director of the Office of Management and Budget shall report to Congress

on agency compliance with the policies and procedures established under subsection (a).''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for subtitle II for chapter 35 of title 44, United States Code, as amended by section 201 of this Act, is amended by adding at the end the following:

''3559. Privacy breach requirements.''.

**SEC. 206. AMENDMENTS TO THE E-GOVERNMENT ACT OF 2002.**

Section 208(b)(1)(A) of the E-Government Act of 2002 (44 U.S.C. 3501 note; Public Law 107–347) is amended—

(1) in clause (i), by striking ''or'' at the end;

(2) in clause (ii), by striking the period at the end and inserting ''; or''; and

(3) by adding at the end the following:

''(iii) using information in an identifiable form purchased, or subscribed to for a fee, from a commercial data source.''.

**SEC. 207. AUTHORITY OF THE DIRECTOR OF THE OFFICE OF MANAGEMENT AND BUDGET WITH RESPECT TO FEDERAL INFORMATION POLICY.**

Section 3504(g) of title 44, United States Code, is amended—

(1) paragraph (1), by striking ''and'' at the end;

(2) in paragraph (2), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following:

''(3) designate a Federal Chief Privacy Officer within the Office of Management and Budget who is a noncareer appointee in a Senior Executive Service position and who is a trained and experienced privacy professional to carry out the responsibilities of the Director with regard to privacy.''.

**SEC. 208. CIVIL REMEDIES UNDER THE PRIVACY ACT.**

Section 552a(g)(4)(A) of title 5, United States Code, is amended—

(1) by striking ''actual damages'' and inserting ''provable damages, including damages that are not pecuniary damages,''; and

(2) by striking '', but in no case shall a person entitled to recovery receive less than the sum of $1,000'' and inserting ''or the sum of $1,000, whichever is greater.''.

On page 188, lines 5 through 7, strike ''the Chief Privacy and Civil Liberties Officer of the Department of Justice and the Chief Privacy Officer of the Department'' and insert ''the Federal Chief Privacy Officer''.

On page 191, line 19, strike ''actual damages'' and insert ''provable damages, including damages that are not pecuniary damages,''

---

**SA 2749.** Mrs. MURRAY (for herself and Ms. LANDRIEU) submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 11, strike lines 12 and 13 and insert the following:

as appropriate;

(7) the National Guard Bureau; and

(8) the Department.

At the end of title IV, add the following:

**SEC. 416. REPORT ON ROLES AND MISSIONS OF THE NATIONAL GUARD IN STATE STATUS IN SUPPORT OF THE CYBERSECURITY EFFORTS OF THE FEDERAL GOVERNMENT.**

(a) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall, in consultation with the Secretary of Defense and the Chief of the National Guard Bureau, submit to the appropriate committees of Congress a report on the roles and missions of the National Guard in State status (commonly referred to as ''title 32 status'') in support of the cybersecurity efforts of the Department of Homeland Security, the Department of Defense, and other departments and agencies of the Federal Government.

(b) ELEMENTS.—The report required by subsection (a) shall include the following:

(1) A description of the current roles and missions of the National Guard in State status in support of the cybersecurity efforts of the Federal Government, and a description of the policies and authorities governing the discharge of such roles and missions.

(2) A description of the current roles and missions of the National Guard while on active duty in support of the cybersecurity efforts of the Federal Government, and a comparison of the costs to organize, train, and equip units of the National Guard on active duty in support of such efforts with the costs to organize, train, and equip units of the regular components of the Armed Forces with the same or similar capabilities in support of such efforts.

(3) A description of potential roles and missions for the National Guard in State status in support of the cybersecurity efforts of the Federal Government, a description of the policies and authorities to govern the discharge of such roles and missions, and recommendations for such legislative or administrative actions as may be required to establish and implement such roles and missions.

(4) An assessment of the feasability and advisability of public-private partnerships on homeland cybersecurity missions involving the National Guard in State status, including the advisability of using pilot programs to evaluate feasability and advisability of such partnerships.

(c) APPROPRIATE COMMITTEES OF CONGRESS DEFINED.—In this section, the term ''appropriate committees of Congress'' means—

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

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

---

**SA 2750.** Mr. MANCHIN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of title IV, add the following:

**SEC. 416. GOVERNMENT ACCOUNTABILITY OFFICE REPORT ON CRITICAL INFRASTRUCTURE OPERATIONS.**

(a) STUDY.—

(1) IN GENERAL.—The Comptroller General of the United States shall conduct a study of the efforts and authorities of the Federal Government and States relating to the resiliency of public and private critical infrastructure operations after natural or manmade disasters, cyber attacks, or accidents, including the ability to operate critical infrastructure with backup or alternative power generation.

(2) CONTENTS.—In conducting the study under paragraph (1), the Comptroller General shall—

(A) examine critical infrastructure, including—

(i) fueling stations;

(ii) water treatment facilities;

(iii) banking institutions;

(iv) health care facilities;

(v) the Emergency Alert System;

(vi) emergency 911 operations; and

(vii) any other critical infrastructure that the Comptroller General identifies;

(B) examine the role and authority of—

(i) State public utility or service commissions;

(ii) the Federal Communications Commission;

(iii) the Federal Energy Regulatory Commission;

(iv) the North American Electric Reliability Corporation;

(v) the Department of Energy; and

(vi) the Department;

(C) review policies on the priorities for restoring electrical power; and

(D) consider—

(i) the voluntary Defense Industrial Base Critical Infrastructure Protection program of the Department of Defense; and

(ii) the West Virginia University project for Cyber Security in Critical Infrastructure.

(b) REPORT.—Not later than 6 months after the date of enactment of this Act, the Comptroller General shall submit to Congress a report on the study conducted under subsection (a) that includes recommendations, if any, to improve the reliability, resiliency, and sustainability of, and to reduce any redundancy in, the critical infrastructure and related systems studied.

---

**SA 2751.** Mr. LIEBERMAN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 6, beginning on line 2, strike ''the underlying framework that information systems and assets rely on'' and insert ''information and information systems relied upon''.

On page 7, strike line 20 and all that follows through page 8, line 9, and insert the following:

(21) OPERATOR.—The term ''operator''—

(A) means an entity that manages, runs, or operates, in whole or in part, the day-to-day operations of critical infrastructure; and

(B) may include the owner of critical infrastructure.

(22) OWNER.—The term ''owner''—

(A) means an entity that owns critical infrastructure; and

(B) does not include a company contracted by the owner to manage, run, or operate that critical infrastructure, or to provide a specific information technology product or service that is used or incorporated into that critical infrastructure.

On page 8, beginning on line 14, strike '', or an attempted to cause an incident that, if successful, would have resulted in''.

On page 8, after line 22, insert the following:

**SEC. 3. RULE OF CONSTRUCTION.**

(a) DEFINITION.—In this section, the term ''covered information'' means information collected by a Federal agency solely for statistical purposes under a pledge of confidentiality.

(b) RULE OF CONSTRUCTION RELATING TO COVERED INFORMATION.—Nothing in this Act or an amendment made by this Act shall be construed to alter, amend, or repeal any provision of title 13, United States Code, the International Investment and Trade in Services Survey Act (22 U.S.C. 3101 et seq.), or the Confidential Information Protection and Statistical Efficiency Act of 2002 (44 U.S.C. 3501 note), or any similar provision of law, that relates to the unauthorized disclosure or use of covered information, except that the head of each Federal agency that collects covered information pursuant to any such provision of law is authorized to disclose the covered information to the Secretary to fulfill the information security responsibilities

of the head of the Federal agency and the Secretary under sections 3553 and 3554 of title 44, United States Code, as amended by this Act.

On page 10, line 7, before ''; and'' insert '', in connection with activities authorized and conducted in accordance with this title''.

On page 10, beginning on line 9, strike ''technical guidance or assistance to owners and operators consistent with this title'' and insert ''guidance on the application of cybersecurity practices in accordance with this title''.

On page 10, line 18, insert ''and'' after the semicolon.

On page 11, strike lines 1 through 13 and insert the following:

(d) MEMBERSHIP.—The Council shall be comprised of—

(1) the Secretary of Commerce;

(2) the Secretary of Defense;

(3) the Attorney General;

(4) the Director of National Intelligence;

(5) the heads of sector-specific Federal agencies that are appointed by the President, by and with the advice and consent of the Senate, as determined by the President in accordance with subsection (g);

(6) the heads of Federal agencies with responsibility for regulating the security of critical cyber infrastructure that are appointed by the President, by and with the advice and consent of the Senate, as determined by the President in accordance with subsection (g); and

(7) the Secretary.

On page 12, line 3, after ''provide'' insert '', to the maximum extent possible,''.

On page 12, line 5, after ''provide'' insert '', to the maximum extent possible,''.

On page 12, line 8, strike ''A'' and insert ''The head of a''.

On page 12, line 9, strike ''and a'' and insert ''or a''.

On page 12, line 13, after ''responsibility'' insert '', including''.

On page 13, line 13, after ''with'' insert ''appropriate''.

On page 13, line 20, strike ''180 days'' and insert ''90 days''.

On page 15, between lines 9 and 10, insert the following:

(6) INITIAL ASSESSMENTS.—Not later than 270 days after the date of enactment of this Act, the member agency designated under paragraph (1) shall complete initial cyber risk assessments described in paragraph (2)(B).

On page 17, line 16, strike ''damage'' and insert ''harm''.

On page 18, line 2, strike ''damage'' and insert ''harm''.

On page 20, line 5, strike ''180 days'' and insert ''1 year''.

On page 20, line 12, strike '', standards,''.

On page 20, line 22, after ''with'' insert ''appropriate''.

On page 21, beginning on line 3, strike ''relevant security experts and'' and insert ''appropriate security experts,''.

On page 21, between lines 17 and 18, insert the following:

(2) NIST INVOLVEMENT.—As part of the process described in paragraph (1), the Director of the National Institute of Standards and Technology shall be invited to provide advice and guidance on any possible amendments to the cybersecurity practices and any additional cybersecurity practices in consultation with appropriate public and private stakeholders.

On page 21, line 18, strike ''(2)'' and insert ''(3)''.

On page 21, line 19, strike ''1 year'' and insert ''18 months''.

On page 22, beginning on line 11, strike ''180 days'' and insert ''1 year''.

On page 22, line 13, strike ''1 year'' and insert ''18 months''.

On page 25, strike lines 10 through 17 and insert the following:

(1) IN GENERAL.—After the Council adopts a cybersecurity practice, a relevant sector coordinating council and the Critical Infrastructure Partnership Advisory Council may issue a public report evaluating the cybersecurity practice, which may include input from appropriate institutions of higher education, including university information security centers, national laboratories, and appropriate nongovernmental cybersecurity experts.

On page 25, line 19, strike ''consider any review conducted'' and insert ''consider, in accordance with subsection (c), any public report issued''.

On page 25, strike lines 21 through 24 and insert the following:

(i) VOLUNTARY GUIDANCE.—At the request of an owner or operator, the Council may provide guidance on the application of cybersecurity practices to the critical infrastructure in accordance with this title.

On page 26, line 5, strike ''1 year'' and insert ''18 months''.

On page 27, line 13, strike ''an assessment'' and insert ''a third-party assessment, in accordance with subsection (b),''.

On page 28, beginning on line 15, strike ''specific cybersecurity measures that, if implemented, would'' and insert ''guidance on how to''.

On page 29, line 5, strike ''owner'' and all that follows through line 7, and insert the following: ''owner has effectively implemented cybersecurity measures sufficient to satisfy the outcome-based cybersecurity practices established under section 103.''.

On page 30, line 20, strike ''Subaragraph'' and insert ''Subparagraph''.

On page 34, line 15, before ''or'' insert ''including under title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.),''.

On page 35, beginning on line 19, strike ''treated as voluntarily shared critical infrastructure information under'' and insert ''afforded the protections of''.

On page 36, beginning on line 16, strike ''covered critical'' and insert ''critical cyber''.

On page 36, beginning on line 19, strike ''concerns (in addition to any concerns described under subparagraph (A))'' and insert ''other concerns''.

On page 37, line 11, strike ''specifically prohibited by law or is''.

On page 37, line 14, after ''affairs'' insert ''or the disclosure of which is otherwise subject to legal restrictions''.

On page 41, line 4, strike ''1 year'' and insert ''2 years''.

On page 42, line 16, strike ''covered critical'' and insert ''critical cyber''.

On page 43, line 14, after ''and'' insert ''in connection with affording the protections of section 214 of the Homeland Security Act of 2012 (6 U.S.C. 133) to covered information in accordance with''.

On page 44, beginning on line 6, strike ''a private sector coordinating council'' and insert ''the entity''.

On page 44, line 9, strike ''sector of critical infrastructure'' and insert ''critical infrastructure or key resource sector''.

On page 44, line 10, after ''Plan'' insert '', or any successor plan''.

On page 44, line 15, strike ''under the National'' and all that follows through line 18, and insert the following: '', as designated by the President or the President's designee.''.

On page 46, beginning on line 6, strike ''improve and continuously monitor'' and insert ''continuously monitor and improve''.

On page 46, beginning on line 25, strike ''the complete set of''.

On page 47, line 2, after ''system'' insert ''have been implemented and''.

On page 47, line 5, strike ''To the maximum'' and all that follows through line 9.

On page 47, line 22, after ''protected'' insert '', or in accordance with section 3553(d)(3)''.

On page 47, between lines 22 and 23, insert the following:

''(4) CYBERSECURITY SERVICES.—The term ''cybersecurity services'' means products, goods, or services intended to detect, mitigate, or prevent cybersecurity threats.

On page 47, line 23, strike ''(4)'' and insert ''(5)''.

On page 48, line 8, strike ''(5)'' and insert ''(6)''.

On page 49, line 1, strike ''(6)'' and insert ''(7)''.

On page 49, line 4, strike ''(7)'' and insert ''(8)''.

On page 50, line 13, strike ''(8)'' and insert ''(9)''.

On page 53, line 7, strike ''and penetration testing'' and insert '', penetration testing, and the operation of a continuous monitoring capability to provide real-time visibility into the condition and status of agency information systems''.

On page 57, beginning on line 21, strike ''or information security services'' and insert ''services, remote computing services, or cybersecurity services''.

On page 57, line 24, strike ''or to deploy countermeasures'' and insert '', deploy countermeasures, or otherwise operate protective capabilities''.

On page 60, line 17, strike ''Assistant Secretary'' and all that follows through line 19, and insert the following: ''Director of the National Center for Cybersecurity and Communications.''.

On page 76, line 5, strike ''section 3553'' and insert ''section 3553(d)(3)''.

On page 77, beginning on line 17, strike ''under the control of the Department of Defense'' and insert ''described in section 3553(g)(2)''.

On page 77, beginning on line 20, strike ''under the control of the Central Intelligence Agency'' and insert ''described in section 3553(g)(3)''.

On page 77, beginning on line 24, strike ''under the control of the Office of the Director of National Intelligence'' and insert ''described in section 3553(g)(4)''.

On page 81, strike the matter between lines 15 and 16 and insert the following:

''SUBCHAPTER II—INFORMATION SECURITY

''3551. Purposes.
''3552. Definitions.
''3553. Federal information security authority and coordination.
''3554. Agency responsibilities.
''3555. Annual assessments.
''3556. Independent evaluations.
''3557. National security systems.
''3558. Effect on existing law.''.

On page 90, line 16, before ''National'' insert ''functions of the''.

On page 90, beginning on line 17, strike ''on the date of enactment of the Cybersecurity Act of 2012'' and insert ''transferred to the Department''.

On page 90, line 19, strike ''Order 12472'' and insert ''Order 13618''.

On page 91, beginning on line 19, strike ''National Communications System'' and insert ''functions of the National Communications System transferred to the Department under section 201(g)''.

On page 91, line 20, strike ''the'' and insert ''their''.

On page 91, line 21, strike ''liabilities of the'' and all that follows through line 24, and insert ''liabilities.''.

On page 93, line 20, after ''providing'' insert ''technical assistance, analysis of incidents, and other''.

On page 102, line 5, after ''as'' insert ''appropriate and''.

On page 105, line 23, strike ''authorized'' and insert ''permitted''.

On page 105, line 24, strike ''Code, or'' and insert ''Code,''.

On page 106, line 2, after ''et seq.)'' insert '', or section 3553 of title 44, United States Code''.

On page 113, line 19, after ''Communications'' insert '', and in consultation with the Director of the National Institute of Standards and Technology and the Administrator of the National Telecommunications and Information Administration''.

On page 120, line 15, before ''of'' insert ''and the Committee on Homeland Security and Governmental Affairs''.

On page 120, line 16, after ''Technology'' insert ''and the Committee on Oversight and Government Reform''.

On page 125, line 15, after ''other'' insert ''cybersecurity''.

On page 128, line 18, after ''Secretary'' insert ''and the Director of the Office of Personnel Management''.

On page 130, line 12, strike ''shall'' and insert ''may''.

On page 131, line 16, after ''Foundation'' insert '', in coordination with the Director of the Office of Personnel Management,''.

On page 134, line 6, strike ''all'' and insert ''appropriate''.

On page 136, line 17, strike ''engaged in'' and insert ''in vacant positions that are part of the Federal''.

On page 147, strike the matter between lines 3 and 4 and insert the following:

''Sec. 245. National Center for Cybersecurity and Communications acquisition authorities.

''Sec. 246. Recruitment and retention program for the National Center for Cybersecurity and Communications.''.

On page 152, strike line 20 and all that follows through page 153, line 14, and insert the following:

(1) legal or other impediments to appropriate public awareness of the nature of, methods of propagation of, and damage caused by common cybersecurity threats such as computer viruses, phishing techniques, and malware; and

(2) a summary of the plans of the Secretary to enhance public awareness of common cybersecurity threats, including a description of the metrics used by the Department for evaluating the efficacy of public awareness campaigns.

On page 201, line 19, strike ''or''.

On page 201, between lines 19 and 20, insert the following:

(11) to alter or amend the law enforcement or intelligence authorities of any agency or Federal cybersecurity center; or

On page 201, line 20, strike ''(11)'' and insert ''(12)''.

---

**SA 2752.** Mr. JOHNSON of South Dakota submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 156, line 3, strike ''(1);'' and all that follows through ''any public'' on line 10 and insert ''(1); and

''(3) any public''.

---

**SA 2753.** Mr. JOHNSON of South Dakota submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 61, between lines 4 and 5, insert the following:

''(D) CRITICAL INFRASTRUCTURE.—Notwithstanding subparagraph (A), if an agency identifies a system to the Secretary in writing as a system the disruption of which would cause grave damage to the economic infrastructure of the United States, including a system used to carry out payment, fiscal agency, lending, or liquidity activities or Federal open market operations, the Secretary may authorize the use of protective capabilities that affect the system only with the concurrence of the head of that agency.

---

**SA 2754.** Mr. JOHNSON of South Dakota submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 60, strike lines 1 through 13 and insert the following:

''(A) IN GENERAL.—If the Secretary determines that there is a substantial and imminent threat to agency information systems and, after consultation with the affected agency, determines that a directive under this subsection is not reasonably likely to result in a timely response to the threat, the Secretary may authorize the use of protective capabilities under the control of the Secretary for communications or other system traffic transiting to or from or stored on an agency information system. If prior consultation with the affected agency is not reasonably practicable under the circumstances, the Secretary may authorize the use of the protective capabilities without prior consultation with the affected agency for the purpose of ensuring the security of the information or information system or other agency information systems.

---

**SA 2755.** Mr. JOHNSON of South Dakota submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 58, strike lines 18 through 21 and insert the following:

''(B) EXCEPTION.—The authorities of the Secretary under this subsection shall not apply to—

''(i) a system described in paragraph (2), (3), or (4) of subsection (g); or

''(ii) a system used to carry out payment, fiscal agency, lending, or liquidity activities or Federal open market operations where the disruption of such system could reasonably result in catastrophic economic damage to the United States.

---

**SA 2756.** Mr. JOHNSON of South Dakota submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 55, line 22, insert '', with the concurrence of the affected agency,'' after ''the Secretary''.

---

**SA 2757.** Mr. JOHNSON of South Dakota submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 51, line 12, strike ''used or''.

---

**SA 2758.** Mr. JOHNSON of South Dakota submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 18, line 25, strike ''or'' and all that follows through page 19, line 2, and insert the following:

(C) a commercial item that organizes or communicates information electronically; or

(D) critical infrastructure that is subject to the requirements under subchapter II of chapter 35 of title 44, United States Code, as amended by section 201 of this Act.

---

**SA 2759.** Mr. JOHNSON of South Dakota submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 12, between lines 21 and 22, insert the following:

(h) FEDERAL RESERVE BANKS.—For purposes of this title, the Federal agency with responsibility for regulating the security of critical cyber infrastructure of the Federal Reserve Banks is the Board of Governors of the Federal Reserve System.

---

**SA 2760.** Mr. JOHNSON of South Dakota submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 12, line 12, insert ''or owner'' after ''the sector''.

---

**SA 2761.** Mr. JOHNSON of South Dakota submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 11, between lines 12 and 13, insert the following:

(7) the Department of the Treasury; and

---

**SA 2762.** Mr. JOHNSON of South Dakota submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 11, line 12, strike ''and''.

On page 11, between lines 12 and 13, insert the following:

(7) the Department of the Treasury; and

On page 11, line 13, strike ''(7)'' and insert ''(8)''.

On page 12, line 12, insert ''or owner'' after ''the sector''.

On page 12, between lines 21 and 22, insert the following:

(h) FEDERAL RESERVE BANKS.—For purposes of this title, the Federal agency with responsibility for regulating the security of critical cyber infrastructure of the Federal Reserve Banks is the Board of Governors of the Federal Reserve System.

On page 18, line 25, strike ''or'' and all that follows through page 19, line 2, and insert the following:

(C) a commercial item that organizes or communicates information electronically; or

(D) critical infrastructure that is subject to the requirements under subchapter II of chapter 35 of title 44, United States Code, as amended by section 201 of this Act.

On page 51, line 12, strike ''used or''.

On page 55, line 22, insert '', with the concurrence of the affected agency,'' after ''the Secretary''.

On page 58, strike line 18 and all that follows through page 60, line 13, and insert the following:

''(B) EXCEPTION.—The authorities of the Secretary under this subsection shall not apply to—

''(i) a system described in paragraph (2), (3), or (4) of subsection (g); or

''(ii) a system used to carry out payment, fiscal agency, lending, or liquidity activities or Federal open market operations where the disruption of such system could reasonably result in catastrophic economic damage to the United States.

''(2) PROCEDURES FOR USE OF AUTHORITY.—The Secretary shall—

''(A) in coordination with the Director of the Office of Management and Budget and, as appropriate, in consultation with operators of information systems, establish procedures governing the circumstances under which a directive may be issued under this subsection, which shall include—

''(i) thresholds and other criteria;

''(ii) privacy and civil liberties protections; and

''(iii) providing notice to potentially affected third parties;

''(B) specify the reasons for the required action and the duration of the directive;

''(C) minimize the impact of directives under this subsection by—

''(i) adopting the least intrusive means possible under the circumstances to secure the agency information systems; and

''(ii) limiting directives to the shortest period practicable; and

''(D) notify the Director of the Office of Management and Budget and head of any affected agency immediately upon the issuance of a directive under this subsection.

''(3) IMMINENT THREATS.—

''(A) IN GENERAL.—If the Secretary determines that there is a substantial and imminent threat to agency information systems and, after consultation with the affected agency, determines that a directive under this subsection is not reasonably likely to result in a timely response to the threat, the Secretary may authorize the use of protective capabilities under the control of the Secretary for communications or other system traffic transiting to or from or stored on an agency information system. If prior consultation with the affected agency is not reasonably practicable under the circumstances, the Secretary may authorize the use of the protective capabilities without prior consultation with the affected agency for the purpose of ensuring the security of the information or information system or other agency information systems.

On page 61, between lines 4 and 5, insert the following:

''(D) CRITICAL INFRASTRUCTURE.—Notwithstanding subparagraph (A), if an agency identifies a system to the Secretary in writing as a system the disruption of which would cause grave damage to the economic infrastructure of the United States, including a system used to carry out payment, fiscal agency, lending, or liquidity activities or Federal open market operations, the Secretary may authorize the use of protective capabilities that affect the system only with the concurrence of the head of that agency.

On page 61, line 5, strike ''(D)'' and insert ''(E)''.

On page 156, line 3, insert ''and'' after the semicolon.

On page 156, strike lines 4 through 9.

On page 156, line 10, strike ''(4)'' and insert ''(3)''.

---

**SA 2763.** Ms. LANDRIEU submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 108, line 21, after ''software'' insert '', hardware, and other cybersecurity technology''.

On page 121, line 6, after ''science'' insert ''and cyber-engineering''.

On page 121, line 14, after ''Foundation'' insert '', in consultation with the Secretary,''.

On page 124, line 13, strike ''national and statewide'' and insert ''national, statewide, regional, and local''.

On page 125, line 24, after ''other'' insert ''nonprofit or''.

On page 137, between lines 5 and 6, insert the following:

(e) REPORT.—The Secretary, in coordination with the Director of the Office of Personnel Management, the Director of National Intelligence, the Secretary of Defense, and the Chief Information Officers Council established under section 3603 of title 44, United States Code, shall submit a report to the appropriate committees of Congress on whether the establishment of a national institute dedicated to cybersecurity education and training described under subsection (b) is appropriate.

---

**SA 2764.** Mr. COCHRAN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

**SEC. ___. CRITICAL COMMUNICATIONS INFRASTRUCTURE PILOT PROGRAM.**

(a) DEFINITION.—In this section, the term ''passive Internet Protocol route analytics'' means a method for determining behaviors, patterns, and statuses of Internet Protocol network equipment and paths without—

(1) actively communicating directly with network equipment, such as routers and switches; or

(2) significantly inspecting the contents of an Internet Protocol network packet.

(b) ESTABLISHMENT.—Not later than 6 months after the date of enactment of this Act, the Manager of the National Coordinating Center for Telecommunications, acting through the National Communications System, shall initiate a 12-month pilot program to evaluate enhanced critical communications infrastructure, including systems supporting operational and situational awareness, national security, and emergency preparedness.

(c) EVALUATION CRITERIA.—By means of passive Internet Protocol route analytics, the pilot program under this section shall include criteria to evaluate the status of a representative subset of critical communications infrastructure.

(d) CONNECTIVITY.—The program shall at a minimum provide—

(1) end-to-end connectivity between the National Center for Critical Information Processing and Storage and United States Pacific Command facilities; and

(2) undersea communications between the mainland of the United States and Europe.

(e) TERMINATION.—The pilot program established under this section shall terminate 1 year after the date on which the program is established.

(f) REPORT.—Not later than 6 months after the termination date described in subsection (e), the Manager of the National Coordinating Center for Telecommunications, acting through the National Communications System, shall submit to the appropriate Congressional committees a report on the effectiveness and scalability of enhanced critical communications infrastructure, including systems supporting operational and situational awareness, national security, and emergency preparedness.

---

**SA 2765.** Mr. COCHRAN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 107, line 1, after ''science'' insert '', legal,''.

On page 108, strike lines 10 and 11 and insert the following:

amended by subsection (f);

(12) how improved education of judges and other legal professionals can contribute to cybersecurity; and

(13) any additional objectives the Director or

On page 115, line 11, before ''; and'' insert the following: '', including by increasing educational opportunities for judges and other legal professionals''.

On page 125, line 20, after ''State,'' insert ''national,''.

On page 126, strike lines 9 through 11 and insert the following:

(F) offensive and defensive cyber operations;

(G) legal analysis of cyber crime and cybersecurity; and

(H) other areas to fulfill the cybersecurity

At the end of title IV, add the following:

**SEC. 416. CYBER EDUCATION AT INSTITUTIONS OF HIGHER EDUCATION AND CAREER AND TECHNICAL INSTITUTIONS.**

The Secretary of Education, in coordination with the Secretary, and after consultation with appropriate private entities, shall—

(1) develop model curriculum standards and guidelines to address cyber safety, cybersecurity, and cyber ethics for all students enrolled in institutions of higher education, and all students enrolled in career and technical institutions, in the United States; and

(2) analyze and develop recommended courses for students interested in pursuing careers in information technology, communications, computer science, engineering, law, mathematics, and science, as those subjects relate to cybersecurity.

---

**SA 2766.** Mr. COCHRAN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 174, strike line 12 and all that follows through page 180, line 14, and insert the following:

**SEC. 703. CYBERSECURITY EXCHANGES.**

(a) DESIGNATION OF CYBERSECURITY EXCHANGES.—The Secretary of Homeland Security, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, shall establish—

(1) a process for designating one or more appropriate civilian Federal entities or non-Federal entities to serve as cybersecurity exchanges to receive and distribute cybersecurity threat indicators;

(2) procedures to facilitate and ensure the sharing of classified and unclassified cybersecurity threat indicators in as close to real time as possible with appropriate Federal entities and non-Federal entities in accordance with this title, including through automated and other means that allow for the immediate sharing of such indicators in accordance with this title; and

(3) a process for identifying certified entities to receive classified cybersecurity threat indicators in accordance with paragraph (2).

(b) PURPOSE.—The purpose of a cybersecurity exchange is to receive and distribute, in as close to real time as possible, cybersecurity threat indicators in accordance with the requirements of this title and the procedures established under subsection (a)(2), and to thereby avoid unnecessary and duplicative Federal bureaucracy for information sharing as provided in this title.

(c) REQUIREMENT FOR A LEAD FEDERAL CIVILIAN CYBERSECURITY EXCHANGE.—

(1) IN GENERAL.—The Secretary, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, shall designate a civilian Federal entity as the lead cybersecurity exchange to serve as a focal point within the Federal Government for cybersecurity information sharing among Federal entities and with non-Federal entities.

(2) RESPONSIBILITIES.—The lead Federal civilian cybersecurity exchange designated under paragraph (1) shall—

(A) receive and distribute, in as close to real time as possible, cybersecurity threat indicators in accordance with this title and the procedures established under subsection (a)(2);

(B) facilitate information sharing, interaction, and collaboration among and between—

(i) Federal entities;

(ii) State, local, tribal, and territorial governments;

(iii) private entities;

(iv) academia;

(v) international partners, in consultation with the Secretary of State; and

(vi) other cybersecurity exchanges;

(C) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information lawfully obtained from any source, including alerts, advisories, indicators, signatures, and mitigation and response measures, to appropriate Federal and non-Federal entities in accordance with this title and the procedures established under subsection (a)(2) in as close to real time as possible to improve the security and protection of information systems;

(D) coordinate with other Federal and non-Federal entities, as appropriate, to integrate information from Federal and non-Federal entities, including Federal cybersecurity centers, non-Federal network or security operation centers, other cybersecurity exchanges, and non-Federal entities that disclose cybersecurity threat indicators under section 704(a), in accordance with this title and the procedures established under subsection (a)(2) in as close to real time as possible, to provide situational awareness of the United States information security posture and foster information security collaboration among information system owners and operators;

(E) conduct, in consultation with private entities and relevant Federal and other governmental entities, regular assessments of existing and proposed information sharing models to eliminate bureaucratic obstacles to information sharing and identify best practices for such sharing; and

(F) coordinate with other Federal entities, as appropriate, to compile and analyze information about risks and incidents that threaten information systems, including information voluntarily submitted in accordance with section 704(a) or otherwise in accordance with applicable laws.

(3) SCHEDULE FOR DESIGNATION.—The designation of a lead Federal civilian cybersecurity exchange under paragraph (1) shall be made concurrently with the issuance of the interim policies and procedures under section 704(g)(3)(D).

(d) ADDITIONAL CIVILIAN FEDERAL CYBERSECURITY EXCHANGES.—In accordance with the process and procedures established in subsection (a), the Secretary, in consultation with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, may designate additional civilian Federal entities to receive and distribute cybersecurity threat indicators, if such entities are subject to the requirements for use, retention, and disclosure of information by a cybersecurity exchange under section 704(b) and the special requirements for Federal entities under section 704(g).

(e) REQUIREMENTS FOR NON-FEDERAL CYBERSECURITY EXCHANGES.—

(1) IN GENERAL.—In considering whether to designate a private entity or any other non-Federal entity as a cybersecurity exchange to receive and distribute cybersecurity threat indicators under section 704, and what entity to designate, the Secretary shall consider the following factors:

(A) The net effect that such designation would have on the overall cybersecurity of the United States.

(B) Whether such designation could substantially improve such overall cybersecurity by serving as a hub for receiving and sharing cybersecurity threat indicators in as close to real time as possible, including the capacity of the non-Federal entity for performing those functions in accordance with this title and the procedures established under subsection (a)(2).

(C) The capacity of such non-Federal entity to safeguard cybersecurity threat indicators from unauthorized disclosure and use.

(D) The adequacy of the policies and procedures of such non-Federal entity to protect personally identifiable information from unauthorized disclosure and use.

(E) The ability of the non-Federal entity to sustain operations using entirely non-Federal sources of funding.

(2) REGULATIONS.—The Secretary may promulgate regulations as may be necessary to carry out this subsection.

(f) CONSTRUCTION WITH OTHER AUTHORITIES.—Nothing in this section may be construed to alter the authorities of a Federal cybersecurity center, unless such cybersecurity center is acting in its capacity as a designated cybersecurity exchange.

(g) CONGRESSIONAL NOTIFICATION OF DESIGNATION OF CYBERSECURITY EXCHANGES.—

(1) IN GENERAL.—The Secretary, in coordination with the Director of National Intelligence, the Attorney General, and the Secretary of Defense, shall promptly notify Congress, in writing, of any designation of a cybersecurity exchange under this title.

(2) REQUIREMENT.—Written notification under paragraph (1) shall include a description of the criteria and processes used to make the designation.

---

**SA 2767.** Mr. COCHRAN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 117, strike line 14 and all that follows to page 119, line 2 and insert the following:

(a) ESTABLISHMENT.—Not later than 1 year after the date of enactment of this Act, the Director of the National Science Foundation, in coordination with the Secretary, shall establish cybersecurity research centers based at institutions of higher education and other entities that meet the criteria described in subsection (b) to develop solutions and strategies that support the efforts of the Federal Government under this Act in—

(1) improving the security and resilience of information infrastructure;

(2) reducing cyber vulnerabilities;

(3) mitigating the consequences of cyber attacks on critical infrastructure;

(4) developing awareness training strategies for owners and operators of critical infrastructure; and

(5) diversifying cybersecurity research and education.

(b) CRITERIA FOR SELECTION.—In selecting an institution of higher education or other entity to serve as a Research Center for Cybersecurity, the Director of the National Science Foundation shall consider—

(1) demonstrated expertise in systems security, wireless security, networking and protocols, formal methods and high-performance computing, nanotechnology, and industrial control systems;

(2) demonstrated capability to conduct high performance computation integral to complex cybersecurity research, whether through on-site or off-site computing;

(3) demonstrated expertise in interdisciplinary cybersecurity research;

(4) affiliation with private sector entities involved with industrial research described in paragraph (1) and ready access to testable commercial data;

(5) prior formal research collaboration arrangements with institutions of higher education and Federal research laboratories;

(6) capability to conduct research in a secure environment; and

(7) affiliation with existing research programs of the Federal Government, including designation as a National Center of Academic Excellence by the National Security Agency.

(c) REQUIREMENTS.—The research centers established under subsection (a) shall include centers led by institutions of higher education that are eligible institutions, as defined in section 371(a) of the Higher Education Act of 1965 (20 U.S.C. 1067q(a)) that—

(1) have accredited engineering and law schools

(2) are classified by the Carnegie Foundation as research universities with high research activity; and

(3) have been designated as a center of excellence or model institute of excellence by a Federal agency.

(d) ADVISORY BOARD.—

(1) IN GENERAL.—The Secretary of Homeland Security shall establish a cybersecurity research advisory board, which shall meet regularly with the Director of the National Science Foundation, the Department of

Homeland Security Under Secretary for Science and Technology, and the Department of Homeland Security Under Secretary for the National Protection and Programs Directorate to review the activities of the research centers established under subsection (a).

(2) MEMBERSHIPS.—In establishing the advisory board under subsection (d), the Secretary of Homeland Security shall ensure that the members of the advisory board are—

(A) from institutions of higher education with the expertise in the protection of critical infrastructure against cyber attacks;

(B) from institutions described in subsection (c); and

(C) equally representative of the 10 Federal regions that comprise the Standard Federal Regions established by the Office of Management and Budget in the document entitled ''Standard Federal Regions'' and dated April 1974 (circular A-105).

---

**SA 2768.** Mr. COCHRAN submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

**SEC. ___. FEDERAL CYBERSECURITY SCHOLARSHIP FOR SERVICE PROGRAM.**

(a) DEFINITION.—In this section, the term ''veteran'' has the meaning given that term under section 101 of title 38, United States Code.

(b) ESTABLISHMENT OF PROGRAM.—Not later than 180 days after the date of enactment of this Act, the Director of the Office of Personnel Management, in coordination with the National Initiative for Cybersecurity Education of the National Institute of Standards and Technology and the Director of the National Science Foundation, shall establish a program within the Federal Cyber Service Scholarship for Service to provide education and training in the area of cybersecurity to veterans (in this section referred to as the ''program'').

(c) ELIGIBLE STUDENTS.—To be eligible under the program, an applicant shall—

(1) be a veteran; and

(2) pursue a baccalaureate, master's, or doctorate degree in a program of study relevant to cybersecurity.

(d) PRIORITY FOR DISABLED VETERANS.—Priority for eligibility under the program shall be given to veterans who are disabled.

(e) ELIGIBLE INSTITUTIONS.—In developing the program, the Director of the Office of Personnel Management, in coordination with the Director of the National Institute of Standards and Technology, shall designate multiple institutions participating in the Federal Cyber Service Scholarship for Service program on the date of enactment of this Act as Centers of Academic Excellence in Veteran Cyber Security Education, which shall be participating institutions for purposes of the program.

(f) BENEFITS.—Subject to the availability of appropriations, the Director of the National Science Foundation shall provide scholarship benefits to eligible students for attendance at an institution designated under subsection (e).

(g) DIRECT HIRING AUTHORITY.—The Director of the Office of Personnel Management shall establish direct hiring authority, which shall not be limited to a specific job code or grade, for relevant Federal agencies desiring to hire graduates of the program.

---

**SA 2769.** Mr. LEAHY submitted an amendment intended to be proposed to amendment SA 2579 submitted by Mr. LEAHY and intended to be proposed to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

On page 11, strike lines 1 through 10.

---

**SA 2770.** Mr. REID (for Mr. CARPER (for himself, Ms. COLLINS, Mr. BROWN of Massachusetts, and Mr. COBURN)) proposed an amendment to the bill S. 1409, to intensify efforts to identify, prevent, and recover payment error, waste, fraud, and abuse within Federal spending.

In lieu of the matter proposed to be inserted, insert the following:

**SECTION 1. SHORT TITLE.**

This Act may be cited as the ''Improper Payments Elimination and Recovery Improvement Act of 2012''.

**SEC. 2. DEFINITIONS.**

In this Act—

(1) the term ''agency'' means an executive agency as that term is defined under section 102 of title 31, United States Code; and

(2) the term ''improper payment'' has the meaning given that term in section 2(g) of the Improper Payments Information Act of 2002 (31 U.S.C. 3321 note), as redesignated by section 3(a)(1) of this Act.

**SEC. 3. IMPROVING THE DETERMINATION OF IMPROPER PAYMENTS BY FEDERAL AGENCIES.**

(a) IN GENERAL.—Section 2 of the Improper Payments Information Act of 2002 (31 U.S.C. 3321 note) is amended—

(1) by redesignating subsections (b) through (g) as subsections (c) through (h), respectively;

(2) by inserting after subsection (a) the following:

''(b) IMPROVING THE DETERMINATION OF IMPROPER PAYMENTS.—

''(1) IN GENERAL.—The Director of the Office of Management and Budget shall on an annual basis—

''(A) identify a list of high-priority Federal programs for greater levels of oversight and review—

''(i) in which the highest dollar value or highest rate of improper payments occur; or

''(ii) for which there is a higher risk of improper payments; and

''(B) in coordination with the agency responsible for administering the high-priority program, establish annual targets and semi-annual or quarterly actions for reducing improper payments associated with each high-priority program.

''(2) REPORT ON HIGH-PRIORITY IMPROPER PAYMENTS.—

''(A) IN GENERAL.—Subject to Federal privacy policies and to the extent permitted by law, each agency with a program identified under paragraph (1)(A) on an annual basis shall submit to the Inspector General of that agency, and make available to the public (including availability through the Internet), a report on that program.

''(B) CONTENTS.—Each report under this paragraph—

''(i) shall describe—

''(I) any action the agency—

''(aa) has taken or plans to take to recover improper payments; and

''(bb) intends to take to prevent future improper payments; and

''(ii) shall not include any referrals the agency made or anticipates making to the Department of Justice, or any information provided in connection with such referrals.

''(C) PUBLIC AVAILABILITY ON CENTRAL WEBSITE.—The Office of Management and Budget shall make each report submitted under this paragraph available on a central website.

''(D) AVAILABILITY OF INFORMATION TO INSPECTOR GENERAL.—Subparagraph (B)(ii) shall not prohibit any referral or information being made available to an Inspector General as otherwise provided by law.

''(E) ASSESSMENT AND RECOMMENDATIONS.—The Inspector General of each agency that submits a report under this paragraph shall, for each program of the agency that is identified under paragraph (1)(A)—

''(i) review—

''(I) the assessment of the level of risk associated with the program, and the quality of the improper payment estimates and methodology of the agency relating to the program; and

''(II) the oversight or financial controls to identify and prevent improper payments under the program; and

''(ii) submit to Congress recommendations, which may be included in another report submitted by the Inspector General to Congress, for modifying any plans of the agency relating to the program, including improvements for improper payments determination and estimation methodology.'';

(3) in subsection (d) (as redesignated by paragraph (1) of this subsection), by striking ''subsection (b)'' each place that term appears and inserting ''subsection (c)'';

(4) in subsection (e) (as redesignated by paragraph (1) of this subsection), by striking ''subsection (b)'' and inserting ''subsection (c)''; and

(5) in subsection (g)(3) (as redesignated by paragraph (1) of this subsection), by inserting ''or a Federal employee'' after ''non-Federal person or entity''.

(b) IMPROVED ESTIMATES.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Director of the Office of Management and Budget shall provide guidance to agencies for improving the estimates of improper payments under the Improper Payments Information Act of 2002 (31 U.S.C. 3321 note).

(2) GUIDANCE.—Guidance under this subsection shall—

(A) strengthen the estimation process of agencies by setting standards for agencies to follow in determining the underlying validity of sampled payments to ensure amounts being billed are proper; and

(B) instruct agencies to give the persons or entities performing improper payments estimates access to all necessary payment data, including access to relevant documentation;

(C) explicitly bar agencies from relying on self-reporting by the recipients of agency payments as the sole source basis for improper payments estimates;

(D) require agencies to include all identified improper payments in the reported estimate, regardless of whether the improper payment in question has been or is being recovered;

(E) include payments to employees, including salary, locality pay, travel pay, purchase card use, and other employee payments, as subject to risk assessment and, where appropriate, improper payment estimation; and

(F) require agencies to tailor their corrective actions for the high-priority programs identified under section 2(b)(1)(A) of the Improper Payments Information Act of 2002 (31 U.S.C. 3321 note) to better reflect the unique processes, procedures, and risks involved in each specific program.

(c) TECHNICAL AND CONFORMING AMENDMENTS.—The Improper Payments Elimination and Recovery Act of 2010 (Public Law 111–204; 124 Stat. 2224) is amended—

(1) in section 2(h)(1) (31 U.S.C. 3321 note), by striking ''section 2(f)'' and all that follows and inserting ''section 2(g) of the Improper Payments Information Act of 2002 (31 U.S.C. 3321 note).''; and

(2) in section 3(a) (31 U.S.C. 3321 note)—

(A) in paragraph (1), by striking ''section 2(f)'' and all that follows and inserting ''section 2(g) of the Improper Payments Information Act of 2002 (31 U.S.C. 3321 note).''; and

(B) in paragraph (3)—

(i) by striking ''section 2(b)'' each place it appears and inserting ''section 2(c)''; and

(ii) by striking ''section 2(c)'' each place it appears and inserting ''section 2(d)''.

**SEC. 4. IMPROPER PAYMENTS INFORMATION.**

Section 2(a)(3)(A)(ii) of the Improper Payments Information Act of 2002 (31 U.S.C. 3321 note) is amended by striking ''with respect to fiscal years following September 30th of a fiscal year beginning before fiscal year 2013 as determined by the Office of Management and Budget'' and inserting ''with respect to fiscal year 2014 and each fiscal year thereafter''.

**SEC. 5. DO NOT PAY INITIATIVE.**

(a) PREPAYMENT AND PREAWARD PROCEDURES.—

(1) IN GENERAL.—Each agency shall review prepayment and preaward procedures and ensure that a thorough review of available databases with relevant information on eligibility occurs to determine program or award eligibility and prevent improper payments before the release of any Federal funds.

(2) DATABASES.—At a minimum and before issuing any payment and award, each agency shall review as appropriate the following databases to verify eligibility of the payment and award:

(A) The Death Master File of the Social Security Administration.

(B) The General Services Administration's Excluded Parties List System.

(C) The Debt Check Database of the Department of the Treasury.

(D) The Credit Alert System or Credit Alert Interactive Voice Response System of the Department of Housing and Urban Development.

(E) The List of Excluded Individuals/Entities of the Office of Inspector General of the Department of Health and Human Services.

(b) DO NOT PAY INITIATIVE.—

(1) ESTABLISHMENT.—There is established the Do Not Pay Initiative which shall include—

(A) use of the databases described under subsection (a)(2); and

(B) use of other databases designated by the Director of the Office of Management and Budget in consultation with agencies and in accordance with paragraph (2).

(2) OTHER DATABASES.—In making designations of other databases under paragraph (1)(B), the Director of the Office of Management and Budget shall—

(A) consider any database that substantially assists in preventing improper payments; and

(B) provide public notice and an opportunity for comment before designating a database under paragraph (1)(B).

(3) ACCESS AND REVIEW BY AGENCIES.—For purposes of identifying and preventing improper payments, each agency shall have access to, and use of, the Do Not Pay Initiative to verify payment or award eligibility in accordance with subsection (a) when the Director of the Office of Management and Budget determines the Do Not Pay Initiative is appropriately established for the agency.

(4) PAYMENT OTHERWISE REQUIRED.—When using the Do Not Pay Initiative, an agency shall recognize that there may be circumstances under which the law requires a payment or award to be made to a recipient, regardless of whether that recipient is identified as potentially ineligible under the Do Not Pay Initiative.

(5) ANNUAL REPORT.—The Director of the Office of Management and Budget shall submit to Congress an annual report, which may be included as part of another report submitted to Congress by the Director, regarding the operation of the Do Not Pay Initiative, which shall—

(A) include an evaluation of whether the Do Not Pay Initiative has reduced improper payments or improper awards; and

(B) provide the frequency of corrections or identification of incorrect information.

(c) DATABASE INTEGRATION PLAN.—Not later than 60 days after the date of enactment of this Act, the Director of the Office of Management and Budget shall provide to the Congress a plan for—

(1) inclusion of other databases on the Do Not Pay Initiative;

(2) to the extent permitted by law, agency access to the Do Not Pay Initiative; and

(3) the multilateral data use agreements described under subsection (e).

(d) INITIAL WORKING SYSTEM.—

(1) ESTABLISHMENT.—Not later than 90 days after the date of enactment of this Act, the Director of the Office of Management and Budget shall establish a working system for prepayment and preaward review that includes the Do Not Pay Initiative as described under this section.

(2) WORKING SYSTEM.—The working system established under paragraph (1)—

(A) may be located within an appropriate agency;

(B) shall include not less than 3 agencies as users of the system; and

(C) shall include investigation activities for fraud and systemic improper payments detection through analytic technologies and other techniques, which may include commercial database use or access.

(3) APPLICATION TO ALL AGENCIES.—Not later than June 1, 2013, each agency shall review all payments and awards for all programs of that agency through the system established under this subsection.

(e) FACILITATING DATA ACCESS BY FEDERAL AGENCIES AND OFFICES OF INSPECTORS GENERAL FOR PURPOSES OF PROGRAM INTEGRITY.—

(1) DEFINITION.—In this subsection, the term ''Inspector General'' means an Inspector General described in subparagraph (A), (B), or (I) of section 11(b)(1) of the Inspector General Act of 1978 (5 U.S.C. App.).

(2) COMPUTER MATCHING BY FEDERAL AGENCIES FOR PURPOSES OF INVESTIGATION AND PREVENTION OF IMPROPER PAYMENTS AND FRAUD.—

(A) IN GENERAL.—Except as provided in this paragraph, in accordance with section 552a of title 5, United States Code (commonly known as the Privacy Act of 1974), each Inspector General and the head of each agency may enter into computer matching agreements that allow ongoing data matching (which shall include automated data matching) in order to assist in the detection and prevention of improper payments.

(B) REVIEW.—Not later than 60 days after a proposal for an agreement under subparagraph (A) has been presented to a Data Integrity Board established under section 552a(u) of title 5, United States Code, for consideration, the Data Integrity Board shall respond to the proposal.

(C) TERMINATION DATE.—An agreement under subparagraph (A)—

(i) shall have a termination date of less than 3 years; and

(ii) during the 3-month period ending on the date on which the agreement is scheduled to terminate, may be renewed by the agencies entering the agreement for not more than 3 years.

(D) MULTIPLE AGENCIES.—For purposes of this paragraph, section 552a(o)(1) of title 5, United States Code, shall be applied by substituting ''between the source agency and the recipient agency or non-Federal agency or an agreement governing multiple agencies'' for ''between the source agency and the recipient agency or non-Federal agency'' in the matter preceding subparagraph (A).

(E) COST-BENEFIT ANALYSIS.—A justification under section 552a(o)(1)(B) of title 5, United States Code, relating to an agreement under subparagraph (A) is not required to contain a specific estimate of any savings under the computer matching agreement.

(F) GUIDANCE BY THE OFFICE OF MANAGEMENT AND BUDGET.—Not later than 6 months after the date of enactment of this Act, and in consultation with the Council of Inspectors General on Integrity and Efficiency, the Secretary of Health and Human Services, the Commissioner of Social Security, and the head of any other relevant agency, the Director of the Office of Management and Budget shall—

(i) issue guidance for agencies regarding implementing this paragraph, which shall include standards for—

(I) reimbursement of costs, when necessary, between agencies;

(II) retention and timely destruction of records in accordance with section 552a(o)(1)(F) of title 5, United States Code;

(III) prohibiting duplication and redisclosure of records in accordance with section 552a(o)(1)(H) of title 5, United States Code;

(ii) review the procedures of the Data Integrity Boards established under section 552a(u) of title 5, United States Code, and develop new guidance for the Data Integrity Boards to—

(I) improve the effectiveness and responsiveness of the Data Integrity Boards; and

(II) ensure privacy protections in accordance with section 552a of title 5, United States Code (commonly known as the Privacy Act of 1974); and

(III) establish standard matching agreements for use when appropriate; and

(iii) establish and clarify rules regarding what constitutes making an agreement entered under subparagraph (A) available upon request to the public for purposes of section 552a(o)(2)(A)(ii) of title 5, United States Code, which shall include requiring publication of the agreement on a public website.

(G) CORRECTIONS.—The Director of the Office of Management and Budget shall establish procedures providing for the correction of data in order to ensure—

(i) compliance with section 552a(p) of title 5, United States Code; and

(ii) that corrections are made in any Do Not Pay Initiative database and in any relevant source databases designated by the Director of the Office of Management and Budget under subsection (b)(1).

(H) COMPLIANCE.—The head of each agency, in consultation with the Inspector General of the agency, shall ensure that any information provided to an individual or entity under this subsection is provided in accordance with protocols established under this subsection.

(I) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to affect the rights of an individual under section 552a(p) of title 5, United States Code.

(f) DEVELOPMENT AND ACCESS TO A DATABASE OF INCARCERATED INDIVIDUALS.—Not later than 1 year after the date of enactment of this Act, the Attorney General shall submit to Congress recommendations for increasing the use of, access to, and the technical feasibility of using data on the Federal,

State, and local conviction and incarceration status of individuals for purposes of identifying and preventing improper payments by Federal agencies and programs and fraud.

(g) PLAN TO CURB FEDERAL IMPROPER PAYMENTS TO DECEASED INDIVIDUALS BY IMPROVING THE QUALITY AND USE BY FEDERAL AGENCIES OF THE SOCIAL SECURITY ADMINISTRATION DEATH MASTER FILE.—

(1) ESTABLISHMENT.—In conjunction with the Commissioner of Social Security and in consultation with relevant stakeholders that have an interest in or responsibility for providing the data, and the States, the Director of the Office of Management and Budget shall establish a plan for improving the quality, accuracy, and timeliness of death data maintained by the Social Security Administration, including death information reported to the Commissioner under section 205(r) of the Social Security Act (42 U.S.C. 405(r)).

(2) ADDITIONAL ACTIONS UNDER PLAN.—The plan established under this subsection shall include recommended actions by agencies to—

(A) increase the quality and frequency of access to the Death Master File and other death data;

(B) achieve a goal of at least daily access as appropriate;

(C) provide for all States and other data providers to use improved and electronic means for providing data;

(D) identify improved methods by agencies for determining ineligible payments due to the death of a recipient through proactive verification means; and

(E) address improper payments made by agencies to deceased individuals as part of Federal retirement programs.

(3) REPORT.—Not later than 120 days after the date of enactment of this Act, the Director of the Office of Management and Budget shall submit a report to Congress on the plan established under this subsection, including recommended legislation.

**SEC. 6. IMPROVING RECOVERY OF IMPROPER PAYMENTS.**

(a) DEFINITION.—In this section, the term ''recovery audit'' means a recovery audit described under section 2(h) of the Improper Payments Elimination and Recovery Act of 2010.

(b) REVIEW.—The Director of the Office of Management and Budget shall determine—

(1) current and historical rates and amounts of recovery of improper payments (or, in cases in which improper payments are identified solely on the basis of a sample, recovery rates and amounts estimated on the basis of the applicable sample), including a list of agency recovery audit contract programs and specific information of amounts and payments recovered by recovery audit contractors; and

(2) targets for recovering improper payments, including specific information on amounts and payments recovered by recovery audit contractors.

## NOTICES OF HEARINGS

COMMITTEE ON ENERGY AND NATURAL RESOURCES

Mr. BINGAMAN. Mr. President, I would like to announce for the information of the Senate and the public that a field hearing has been scheduled before the Senate Committee on Energy and Natural Resources. The hearing will be held on Wednesday, August 15, 2012, at 10:00 a.m., at the University of Colorado, Centennial Room 203, Colorado Springs, 1420 Austin Bluffs Pkwy, Colorado Springs, CO.

The purpose of the hearing is to discuss the recent Colorado wildfires, focusing on lessons learned that can be applied to future suppression, recovery, and mitigation efforts. The Fourmile Canyon fire report that was released on July 25 will be discussed, as will projections for future wildfire conditions and best practices that can improve forest health.

Because of the limited time available for the hearing, witnesses may testify by invitation only. However, those wishing to submit written testimony for the hearing record may do so by sending it to the Committee on Energy and Natural Resources, United States Senate, Washington, DC 20510–6150, or by e-mail to Meagan___Gins@energy.senate.gov.

For further information, please contact Kevin Rennert (202) 224–7826, Meagan Gins at (202) 224–0883, or Jacqueline Emanuel at (202) 224–5512.

COMMITTEE ON ENERGY AND NATURAL RESOURCES

Mr. BINGAMAN. Mr. President, I would like to announce for the information of the Senate and the public that a field hearing has been scheduled before the Senate Committee on Energy and Natural Resources. The hearing will be held on Friday, August 17, 2012, at 10:00 a.m., at the Santa Fe Community College, 6401 Richards Avenue, Room 216 Lecture Hall, West Wing of the Main Building, Santa Fe, NM.

The purpose of the hearing is to examine the current and future impacts of climate change on the Intermountain West, focusing on drought, wildfire frequency and severity, and ecosystems.

Because of the limited time available for the hearing, witnesses may testify by invitation only. However, those wishing to submit written testimony for the hearing record may do so by sending it to the Committee on Energy and Natural Resources, United States Senate, Washington, DC 20510–6150, or by e-mail to Meagan___Gins@energy.senate.gov.

For further information, please contact Kevin Rennert at (202) 224–7826 or Meagan Gins at (202) 224–0883.

## AUTHORITY FOR COMMITTEES TO MEET

COMMITTEE ON AGRICULTURE, NUTRITION, AND FORESTRY

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the Committee on Agriculture, Nutrition, and Forestry be authorized to meet during the session of the Senate on August 1, 2012, at 9 a.m. in room SR 328A of the Russell Senate Office Building.

The PRESIDING OFFICER. Without objection, it is so ordered.

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the Committee on Commerce, Science, and Transportation be authorized to meet during the session of the Senate on August 1, 2012, at 2:30 p.m. in room 253 of the Russell Senate Office Building.

The Committee will hold a hearing entitled, ''Marketplace Fairness: Leveling the Playing Field for Small Business.''

The PRESIDING OFFICER. Without objection, it is so ordered.

COMMITTEE ON ENVIRONMENT AND PUBLIC WORKS

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the Committee on Environment and Public Works be authorized to meet during the session of the Senate on August 1, 2012, at 10 a.m. in Dirksen 406 to conduct a hearing entitled, ''Update on the Latest Climate Change Science and Local Adaptation Measures.''

The PRESIDING OFFICER. Without objection, it is so ordered.

COMMITTEE ON FINANCE

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the Committee on Finance be authorized to meet during the session of the Senate on August 1, 2012, at 10:30 a.m. in room 215 of the Dirksen Senate Office Building, to conduct a hearing entitled ''Tax Reform: Examining the Taxation of Business Entities.''

The PRESIDING OFFICER. Without objection, it is so ordered.

COMMITTEE ON FOREIGN RELATIONS

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the Committee on Foreign Relations be authorized to meet during the session of the Senate on August 1, 2012, at 10 a.m. to hold a hearing entitled ''Next Steps in Syria.''

The PRESIDING OFFICER. Without objection, it is so ordered.

COMMITTEE ON THE JUDICIARY

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the Committee on the Judiciary be authorized to meet during the session of the Senate, on August 1, 2012, at 10 a.m., in room SD–226 of the Dirksen Senate Office Building, to conduct a hearing entitled ''Rising Prison Costs: Restricting Budgets and Crime Prevention Options.''

The PRESIDING OFFICER. Without objection, it is so ordered.

SUBCOMMITTEE ON EUROPEAN AFFAIRS

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the Committee on Foreign Relations be authorized to meet during the session of the Senate on August 1, 2012, at 2:30 p.m., to hold a European Affairs subcommittee hearing entitled, ''The Future of the Eurozone: Outlook and Lessons.''

The PRESIDING OFFICER. Without objection, it is so ordered.

SUBCOMMITTEE ON HOUSING, TRANSPORTATION, AND COMMUNITY DEVELOPMENT

Mr. LIEBERMAN. Mr. President, I ask unanimous consent that the Committee on Banking, Housing, and Urban Affairs Subcommittee on Housing, Transportation, and Community Development be authorized to meet during the session of the Senate on August 1, 2012, at 10 a.m., to conduct a