SA 2714. Mr. BARRASSO submitted an amendment intended to be proposed by him to the bill S. 209, to amend the Indian Tribal Energy Development and Self-Determination Act of 2005, and for other purposes; which was ordered to lie on the table.

SA 2715. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table.

SA 2716. Mr. BURR (for himself and Mrs. FEINSTEIN) proposed an amendment to the bill S. 754, supra.

SA 2717. Mr. UDALL (for himself, Mrs. SHAHEEN, Mr. TESTER, and Mr. MERKLEY) submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2718. Mr. UDALL (for himself, Mrs. SHAHEEN, Mr. TESTER, and Mr. MERKLEY) submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

SA 2719. Mr. ALEXANDER submitted an amendment intended to be proposed by him to the bill S. 754, supra; which was ordered to lie on the table.

TEXT OF AMENDMENTS

SA 2713. Mr. WHITEHOUSE (for himself and Mr. GRAHAM) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

SEC. ___. STOPPING THE SALE OF AMERICANS' FINANCIAL INFORMATION.

Section 1029(h) of title 18, United States Code, is amended by striking ''title if—'' and all that follows through ''therefrom.'' and inserting ''title if the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity organized under the laws of the United States, or any State, the District of Columbia, or other Territory of the United States.''.

SEC. ___. SHUTTING DOWN BOTNETS.

(a) AMENDMENT.—Section 1345 of title 18, United States Code, is amended—

(1) in the heading, by inserting ''**and abuse**'' after ''**fraud**'';

(2) in subsection (a)—

(A) in paragraph (1)—

(i) in subparagraph (B), by striking ''or'' at the end;

(ii) in subparagraph (C), by inserting ''or'' after the semicolon; and

(iii) by inserting after subparagraph (C) the following:

''(D) violating or about to violate section 1030(a)(5) where such conduct has caused or would cause damage (as defined in section 1030) without authorization to 100 or more protected computers (as defined in section 1030) during any 1-year period, including by—

''(i) impairing the availability or integrity of the protected computers without authorization; or

''(ii) installing or maintaining control over malicious software on the protected computers that, without authorization, has caused or would cause damage to the protected computers;''; and

(B) in paragraph (2), by inserting '', a violation described in subsection (a)(1)(D),'' before ''or a Federal''; and

(3) by adding at the end the following:

''(c) A restraining order, prohibition, or other action described in subsection (b), if issued in circumstances described in subsection (a)(1)(D), may, upon application of the Attorney General—

''(1) specify that no cause of action shall lie in any court against a person for complying with the restraining order, prohibition, or other action; and

''(2) provide that the United States shall pay to such person a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in complying with the restraining order, prohibition, or other action.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of section for chapter 63 is amended by striking the item relating to section 1345 and inserting the following:

''1345. Injunctions against fraud and abuse.''.

SEC. ___. AGGRAVATED DAMAGE TO A CRITICAL INFRASTRUCTURE COMPUTER.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

''§ 1030A. Aggravated damage to a critical infrastructure computer

''(a) OFFENSE.—It shall be unlawful, during and in relation to a felony violation of section 1030, to knowingly cause or attempt to cause damage to a critical infrastructure computer, if such damage results in (or, in the case of an attempted offense, would, if completed have resulted in) the substantial impairment—

''(1) of the operation of the critical infrastructure computer; or

''(2) of the critical infrastructure associated with such computer.

''(b) PENALTY.—Any person who violates subsection (a) shall, in addition to the term of punishment provided for the felony violation of section 1030, be fined under this title, imprisoned for not more than 20 years, or both.

''(c) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

''(1) a court shall not place any person convicted of a violation of this section on probation;

''(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony violation of section 1030;

''(3) in determining any term of imprisonment to be imposed for the felony violation of section 1030, a court shall not in any way reduce the term to be imposed for such violation to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

''(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, if such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the United States Sentencing Commission pursuant to section 994 of title 28.

''(d) DEFINITIONS.—In this section

''(1) the terms 'computer' and 'damage' have the meanings given the terms in section 1030; and

''(2) the term 'critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have catastrophic regional or national effects on public health or safety, economic security, or national security.''.

(b) TABLE OF SECTIONS.—The table of sections for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following:

''1030A. Aggravated damage to a critical infrastructure computer.''.

SEC. ___. STOPPING TRAFFICKING IN BOTNETS.

(a) IN GENERAL.—Section 1030 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (7), by adding ''or'' at the end; and

(B) by inserting after paragraph (7) the following:

''(8) intentionally traffics in the means of access to a protected computer, if—

''(A) the trafficker knows or has reason to know the protected computer has been damaged in a manner prohibited by this section; and

''(B) the promise or agreement to pay for the means of access is made by, or on behalf of, a person the trafficker knows or has reason to know intends to use the means of access to—

''(i) damage the protected computer in a manner prohibited by this section; or

''(ii) violate section 1037 or 1343;'';

(2) in subsection (c)(3)—

(A) in subparagraph (A), by striking ''(a)(4) or (a)(7)'' and inserting ''(a)(4), (a)(7), or (a)(8)''; and

(B) in subparagraph (B), by striking ''(a)(4), or (a)(7)'' and inserting ''(a)(4), (a)(7), or (a)(8)'';

(3) in subsection (e)—

(A) in paragraph (11), by striking ''and'' at the end;

(B) in paragraph (12), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(13) the term 'traffic', except as provided in subsection (a)(6), means transfer, or otherwise dispose of, to another as consideration for the receipt of, or as consideration for a promise or agreement to pay, anything of pecuniary value.''; and

(4) in subsection (g), in the first sentence, by inserting '', except for a violation of subsection (a)(8),'' after ''of this section''.

SA 2714. Mr. BARRASSO submitted an amendment intended to be proposed by him to the bill S. 209, to amend the Indian Tribal Energy Development and Self-Determination Act of 2005, and for other purposes; which was ordered to lie on the table; as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Indian Tribal Energy Development and Self-Determination Act Amendments of 2015''.

SEC. 2. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

TITLE II—MISCELLANEOUS AMENDMENTS

TITLE I—INDIAN TRIBAL ENERGY DEVELOPMENT AND SELF-DETERMINATION ACT AMENDMENTS

SEC. 101. INDIAN TRIBAL ENERGY RESOURCE DEVELOPMENT.

(a) IN GENERAL.—Section 2602(a) of the Energy Policy Act of 1992 (25 U.S.C. 3502(a)) is amended—

(1) in paragraph (2)—

(A) in subparagraph (C), by striking ''and'' after the semicolon;

(B) in subparagraph (D), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following:

''(E) consult with each applicable Indian tribe before adopting or approving a well spacing program or plan applicable to the energy resources of that Indian tribe or the members of that Indian tribe.''; and

(2) by adding at the end the following:

''(4) PLANNING.—

''(A) IN GENERAL.—In carrying out the program established by paragraph (1), the Secretary shall provide technical assistance to interested Indian tribes to develop energy plans, including—

''(i) plans for electrification;

''(ii) plans for oil and gas permitting, renewable energy permitting, energy efficiency, electricity generation, transmission planning, water planning, and other planning relating to energy issues;

''(iii) plans for the development of energy resources and to ensure the protection of natural, historic, and cultural resources; and

''(iv) any other plans that would assist an Indian tribe in the development or use of energy resources.

''(B) COOPERATION.—In establishing the program under paragraph (1), the Secretary shall work in cooperation with the Office of Indian Energy Policy and Programs of the Department of Energy.''.

(b) DEPARTMENT OF ENERGY INDIAN ENERGY EDUCATION PLANNING AND MANAGEMENT ASSISTANCE PROGRAM.—Section 2602(b)(2) of the Energy Policy Act of 1992 (25 U.S.C. 3502(b)(2)) is amended—

(1) in the matter preceding subparagraph (A), by inserting '', intertribal organization,'' after ''Indian tribe'';

(2) by redesignating subparagraphs (C) and (D) as subparagraphs (D) and (E), respectively; and

(3) by inserting after subparagraph (B) the following:

''(C) activities to increase the capacity of Indian tribes to manage energy development and energy efficiency programs;''.

(c) DEPARTMENT OF ENERGY LOAN GUARANTEE PROGRAM.—Section 2602(c) of the Energy Policy Act of 1992 (25 U.S.C. 3502(c)) is amended—

(1) in paragraph (1), by inserting ''or a tribal energy development organization'' after ''Indian tribe'';

(2) in paragraph (3)—

(A) in the matter preceding subparagraph (A), by striking ''guarantee'' and inserting ''guaranteed'';

(B) in subparagraph (A), by striking ''or'';

(C) in subparagraph (B), by striking the period at the end and inserting ''; or''; and

(D) by adding at the end the following:

''(C) a tribal energy development organization, from funds of the tribal energy development organization.''; and

(3) in paragraph (5), by striking ''The Secretary of Energy may'' and inserting ''Not later than 1 year after the date of enactment of the Indian Tribal Energy Development and Self-Determination Act Amendments of 2015, the Secretary of Energy shall''.

SEC. 102. INDIAN TRIBAL ENERGY RESOURCE REGULATION.

Section 2603(c) of the Energy Policy Act of 1992 (25 U.S.C. 3503(c)) is amended—

(1) in paragraph (1), by striking ''on the request of an Indian tribe, the Indian tribe'' and inserting ''on the request of an Indian tribe or a tribal energy development organization, the Indian tribe or tribal energy development organization''; and

(2) in paragraph (2)(B), by inserting ''or tribal energy development organization'' after ''Indian tribe''.

SEC. 103. TRIBAL ENERGY RESOURCE AGREEMENTS.

(a) AMENDMENT.—Section 2604 of the Energy Policy Act of 1992 (25 U.S.C. 3504) is amended—

(1) in subsection (a)—

(A) in paragraph (1)—

(i) in subparagraph (A), by striking ''or'' after the semicolon at the end;

(ii) in subparagraph (B)—

(I) by striking clause (i) and inserting the following:

''(i) an electric production, generation, transmission, or distribution facility (including a facility that produces electricity from renewable energy resources) located on tribal land; or''; and

(II) in clause (ii)—

(aa) by inserting '', at least a portion of which have been'' after ''energy resources'';

(bb) by inserting ''or produced from'' after ''developed on''; and

(cc) by striking ''and'' after the semicolon at the end and inserting ''or''; and

(iii) by adding at the end the following:

''(C) pooling, unitization, or communitization of the energy mineral resources of the Indian tribe located on tribal land with any other energy mineral resource (including energy mineral resources owned by the Indian tribe or an individual Indian in fee, trust, or restricted status or by any other persons or entities) if the owner, or, if appropriate, lessee, of the resources has consented or consents to the pooling, unitization, or communitization of the other resources under any lease or agreement; and''; and

(B) by striking paragraph (2) and inserting the following:

''(2) a lease or business agreement described in paragraph (1) shall not require review by, or the approval of, the Secretary under section 2103 of the Revised Statutes (25 U.S.C. 81), or any other provision of law (including regulations), if the lease or business agreement—

''(A) was executed—

''(i) in accordance with the requirements of a tribal energy resource agreement in effect under subsection (e) (including the periodic review and evaluation of the activities of the Indian tribe under the agreement, to be conducted pursuant to subparagraphs (D) and (E) of subsection (e)(2)); or

''(ii) by the Indian tribe and a tribal energy development organization for which the Indian tribe has obtained a certification pursuant to subsection (h); and

''(B) has a term that does not exceed—

''(i) 30 years; or

''(ii) in the case of a lease for the production of oil resources, gas resources, or both, 10 years and as long thereafter as oil or gas is produced in paying quantities.'';

(2) by striking subsection (b) and inserting the following:

''(b) RIGHTS-OF-WAY.—An Indian tribe may grant a right-of-way over tribal land without review or approval by the Secretary if the right-of-way—

''(1) serves—

''(A) an electric production, generation, transmission, or distribution facility (including a facility that produces electricity from renewable energy resources) located on tribal land;

''(B) a facility located on tribal land that extracts, produces, processes, or refines energy resources; or

''(C) the purposes, or facilitates in carrying out the purposes, of any lease or agreement entered into for energy resource development on tribal land;

''(2) was executed—

''(A) in accordance with the requirements of a tribal energy resource agreement in effect under subsection (e) (including the periodic review and evaluation of the activities of the Indian tribe under the agreement, to be conducted pursuant to subparagraphs (D) and (E) of subsection (e)(2)); or

''(B) by the Indian tribe and a tribal energy development organization for which the Indian tribe has obtained a certification pursuant to subsection (h); and

''(3) has a term that does not exceed 30 years.'';

(3) by striking subsection (d) and inserting the following:

''(d) VALIDITY.—No lease or business agreement entered into, or right-of-way granted, pursuant to this section shall be valid unless the lease, business agreement, or right-of-way is authorized by subsection (a) or (b).'';

(4) in subsection (e)—

(A) by striking paragraph (1) and inserting the following:

''(1) IN GENERAL.—

''(A) AUTHORIZATION.—On or after the date of enactment of the Indian Tribal Energy Development and Self-Determination Act Amendments of 2015, a qualified Indian tribe may submit to the Secretary a tribal energy resource agreement governing leases, business agreements, and rights-of-way under this section.

''(B) NOTICE OF COMPLETE PROPOSED AGREEMENT.—Not later than 60 days after the date on which the tribal energy resource agreement is submitted under subparagraph (A), the Secretary shall—

''(i) notify the Indian tribe as to whether the agreement is complete or incomplete;

''(ii) if the agreement is incomplete, notify the Indian tribe of what information or documentation is needed to complete the submission; and

''(iii) identify and notify the Indian tribe of the financial assistance, if any, to be provided by the Secretary to the Indian tribe to assist in the implementation of the tribal energy resource agreement, including the environmental review of individual projects.

''(C) EFFECT.—Nothing in this paragraph precludes the Secretary from providing any financial assistance at any time to the Indian tribe to assist in the implementation of the tribal energy resource agreement.'';

(B) in paragraph (2)—

(i) by striking ''(2)(A)'' and all that follows through the end of subparagraph (A) and inserting the following:

''(2) PROCEDURE.—

''(A) EFFECTIVE DATE.—

''(i) IN GENERAL.—On the date that is 271 days after the date on which the Secretary receives a tribal energy resource agreement from a qualified Indian tribe under paragraph (1), the tribal energy resource agreement shall take effect, unless the Secretary disapproves the tribal energy resource agreement under subparagraph (B).

''(ii) REVISED TRIBAL ENERGY RESOURCE AGREEMENT.—On the date that is 91 days after the date on which the Secretary receives a revised tribal energy resource agreement from a qualified Indian tribe under paragraph (4)(B), the revised tribal energy resource agreement shall take effect, unless the Secretary disapproves the revised tribal energy resource agreement under subparagraph (B).'';

(ii) in subparagraph (B)—

(I) by striking ''(B)'' and all that follows through clause (ii) and inserting the following:

''(B) DISAPPROVAL.—The Secretary shall disapprove a tribal energy resource agreement submitted pursuant to paragraph (1) or (4)(B) only if—

''(i) a provision of the tribal energy resource agreement violates applicable Federal law (including regulations) or a treaty applicable to the Indian tribe;

''(ii) the tribal energy resource agreement does not include 1 or more provisions required under subparagraph (D); or''; and

(II) in clause (iii)—

(aa) in the matter preceding subclause (I), by striking ''includes'' and all that follows through ''section—'' and inserting ''does not include provisions that, with respect to any lease, business agreement, or right-of-way to which the tribal energy resource agreement applies—'';

(bb) by striking subclauses (I), (II), (V), (VIII), and (XV);

(cc) by redesignating clauses (III), (IV), (VI), (VII), (IX) through (XIV), and (XVI) as clauses (I), (II), (III), (IV), (V) through (X), and (XI), respectively;

(dd) in item (bb) of subclause (XI) (as redesignated by item (cc))—

(AA) by striking ''or tribal''; and

(BB) by striking the period at the end and inserting a semicolon; and

(ee) by adding at the end the following:

''(XII) include a certification by the Indian tribe that the Indian tribe has—

''(aa) carried out a contract or compact under title I or IV of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450 et seq.) for a period of not less than 3 consecutive years ending on the date on which the Indian tribe submits the application without material audit exception (or without any material audit exceptions that were not corrected within the 3-year period) relating to the management of tribal land or natural resources; or

''(bb) substantial experience in the administration, review, or evaluation of energy resource leases or agreements or has otherwise substantially participated in the administration, management, or development of energy resources located on the tribal land of the Indian tribe; and

''(XIII) at the option of the Indian tribe, identify which functions, if any, authorizing any operational or development activities pursuant to a lease, right-of-way, or business agreement approved by the Indian tribe, that the Indian tribe intends to conduct.'';

(iii) in subparagraph (C)—

(I) by striking clauses (i) and (ii);

(II) by redesignating clauses (iii) through (v) as clauses (ii) through (iv), respectively; and

(III) by inserting before clause (ii) (as redesignated by subclause (II)) the following:

''(i) a process for ensuring that—

''(I) the public is informed of, and has reasonable opportunity to comment on, any significant environmental impacts of the proposed action; and

''(II) the Indian tribe provides responses to relevant and substantive public comments on any impacts described in subclause (I) before the Indian tribe approves the lease, business agreement, or right-of-way.'';

(iv) in subparagraph (D)(ii), by striking ''subparagraph (B)(iii)(XVI)'' and inserting ''subparagraph (B)(iv)(XI)''; and

(v) by adding at the end the following:

''(F) EFFECTIVE PERIOD.—A tribal energy resource agreement that takes effect pursuant to this subsection shall remain in effect to the extent any provision of the tribal energy resource agreement is consistent with applicable Federal law (including regulations), unless the tribal energy resource agreement is—

''(i) rescinded by the Secretary pursuant to paragraph (7)(D)(iii)(II); or

''(ii) voluntarily rescinded by the Indian tribe pursuant to the regulations promulgated under paragraph (8)(B) (or successor regulations).'';

(C) in paragraph (4), by striking ''date of disapproval'' and all that follows through the end of subparagraph (C) and inserting the following: ''date of disapproval, provide the Indian tribe with—

''(A) a detailed, written explanation of—

''(i) each reason for the disapproval; and

''(ii) the revisions or changes to the tribal energy resource agreement necessary to address each reason; and

''(B) an opportunity to revise and resubmit the tribal energy resource agreement.'';

(D) in paragraph (6)—

(i) in subparagraph (B)—

(I) by striking ''(B) Subject to'' and inserting the following:

''(B) Subject only to''; and

(II) by striking ''subparagraph (D)'' and inserting ''subparagraphs (C) and (D)'';

(ii) in subparagraph (C), in the matter preceding clause (i), by inserting ''to perform the obligations of the Secretary under this section and'' before ''to ensure''; and

(iii) in subparagraph (D), by adding at the end the following:

''(iii) Nothing in this section absolves, limits, or otherwise affects the liability, if any, of the United States for any—

''(I) term of any lease, business agreement, or right-of-way under this section that is not a negotiated term; or

''(II) losses that are not the result of a negotiated term, including losses resulting from the failure of the Secretary to perform an obligation of the Secretary under this section.'';

(E) in paragraph (7)—

(i) in subparagraph (A), by striking ''has demonstrated'' and inserting ''the Secretary determines has demonstrated with substantial evidence'';

(ii) in subparagraph (B), by striking ''any tribal remedy'' and inserting ''all remedies (if any) provided under the laws of the Indian tribe'';

(iii) in subparagraph (D)—

(I) in clause (i), by striking ''determine'' and all that follows through the end of the clause and inserting the following: ''determine—

''(I) whether the petitioner is an interested party; and

''(II) if the petitioner is an interested party, whether the Indian tribe is not in compliance with the tribal energy resource agreement as alleged in the petition.'';

(II) in clause (ii), by striking ''determination'' and inserting ''determinations''; and

(III) in clause (iii), in the matter preceding subclause (I) by striking ''agreement'' the first place it appears and all that follows through '', including'' and inserting ''agreement pursuant to clause (i), the Secretary shall only take such action as the Secretary determines necessary to address the claims of noncompliance made in the petition, including'';

(iv) in subparagraph (E)(i), by striking ''the manner in which'' and inserting '', with respect to each claim made in the petition, how''; and

(v) by adding at the end the following:

''(G) Notwithstanding any other provision of this paragraph, the Secretary shall dismiss any petition from an interested party that has agreed with the Indian tribe to a resolution of the claims presented in the petition of that party.'';

(F) in paragraph (8)—

(i) by striking subparagraph (A);

(ii) by redesignating subparagraphs (B) through (D) as subparagraphs (A) through (C), respectively; and

(iii) in subparagraph (A) (as redesignated by clause (ii))—

(I) in clause (i), by striking ''and'' at the end;

(II) in clause (ii), by adding ''and'' after the semicolon; and

(III) by adding at the end the following:

''(iii) amend an approved tribal energy resource agreement to assume authority for approving leases, business agreements, or rights-of-way for development of another energy resource that is not included in an approved tribal energy resource agreement without being required to apply for a new tribal energy resource agreement;'' and

(G) by adding at the end the following:

''(9) EFFECT.—Nothing in this section authorizes the Secretary to deny a tribal energy resource agreement or any amendment to a tribal energy resource agreement, or to limit the effect or implementation of this section, due to lack of promulgated regulations.'';

(5) by redesignating subsection (g) as subsection (j); and

(6) by inserting after subsection (f) the following:

''(g) FINANCIAL ASSISTANCE IN LIEU OF ACTIVITIES BY THE SECRETARY.—

''(1) IN GENERAL.—Any amounts that the Secretary would otherwise expend to operate or carry out any program, function, service, or activity (or any portion of a program, function, service, or activity) of the Department that, as a result of an Indian tribe carrying out activities under a tribal energy resource agreement, the Secretary does not expend, the Secretary shall, at the request of the Indian tribe, make available to the Indian tribe in accordance with this subsection.

''(2) ANNUAL FUNDING AGREEMENTS.—The Secretary shall make the amounts described in paragraph (1) available to an Indian tribe through an annual written funding agreement that is negotiated and entered into with the Indian tribe that is separate from the tribal energy resource agreement.

''(3) EFFECT OF APPROPRIATIONS.—Notwithstanding paragraph (1)—

''(A) the provision of amounts to an Indian tribe under this subsection is subject to the availability of appropriations; and

''(B) the Secretary shall not be required to reduce amounts for programs, functions, services, or activities that serve any other Indian tribe to make amounts available to an Indian tribe under this subsection.

''(4) DETERMINATION.—

''(A) IN GENERAL.—The Secretary shall calculate the amounts under paragraph (1) in accordance with the regulations adopted under section 103(b) of the Indian Tribal Energy Development and Self-Determination Act Amendments of 2015.

''(B) APPLICABILITY.—The effective date or implementation of a tribal energy resource agreement under this section shall not be delayed or otherwise affected by—

''(i) a delay in the promulgation of regulations under section 103(b) of the Indian Tribal Energy Development and Self-Determination Act Amendments of 2015;

''(ii) the period of time needed by the Secretary to make the calculation required under paragraph (1); or

''(iii) the adoption of a funding agreement under paragraph (2).

''(h) CERTIFICATION OF TRIBAL ENERGY DEVELOPMENT ORGANIZATION.—

''(1) IN GENERAL.—Not later than 90 days after the date on which an Indian tribe submits an application for certification of a tribal energy development organization in accordance with regulations promulgated under section 103(b) of the Indian Tribal Energy Development and Self-Determination Act Amendments of 2015, the Secretary shall approve or disapprove the application.

''(2) REQUIREMENTS.—The Secretary shall approve an application for certification if—

''(A)(i) the Indian tribe has carried out a contract or compact under title I or IV of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450 et seq.); and

''(ii) for a period of not less than 3 consecutive years ending on the date on which the Indian tribe submits the application, the contract or compact—

''(I) has been carried out by the Indian tribe without material audit exceptions (or without any material audit exceptions that were not corrected within the 3-year period); and

''(II) has included programs or activities relating to the management of tribal land; and

''(B)(i) the tribal energy development organization is organized under the laws of the Indian tribe;

''(ii)(I) the majority of the interest in the tribal energy development organization is owned and controlled by the Indian tribe (or the Indian tribe and 1 or more other Indian tribes) the tribal land of which is being developed; and

''(II) the organizing document of the tribal energy development organization requires that the Indian tribe with jurisdiction over the land maintain at all times the controlling interest in the tribal energy development organization;

''(iii) the organizing document of the tribal energy development organization requires that the Indian tribe (or the Indian tribe and 1 or more other Indian tribes) the tribal land of which is being developed own and control at all times a majority of the interest in the tribal energy development organization; and

''(iv) the organizing document of the tribal energy development organization includes a statement that the organization shall be subject to the jurisdiction, laws, and authority of the Indian tribe.

''(3) ACTION BY SECRETARY.—If the Secretary approves an application for certification pursuant to paragraph (2), the Secretary shall, not more than 10 days after making the determination—

''(A) issue a certification stating that—

''(i) the tribal energy development organization is organized under the laws of the Indian tribe and subject to the jurisdiction, laws, and authority of the Indian tribe;

''(ii) the majority of the interest in the tribal energy development organization is owned and controlled by the Indian tribe (or the Indian tribe and 1 or more other Indian tribes) the tribal land of which is being developed;

''(iii) the organizing document of the tribal energy development organization requires that the Indian tribe with jurisdiction over the land maintain at all times the controlling interest in the tribal energy development organization;

''(iv) the organizing document of the tribal energy development organization requires that the Indian tribe (or the Indian tribe and 1 or more other Indian tribes the tribal land of which is being developed) own and control at all times a majority of the interest in the tribal energy development organization; and

''(v) the certification is issued pursuant to this subsection;

''(B) deliver a copy of the certification to the Indian tribe; and

''(C) publish the certification in the Federal Register.

''(i) SOVEREIGN IMMUNITY.—Nothing in this section waives the sovereign immunity of an Indian tribe.''.

(b) REGULATIONS.—Not later than 1 year after the date of enactment of the Indian Tribal Energy Development and Self-Determination Act Amendments of 2015, the Secretary shall promulgate or update any regulations that are necessary to implement this section, including provisions to implement—

(1) section 2604(e)(8) of the Energy Policy Act of 1992 (25 U.S.C. 3504(e)(8)), including the process to be followed by an Indian tribe amending an existing tribal energy resource agreement to assume authority for approving leases, business agreements, or rights-of-way for development of an energy resource that is not included in the tribal energy resource agreement;

(2) section 2604(g) of the Energy Policy Act of 1992 (25 U.S.C. 3504(g)) including the manner in which the Secretary, at the request of an Indian tribe, shall—

(A) identify the programs, functions, services, and activities (or any portions of programs, functions, services, or activities) that the Secretary will not have to operate or carry out as a result of the Indian tribe carrying out activities under a tribal energy resource agreement;

(B) identify the amounts that the Secretary would have otherwise expended to operate or carry out each program, function, service, and activity (or any portion of a program, function, service, or activity) identified pursuant to subparagraph (A); and

(C) provide to the Indian tribe a list of the programs, functions, services, and activities (or any portions of programs, functions, services, or activities) identified pursuant subparagraph (A) and the amounts associated with each program, function, service, and activity (or any portion of a program, function, service, or activity) identified pursuant to subparagraph (B); and

(3) section 2604(h) of the Energy Policy Act of 1992 (25 U.S.C. 3504(h)), including the process to be followed by, and any applicable criteria and documentation required for, an Indian tribe to request and obtain the certification described in that section.

SEC. 104. TECHNICAL ASSISTANCE FOR INDIAN TRIBAL GOVERNMENTS.

Section 2602(b) of the Energy Policy Act of 1992 (25 U.S.C. 3502(b)) is amended—

(1) by redesignating paragraphs (3) through (6) as paragraphs (4) through (7), respectively; and

(2) by inserting after paragraph (2) the following:

''(3) TECHNICAL AND SCIENTIFIC RESOURCES.—In addition to providing grants to Indian tribes under this subsection, the Secretary shall collaborate with the Directors of the National Laboratories in making the full array of technical and scientific resources of the Department of Energy available for tribal energy activities and projects.''.

SEC. 105. CONFORMING AMENDMENTS.

(a) DEFINITION OF TRIBAL ENERGY DEVELOPMENT ORGANIZATION.—Section 2601 of the Energy Policy Act of 1992 (25 U.S.C. 3501) is amended—

(1) by redesignating paragraphs (9) through (12) as paragraphs (10) through (13), respectively;

(2) by inserting after paragraph (8) the following:

''(9) The term 'qualified Indian tribe' means an Indian tribe that has—

''(A) carried out a contract or compact under title I or IV of the Indian Self Determination and Education Assistance Act (25 U.S.C. 450 et seq.) for a period of not less than 3 consecutive years ending on the date on which the Indian tribe submits the application without material audit exception (or without any material audit exceptions that were not corrected within the 3-year period) relating to the management of tribal land or natural resources; or

''(B) substantial experience in the administration, review, or evaluation of energy resource leases or agreements or has otherwise substantially participated in the administration, management, or development of energy resources located on the tribal land of the Indian tribe.''; and

(3) by striking paragraph (12) (as redesignated by paragraph (1)) and inserting the following:

''(12) The term 'tribal energy development organization' means—

''(A) any enterprise, partnership, consortium, corporation, or other type of business organization that is engaged in the development of energy resources and is wholly owned by an Indian tribe (including an organization incorporated pursuant to section 17 of the Indian Reorganization Act of 1934 (25 U.S.C. 477) or section 3 of the Act of June 26, 1936 (25 U.S.C. 503) (commonly known as the 'Oklahoma Indian Welfare Act')); and

''(B) any organization of 2 or more entities, at least 1 of which is an Indian tribe, that has the written consent of the governing bodies of all Indian tribes participating in the organization to apply for a grant, loan, or other assistance under section 2602 or to enter into a lease or business agreement with, or acquire a right-of-way from, an Indian tribe pursuant to subsection (a)(2)(A)(ii) or (b)(2)(B) of section 2604.''.

(b) INDIAN TRIBAL ENERGY RESOURCE DEVELOPMENT.—Section 2602 of the Energy Policy Act of 1992 (25 U.S.C. 3502) is amended—

(1) in subsection (a)—

(A) in paragraph (1), by striking ''tribal energy resource development organizations'' and inserting ''tribal energy development organizations''; and

(B) in paragraph (2), by striking ''tribal energy resource development organizations'' each place it appears and inserting ''tribal energy development organizations''; and

(2) in subsection (b)(2), by striking ''tribal energy resource development organization'' and inserting ''tribal energy development organization''.

(c) WIND AND HYDROPOWER FEASIBILITY STUDY.—Section 2606(c)(3) of the Energy Policy Act of 1992 (25 U.S.C. 3506(c)(3)) is amended by striking ''energy resource development'' and inserting ''energy development''.

(d) CONFORMING AMENDMENTS.—Section 2604(e) of the Energy Policy Act of 1992 (25 U.S.C. 3504(e)) is amended—

(1) in paragraph (3)—

(A) by striking ''(3) The Secretary'' and inserting the following:

''(3) NOTICE AND COMMENT; SECRETARIAL REVIEW.—The Secretary''; and

(B) by striking ''for approval'';

(2) in paragraph (4), by striking ''(4) If the Secretary'' and inserting the following:

''(4) ACTION IN CASE OF DISAPPROVAL.—If the Secretary'';

(3) in paragraph (5)—

(A) by striking ''(5) If an Indian tribe'' and inserting the following:

''(5) PROVISION OF DOCUMENTS TO SECRETARY.—If an Indian tribe''; and

(B) in the matter preceding subparagraph (A), by striking ''approved'' and inserting ''in effect'';

(4) in paragraph (6)—

(A) by striking ''(6)(A) In carrying out'' and inserting the following:

''(6) SECRETARIAL OBLIGATIONS AND EFFECT OF SECTION.—

''(A) In carrying out'';

(B) in subparagraph (A), by indenting clauses (i) and (ii) appropriately;

(C) in subparagraph (B), by striking ''approved'' and inserting ''in effect''; and

(D) in subparagraph (D)—

(i) in clause (i), by striking ''an approved tribal energy resource agreement'' and inserting ''a tribal energy resource agreement in effect under this section''; and

(ii) in clause (ii), by striking ''approved by the Secretary'' and inserting ''in effect''; and

(5) in paragraph (7)—

(A) by striking ''(7)(A) In this paragraph'' and inserting the following:

''(7) PETITIONS BY INTERESTED PARTIES.—

''(A) In this paragraph'';

(B) in subparagraph (A), by striking ''approved by the Secretary'' and inserting ''in effect'';

(C) in subparagraph (B), by striking ''approved by the Secretary'' and inserting ''in effect''; and

(D) in subparagraph (D)(iii)—

(i) in subclause (I), by striking ''approved''; and

(ii) in subclause (II)—

(I) by striking ''approval of'' in the first place it appears; and

(II) by striking ''subsection (a) or (b)'' and inserting ''subsection (a)(2)(A)(i) or (b)(2)(A)''.

SEC. 106. REPORT.

(a) IN GENERAL.—Not later than 18 months after the date of enactment of this Act, the Secretary of the Interior shall submit to the Committee on Indian Affairs of the Senate and the Committee on Natural Resources of the House of Representatives a report that details with respect to activities for energy development on Indian land, how the Department of the Interior—

(1) processes and completes the reviews of energy-related documents in a timely and transparent manner;

(2) monitors the timeliness of agency review for all energy-related documents;

(3) maintains databases to track and monitor the review and approval process for energy-related documents associated with conventional and renewable Indian energy resources that require Secretarial approval prior to development, including—

(A) any seismic exploration permits;

(B) permission to survey;

(C) archeological and cultural surveys;

(D) access permits;

(E) environmental assessments;

(F) oil and gas leases;

(G) surface leases;

(H) rights-of-way agreements; and

(I) communitization agreements;

(4) identifies in the databases—

(A) the date lease applications and permits are received by the agency;

(B) the status of the review;

(C) the date the application or permit is considered complete and ready for review;

(D) the date of approval; and

(E) the start and end dates for any significant delays in the review process;

(5) tracks in the databases, for all energy-related leases, agreements, applications, and permits that involve multiple agency review—

(A) the dates documents are transferred between agencies;

(B) the status of the review;

(C) the date the required reviews are completed; and

(D) the date interim or final decisions are issued.

(b) INCLUSIONS.—The report under subsection (a) shall include—

(1) a description of any intermediate and final deadlines for agency action on any Secretarial review and approval required for Indian conventional and renewable energy exploration and development activities;

(2) a description of the existing geographic database established by the Bureau of Indian Affairs, explaining—

(A) how the database identifies—

(i) the location and ownership of all Indian oil and gas resources held in trust;

(ii) resources available for lease; and

(iii) the location of—

(I) any lease of land held in trust or restricted fee on behalf of any Indian tribe or individual Indian; and

(II) any rights-of-way on that land in effect;

(B) how the information from the database is made available to—

(i) the officials of the Bureau of Indian Affairs with responsibility over the management and development of Indian resources; and

(ii) resource owners; and

(C) any barriers to identifying the information described in subparagraphs (A) and (B) or any deficiencies in that information; and

(3) an evaluation of—

(A) the ability of each applicable agency to track and monitor the review and approval process of the agency for Indian energy development; and

(B) the extent to which each applicable agency complies with any intermediate and final deadlines.

TITLE II—MISCELLANEOUS AMENDMENTS

SEC. 201. ISSUANCE OF PRELIMINARY PERMITS OR LICENSES.

(a) IN GENERAL.—Section 7(a) of the Federal Power Act (16 U.S.C. 800(a)) is amended by striking ''States and municipalities'' and inserting ''States, Indian tribes, and municipalities''.

(b) APPLICABILITY.—The amendment made by subsection (a) shall not affect—

(1) any preliminary permit or original license issued before the date of enactment of the Indian Tribal Energy Development and Self-Determination Act Amendments of 2015; or

(2) an application for an original license, if the Commission has issued a notice accepting that application for filing pursuant to section 4.32(d) of title 18, Code of Federal Regulations (or successor regulations), before the date of enactment of the Indian Tribal Energy Development and Self-Determination Act Amendments of 2015.

(c) DEFINITION OF INDIAN TRIBE.—For purposes of section 7(a) of the Federal Power Act (16 U.S.C. 800(a)) (as amended by subsection (a)), the term ''Indian tribe'' has the meaning given the term in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

SEC. 202. TRIBAL BIOMASS DEMONSTRATION PROJECT.

(a) PURPOSE.—The purpose of this section is to establish a biomass demonstration project for federally recognized Indian tribes and Alaska Native corporations to promote biomass energy production.

(b) TRIBAL BIOMASS DEMONSTRATION PROJECT.—The Tribal Forest Protection Act of 2004 (Public Law 108–278; 118 Stat. 868) is amended—

(1) in section 2(a), by striking ''In this section'' and inserting ''In this Act''; and

(2) by adding at the end the following:

''SEC. 3. TRIBAL BIOMASS DEMONSTRATION PROJECT.

''(a) STEWARDSHIP CONTRACTS OR SIMILAR AGREEMENTS.—For each of fiscal years 2016 through 2020, the Secretary shall enter into stewardship contracts or similar agreements (excluding direct service contracts) with Indian tribes to carry out demonstration projects to promote biomass energy production (including biofuel, heat, and electricity generation) on Indian forest land and in nearby communities by providing reliable supplies of woody biomass from Federal land.

''(b) DEMONSTRATION PROJECTS.—In each fiscal year for which projects are authorized, at least 4 new demonstration projects that meet the eligibility criteria described in subsection (c) shall be carried out under contracts or agreements described in subsection (a).

''(c) ELIGIBILITY CRITERIA.—To be eligible to enter into a contract or agreement under this section, an Indian tribe shall submit to the Secretary an application—

''(1) containing such information as the Secretary may require; and

''(2) that includes a description of—

''(A) the Indian forest land or rangeland under the jurisdiction of the Indian tribe; and

''(B) the demonstration project proposed to be carried out by the Indian tribe.

''(d) SELECTION.—In evaluating the applications submitted under subsection (c), the Secretary shall—

''(1) take into consideration—

''(A) the factors set forth in paragraphs (1) and (2) of section 2(e); and

''(B) whether a proposed project would—

''(i) increase the availability or reliability of local or regional energy;

''(ii) enhance the economic development of the Indian tribe;

''(iii) result in or improve the connection of electric power transmission facilities serving the Indian tribe with other electric transmission facilities;

''(iv) improve the forest health or watersheds of Federal land or Indian forest land or rangeland;

''(v) demonstrate new investments in infrastructure; or

''(vi) otherwise promote the use of woody biomass; and

''(2) exclude from consideration any merchantable logs that have been identified by the Secretary for commercial sale.

''(e) IMPLEMENTATION.—The Secretary shall—

''(1) ensure that the criteria described in subsection (c) are publicly available by not later than 120 days after the date of enactment of this section; and

''(2) to the maximum extent practicable, consult with Indian tribes and appropriate intertribal organizations likely to be affected in developing the application and otherwise carrying out this section.

''(f) REPORT.—Not later than September 20, 2018, the Secretary shall submit to Congress a report that describes, with respect to the reporting period—

''(1) each individual tribal application received under this section; and

''(2) each contract and agreement entered into pursuant to this section.

''(g) INCORPORATION OF MANAGEMENT PLANS.—In carrying out a contract or agreement under this section, on receipt of a request from an Indian tribe, the Secretary shall incorporate into the contract or agreement, to the maximum extent practicable, management plans (including forest management and integrated resource management plans) in effect on the Indian forest land or rangeland of the respective Indian tribe.

''(h) TERM.—A contract or agreement entered into under this section—

''(1) shall be for a term of not more than 20 years; and

''(2) may be renewed in accordance with this section for not more than an additional 10 years.''.

(c) ALASKA NATIVE BIOMASS DEMONSTRATION PROJECT.—

(1) DEFINITIONS.—In this subsection:

(A) FEDERAL LAND.—The term ''Federal land'' means—

(i) land of the National Forest System (as defined in section 11(a) of the Forest and Rangeland Renewable Resources Planning Act of 1974 (16 U.S.C. 1609(a)) administered by the Secretary of Agriculture, acting through the Chief of the Forest Service; and

(ii) public lands (as defined in section 103 of the Federal Land Policy Management Act of 1976 (43 U.S.C. 1702)), the surface of which is administered by the Secretary of the Interior, acting through the Director of the Bureau of Land Management.

(B) INDIAN TRIBE.—The term ''Indian tribe'' has the meaning given the term in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

(C) SECRETARY.—The term ''Secretary'' means—

(i) the Secretary of Agriculture, with respect to land under the jurisdiction of the Forest Service; and

(ii) the Secretary of the Interior, with respect to land under the jurisdiction of the Bureau of Land Management.

(D) TRIBAL ORGANIZATION.—The term ''tribal organization'' has the meaning given the term in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

(2) AGREEMENTS.—For each of fiscal years 2016 through 2020, the Secretary shall enter into an agreement or contract with an Indian tribe or a tribal organization to carry out a demonstration project to promote biomass energy production (including biofuel, heat, and electricity generation) by providing reliable supplies of woody biomass from Federal land.

(3) DEMONSTRATION PROJECTS.—In each fiscal year for which projects are authorized, at least 1 new demonstration project that meets the eligibility criteria described in paragraph (4) shall be carried out under contracts or agreements described in paragraph (2).

(4) ELIGIBILITY CRITERIA.—To be eligible to enter into a contract or agreement under this subsection, an Indian tribe or tribal organization shall submit to the Secretary an application—

(A) containing such information as the Secretary may require; and

(B) that includes a description of the demonstration project proposed to be carried out by the Indian tribe or tribal organization.

(5) SELECTION.—In evaluating the applications submitted under paragraph (4), the Secretary shall—

(A) take into consideration whether a proposed project would—

(i) increase the availability or reliability of local or regional energy;

(ii) enhance the economic development of the Indian tribe;

(iii) result in or improve the connection of electric power transmission facilities serving the Indian tribe with other electric transmission facilities;

(iv) improve the forest health or watersheds of Federal land or non-Federal land;

(v) demonstrate new investments in infrastructure; or

(vi) otherwise promote the use of woody biomass; and

(B) exclude from consideration any merchantable logs that have been identified by the Secretary for commercial sale.

(6) IMPLEMENTATION.—The Secretary shall—

(A) ensure that the criteria described in paragraph (4) are publicly available by not later than 120 days after the date of enactment of this subsection; and

(B) to the maximum extent practicable, consult with Indian tribes and appropriate tribal organizations likely to be affected in developing the application and otherwise carrying out this subsection.

(7) REPORT.—Not later than September 20, 2018, the Secretary shall submit to Congress a report that describes, with respect to the reporting period—

(A) each individual application received under this subsection; and

(B) each contract and agreement entered into pursuant to this subsection.

(8) TERM.—A contract or agreement entered into under this subsection—

(A) shall be for a term of not more than 20 years; and

(B) may be renewed in accordance with this subsection for not more than an additional 10 years.

SEC. 203. WEATHERIZATION PROGRAM.

Section 413(d) of the Energy Conservation and Production Act (42 U.S.C. 6863(d)) is amended—

(1) by striking paragraph (1) and inserting the following:

''(1) RESERVATION OF AMOUNTS.—

''(A) IN GENERAL.—Subject to subparagraph (B) and notwithstanding any other provision of this part, the Secretary shall reserve from amounts that would otherwise be allocated to a State under this part not less than 100 percent, but not more than 150 percent, of an amount which bears the same proportion to the allocation of that State for the applicable fiscal year as the population of all low-income members of an Indian tribe in that State bears to the population of all low-income individuals in that State.

''(B) RESTRICTIONS.—Subparagraph (A) shall apply only if—

''(i) the tribal organization serving the low-income members of the applicable Indian tribe requests that the Secretary make a grant directly; and

''(ii) the Secretary determines that the low-income members of the applicable Indian tribe would be equally or better served by making a grant directly than a grant made to the State in which the low-income members reside.

''(C) PRESUMPTION.—If the tribal organization requesting the grant is a tribally designated housing entity (as defined in section 4 of the Native American Housing Assistance and Self-Determination Act of 1996 (25 U.S.C. 4103)) that has operated without material audit exceptions (or without any material audit exceptions that were not corrected within a 3-year period), the Secretary shall presume that the low-income members of the applicable Indian tribe would be equally or better served by making a grant directly to the tribal organization than by a grant made to the State in which the low-income members reside.'';

(2) in paragraph (2)—

(A) by striking ''The sums'' and inserting ''ADMINISTRATION.—The amounts'';

(B) by striking ''on the basis of his determination'';

(C) by striking ''individuals for whom such a determination has been made'' and inserting ''low-income members of the Indian tribe''; and

(D) by striking ''he'' and inserting ''the Secretary''; and

(3) in paragraph (3), by striking ''In order'' and inserting ''APPLICATION.—In order''.

SEC. 204. APPRAISALS.

(a) IN GENERAL.—Title XXVI of the Energy Policy Act of 1992 (25 U.S.C. 3501 et seq.) is amended by adding at the end the following:

''SEC. 2607. APPRAISALS.

''(a) IN GENERAL.—For any transaction that requires approval of the Secretary and involves mineral or energy resources held in trust by the United States for the benefit of an Indian tribe or by an Indian tribe subject to Federal restrictions against alienation, any appraisal relating to fair market value of those resources required to be prepared under applicable law may be prepared by—

''(1) the Secretary;

''(2) the affected Indian tribe; or

''(3) a certified, third-party appraiser pursuant to a contract with the Indian tribe.

''(b) SECRETARIAL REVIEW AND APPROVAL.—Not later than 45 days after the date on which the Secretary receives an appraisal prepared by or for an Indian tribe under paragraph (2) or (3) of subsection (a), the Secretary shall—

''(1) review the appraisal; and

''(2) approve the appraisal unless the Secretary determines that the appraisal fails to meet the standards set forth in regulations promulgated under subsection (d).

''(c) NOTICE OF DISAPPROVAL.—If the Secretary determines that an appraisal submitted for approval under subsection (b) should be disapproved, the Secretary shall give written notice of the disapproval to the Indian tribe and a description of—

''(1) each reason for the disapproval; and

''(2) how the appraisal should be corrected or otherwise cured to meet the applicable standards set forth in the regulations promulgated under subsection (d).

''(d) REGULATIONS.—The Secretary shall promulgate regulations to carry out this section, including standards the Secretary shall use for approving or disapproving the appraisal described in subsection (a).''.

SEC. 205. LEASES OF RESTRICTED LANDS FOR NAVAJO NATION.

(a) IN GENERAL.—Subsection (e)(1) of the first section of the Act of August 9, 1955 (commonly known as the ''Long-Term Leasing Act'') (25 U.S.C. 415(e)(1)), is amended—

(1) by striking '', except a lease for'' and inserting '', including a lease for'';

(2) by striking subparagraph (A) and inserting the following:

''(A) in the case of a business or agricultural lease, 99 years;'';

(3) in subparagraph (B), by striking the period at the end and inserting ''; and''; and

(4) by adding at the end the following:

''(C) in the case of a lease for the exploration, development, or extraction of any mineral resource (including geothermal resources), 25 years, except that—

''(i) any such lease may include an option to renew for 1 additional term of not to exceed 25 years; and

''(ii) any such lease for the exploration, development, or extraction of an oil or gas resource shall be for a term of not to exceed 10 years, plus such additional period as the Navajo Nation determines to be appropriate in any case in which an oil or gas resource is produced in a paying quantity.''.

(b) GAO REPORT.—Not later than 5 years after the date of enactment of this Act, the Comptroller General of the United States shall prepare and submit to Congress a report describing the progress made in carrying out the amendment made by subsection (a).

SEC. 206. EXTENSION OF TRIBAL LEASE PERIOD FOR THE CROW TRIBE OF MONTANA.

Subsection (a) of the first section of the Act of August 9, 1955 (25 U.S.C. 415(a)), is amended in the second sentence by inserting '', land held in trust for the Crow Tribe of Montana'' after ''Devils Lake Sioux Reservation''.

SEC. 207. TRUST STATUS OF LEASE PAYMENTS.

(a) DEFINITION OF SECRETARY.—In this section, the term ''Secretary'' means the Secretary of the Interior.

(b) TREATMENT OF LEASE PAYMENTS.—

(1) IN GENERAL.—Except as provided in paragraph (2) and at the request of the Indian tribe or individual Indian, any advance

payments, bid deposits, or other earnest money received by the Secretary in connection with the review and Secretarial approval under any other Federal law (including regulations) of a sale, lease, permit, or any other conveyance of any interest in any trust or restricted land of any Indian tribe or individual Indian shall, upon receipt and prior to Secretarial approval of the contract or conveyance instrument, be held in the trust fund system for the benefit of the Indian tribe and individual Indian from whose land the funds were generated.

(2) RESTRICTION.—If the advance payment, bid deposit, or other earnest money received by the Secretary results from competitive bidding, upon selection of the successful bidder, only the funds paid by the successful bidder shall be held in the trust fund system.

(c) USE OF FUNDS.—

(1) IN GENERAL.—On the approval of the Secretary of a contract or other instrument for a sale, lease, permit, or any other conveyance described in subsection (b)(1), the funds held in the trust fund system and described in subsection (b), along with all income generated from the investment of those funds, shall be disbursed to the Indian tribe or individual Indian landowners.

(2) ADMINISTRATION.—If a contract or other instrument for a sale, lease, permit, or any other conveyance described in subsection (b)(1) is not approved by the Secretary, the funds held in the trust fund system and described in subsection (b), along with all income generated from the investment of those funds, shall be paid to the party identified in, and in such amount and on such terms as set out in, the applicable regulations, advertisement, or other notice governing the proposed conveyance of the interest in the land at issue.

(d) APPLICABILITY.—This section shall apply to any advance payment, bid deposit, or other earnest money received by the Secretary in connection with the review and Secretarial approval under any other Federal law (including regulations) of a sale, lease, permit, or any other conveyance of any interest in any trust or restricted land of any Indian tribe or individual Indian on or after the date of enactment of this Act.

SA 2715. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. PROHIBITION ON THE INDEFINITE DETENTION OF CITIZENS AND LAWFUL PERMANENT RESIDENTS.

Section 4001 of title 18, United States Code, is amended—

(1) by striking subsection (a) and inserting the following:

''(a) No citizen or lawful permanent resident shall be imprisoned or otherwise detained by the United States except consistent with the Constitution and pursuant to an Act of Congress that expressly authorizes such imprisonment or detention.'';

(2) by redesignating subsection (b) as subsection (c); and

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

''(b)(1) A general authorization to use military force, a declaration of war, or any similar authority, on its own, shall not be construed to authorize the imprisonment or detention without charge or trial of a citizen or lawful permanent resident of the United States apprehended in the United States.

''(2) Paragraph (1) applies to an authorization to use military force, a declaration of war, or any similar authority enacted before, on, or after the date of the enactment of the Cybersecurity Information Sharing Act of 2015.

''(3) This section shall not be construed to authorize the imprisonment or detention of a citizen of the United States, a lawful permanent resident of the United States, or any other person who is apprehended in the United States.''.

SA 2716. Mr. BURR (for himself and Mrs. FEINSTEIN) proposed an amendment to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. TABLE OF CONTENTS.

The table of contents of this Act is as follows:

TITLE I—CYBERSECURITY INFORMATION SHARING

SEC. 101. SHORT TITLE.

This title may be cited as the ''Cybersecurity Information Sharing Act of 2015''.

SEC. 102. DEFINITIONS.

In this title:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(2) ANTITRUST LAWS.—The term ''antitrust laws''—

(A) has the meaning given the term in section 1 of the Clayton Act (15 U.S.C. 12);

(B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and

(C) includes any State law that has the same intent and effect as the laws under subparagraphs (A) and (B).

(3) APPROPRIATE FEDERAL ENTITIES.—The term ''appropriate Federal entities'' means the following:

(A) The Department of Commerce.
(B) The Department of Defense.
(C) The Department of Energy.
(D) The Department of Homeland Security.
(E) The Department of Justice.
(F) The Department of the Treasury.
(G) The Office of the Director of National Intelligence.

(4) CYBERSECURITY PURPOSE.—The term ''cybersecurity purpose'' means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

(5) CYBERSECURITY THREAT.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term ''cybersecurity threat'' means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

(B) EXCLUSION.—The term ''cybersecurity threat'' does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

(6) CYBER THREAT INDICATOR.—The term ''cyber threat indicator'' means information that is necessary to describe or identify—

(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

(B) a method of defeating a security control or exploitation of a security vulnerability;

(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

(E) malicious cyber command and control;

(F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

(H) any combination thereof.

(7) DEFENSIVE MEASURE.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term ''defensive measure'' means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting

an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

(B) EXCLUSION.—The term ''defensive measure'' does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or data on an information system not belonging to—

(i) the private entity operating the measure; or

(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

(8) ENTITY.—

(A) IN GENERAL.—Except as otherwise provided in this paragraph, the term ''entity'' means any private entity, non-Federal government agency or department, or State, tribal, or local government (including a political subdivision, department, or component thereof).

(B) INCLUSIONS.—The term ''entity'' includes a government agency or department of the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

(C) EXCLUSION.—The term ''entity'' does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(9) FEDERAL ENTITY.—The term ''Federal entity'' means a department or agency of the United States or any component of such department or agency.

(10) INFORMATION SYSTEM.—The term ''information system''—

(A) has the meaning given the term in section 3502 of title 44, United States Code; and

(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

(11) LOCAL GOVERNMENT.—The term ''local government'' means any borough, city, county, parish, town, township, village, or other political subdivision of a State.

(12) MALICIOUS CYBER COMMAND AND CONTROL.—The term ''malicious cyber command and control'' means a method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

(13) MALICIOUS RECONNAISSANCE.—The term ''malicious reconnaissance'' means a method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(14) MONITOR.—The term ''monitor'' means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

(15) PRIVATE ENTITY.—

(A) IN GENERAL.—Except as otherwise provided in this paragraph, the term ''private entity'' means any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof.

(B) INCLUSION.—The term ''private entity'' includes a State, tribal, or local government performing electric or other utility services.

(C) EXCLUSION.—The term ''private entity'' does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(16) SECURITY CONTROL.—The term ''security control'' means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

(17) SECURITY VULNERABILITY.—The term ''security vulnerability'' means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

(18) TRIBAL.—The term ''tribal'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

SEC. 103. SHARING OF INFORMATION BY THE FEDERAL GOVERNMENT.

(a) IN GENERAL.—Consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate Federal entities, shall develop and promulgate procedures to facilitate and promote—

(1) the timely sharing of classified cyber threat indicators in the possession of the Federal Government with cleared representatives of relevant entities;

(2) the timely sharing with relevant entities of cyber threat indicators or information in the possession of the Federal Government that may be declassified and shared at an unclassified level;

(3) the sharing with relevant entities, or the public if appropriate, of unclassified, including controlled unclassified, cyber threat indicators in the possession of the Federal Government;

(4) the sharing with entities, if appropriate, of information in the possession of the Federal Government about cybersecurity threats to such entities to prevent or mitigate adverse effects from such cybersecurity threats; and

(5) the period sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analysis of cyber threat indicators and information in possession of the Federal Government, with attention to accessibility and implementation challenges faced by small business concerns (as defined in section 3 of the Small Business Act (15 U.S.C. 532)).

(b) DEVELOPMENT OF PROCEDURES.—

(1) IN GENERAL.—The procedures developed and promulgated under subsection (a) shall—

(A) ensure the Federal Government has and maintains the capability to share cyber threat indicators in real time consistent with the protection of classified information;

(B) incorporate, to the greatest extent practicable, existing processes and existing roles and responsibilities of Federal and non-Federal entities for information sharing by the Federal Government, including sector specific information sharing and analysis centers;

(C) include procedures for notifying, in a timely manner, entities that have received a cyber threat indicator from a Federal entity under this title that is known or determined to be in error or in contravention of the requirements of this title or another provision of Federal law or policy of such error or contravention;

(D) include requirements for Federal entities sharing cyber threat indicators or defensive measures to implement and utilize security controls to protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures;

(E) include procedures that require a Federal entity, prior to the sharing of a cyber threat indicator—

(i) to review such cyber threat indicator to assess whether such cyber threat indicator contains any information that such Federal entity knows at the time of sharing to be personal information or information that identifies a specific person not directly related to a cybersecurity threat and remove such information; or

(ii) to implement and utilize a technical capability configured to remove any personal information or information that identifies a specific person not directly related to a cybersecurity threat; and

(F) include procedures for notifying, in a timely manner, any United States person whose personal information is known or determined to have been shared by a Federal entity in violation of this Act.

(2) COORDINATION.—In developing the procedures required under this section, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General shall coordinate with appropriate Federal entities, including the Small Business Administration and the National Laboratories (as defined in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801)), to ensure that effective protocols are implemented that will facilitate and promote the sharing of cyber threat indicators by the Federal Government in a timely manner.

(c) SUBMITTAL TO CONGRESS.—Not later than 60 days after the date of the enactment of this Act, the Director of National Intelligence, in consultation with the heads of the appropriate Federal entities, shall submit to Congress the procedures required by subsection (a).

SEC. 104. AUTHORIZATIONS FOR PREVENTING, DETECTING, ANALYZING, AND MITIGATING CYBERSECURITY THREATS.

(a) AUTHORIZATION FOR MONITORING.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, monitor—

(A) an information system of such private entity;

(B) an information system of another entity, upon the authorization and written consent of such other entity;

(C) an information system of a Federal entity, upon the authorization and written consent of an authorized representative of the Federal entity; and

(D) information that is stored on, processed by, or transiting an information system monitored by the private entity under this paragraph.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to authorize the monitoring of an information system, or the use of any information obtained through such monitoring, other than as provided in this title; or

(B) to limit otherwise lawful activity.

(b) AUTHORIZATION FOR OPERATION OF DEFENSIVE MEASURES.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, operate a defensive measure that is applied to—

(A) an information system of such private entity in order to protect the rights or property of the private entity;

(B) an information system of another entity upon written consent of such entity for operation of such defensive measure to protect the rights or property of such entity; and

(C) an information system of a Federal entity upon written consent of an authorized representative of such Federal entity for operation of such defensive measure to protect the rights or property of the Federal Government.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to authorize the use of a defensive measure other than as provided in this subsection; or

(B) to limit otherwise lawful activity.

(c) AUTHORIZATION FOR SHARING OR RECEIVING CYBER THREAT INDICATORS OR DEFENSIVE MEASURES.—

(1) IN GENERAL.—Except as provided in paragraph (2) and notwithstanding any other provision of law, an entity may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other entity or the Federal Government a cyber threat indicator or defensive measure.

(2) LAWFUL RESTRICTION.—An entity receiving a cyber threat indicator or defensive measure from another entity or Federal entity shall comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicator or defensive measure by the sharing entity or Federal entity.

(3) CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to authorize the sharing or receiving of a cyber threat indicator or defensive measure other than as provided in this subsection; or

(B) to limit otherwise lawful activity.

(d) PROTECTION AND USE OF INFORMATION.—

(1) SECURITY OF INFORMATION.—An entity monitoring an information system, operating a defensive measure, or providing or receiving a cyber threat indicator or defensive measure under this section shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicator or defensive measure.

(2) REMOVAL OF CERTAIN PERSONAL INFORMATION.—An entity sharing a cyber threat indicator pursuant to this title shall, prior to such sharing—

(A) review such cyber threat indicator to assess whether such cyber threat indicator contains any information that the entity knows at the time of sharing to be personal information or information that identifies a specific person not directly related to a cybersecurity threat and remove such information; or

(B) implement and utilize a technical capability configured to remove any information contained within such indicator that the entity knows at the time of sharing to be personal information or information that identifies a specific person not directly related to a cybersecurity threat.

(3) USE OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY ENTITIES.—

(A) IN GENERAL.—Consistent with this title, a cyber threat indicator or defensive measure shared or received under this section may, for cybersecurity purposes—

(i) be used by an entity to monitor or operate a defensive measure that is applied to—

(I) an information system of the entity; or

(II) an information system of another entity or a Federal entity upon the written consent of that other entity or that Federal entity; and

(ii) be otherwise used, retained, and further shared by an entity subject to—

(I) an otherwise lawful restriction placed by the sharing entity or Federal entity on such cyber threat indicator or defensive measure; or

(II) an otherwise applicable provision of law.

(B) CONSTRUCTION.—Nothing in this paragraph shall be construed to authorize the use of a cyber threat indicator or defensive measure other than as provided in this section.

(4) USE OF CYBER THREAT INDICATORS BY STATE, TRIBAL, OR LOCAL GOVERNMENT.—

(A) LAW ENFORCEMENT USE.—

(i) PRIOR WRITTEN CONSENT.—Except as provided in clause (ii), a cyber threat indicator shared with a State, tribal, or local government under this section may, with the prior written consent of the entity sharing such indicator, be used by a State, tribal, or local government for the purpose of preventing, investigating, or prosecuting any of the offenses described in section 105(d)(5)(A)(vi).

(ii) ORAL CONSENT.—If exigent circumstances prevent obtaining written consent under clause (i), such consent may be provided orally with subsequent documentation of the consent.

(B) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator shared with a State, tribal, or local government under this section shall be—

(i) deemed voluntarily shared information; and

(ii) exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records.

(C) STATE, TRIBAL, AND LOCAL REGULATORY AUTHORITY.—

(i) IN GENERAL.—Except as provided in clause (ii), a cyber threat indicator or defensive measure shared with a State, tribal, or local government under this title shall not be directly used by any State, tribal, or local government to regulate, including an enforcement action, the lawful activity of any entity, including an activity relating to monitoring, operating a defensive measure, or sharing of a cyber threat indicator.

(ii) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS.—A cyber threat indicator or defensive measures shared as described in clause (i) may, consistent with a State, tribal, or local government regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of a regulation relating to such information systems.

(e) ANTITRUST EXEMPTION.—

(1) IN GENERAL.—Except as provided in section 108(e), it shall not be considered a violation of any provision of antitrust laws for 2 or more private entities to exchange or provide a cyber threat indicator, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity threat, for cybersecurity purposes under this title.

(2) APPLICABILITY.—Paragraph (1) shall apply only to information that is exchanged or assistance provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system; or

(B) communicating or disclosing a cyber threat indicator to help prevent, investigate, or mitigate the effect of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system.

(f) NO RIGHT OR BENEFIT.—The sharing of a cyber threat indicator with an entity under this title shall not create a right or benefit to similar information by such entity or any other entity.

SEC. 105. SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH THE FEDERAL GOVERNMENT.

(a) REQUIREMENT FOR POLICIES AND PROCEDURES.—

(1) INTERIM POLICIES AND PROCEDURES.—Not later than 60 days after the date of the enactment of this Act, the Attorney General and the Secretary of Homeland Security shall, in coordination with the heads of the appropriate Federal entities, develop and submit to Congress interim policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government.

(2) FINAL POLICIES AND PROCEDURES.—Not later than 180 days after the date of the enactment of this Act, the Attorney General and the Secretary of Homeland Security shall, in coordination with the heads of the appropriate Federal entities, promulgate final policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government.

(3) REQUIREMENTS CONCERNING POLICIES AND PROCEDURES.—Consistent with the guidelines required by subsection (b), the policies and procedures developed and promulgated under this subsection shall—

(A) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 104(c) through the real-time process described in subsection (c) of this section—

(i) are shared in an automated manner with all of the appropriate Federal entities;

(ii) are only subject to a delay, modification, or other action due to controls established for such real-time process that could impede real-time receipt by all of the appropriate Federal entities when the delay, modification, or other action is due to controls—

(I) agreed upon unanimously by all of the heads of the appropriate Federal entities;

(II) carried out before any of the appropriate Federal entities retains or uses the cyber threat indicators or defensive measures; and

(III) uniformly applied such that each of the appropriate Federal entities is subject to the same delay, modification, or other action; and

(iii) may be provided to other Federal entities;

(B) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 104 in a manner other than the real time process described in subsection (c) of this section—

(i) are shared as quickly as operationally practicable with all of the appropriate Federal entities;

(ii) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities; and

(iii) may be provided to other Federal entities;

(C) consistent with this title, any other applicable provisions of law, and the fair information practice principles set forth in appendix A of the document entitled ''National Strategy for Trusted Identities in Cyberspace'' and published by the President in April, 2011, govern the retention, use, and dissemination by the Federal Government of cyber threat indicators shared with the Federal Government under this title, including the extent, if any, to which such cyber threat indicators may be used by the Federal Government; and

(D) ensure there are—

(i) audit capabilities; and

(ii) appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under this title in an unauthorized manner.

(4) GUIDELINES FOR ENTITIES SHARING CYBER THREAT INDICATORS WITH FEDERAL GOVERNMENT.—

(A) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Attorney General and the Secretary of Homeland Security shall develop and make publicly available guidance to assist entities and promote sharing of cyber threat indicators with Federal entities under this title.

(B) CONTENTS.—The guidelines developed and made publicly available under subparagraph (A) shall include guidance on the following:

(i) Identification of types of information that would qualify as a cyber threat indicator under this title that would be unlikely to include personal information or information that identifies a specific person not directly related to a cyber security threat.

(ii) Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat.

(iii) Such other matters as the Attorney General and the Secretary of Homeland Security consider appropriate for entities sharing cyber threat indicators with Federal entities under this title.

(b) PRIVACY AND CIVIL LIBERTIES.—

(1) GUIDELINES OF ATTORNEY GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1), develop, submit to Congress, and make available to the public interim guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this title.

(2) FINAL GUIDELINES.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1) and such private entities with industry expertise as the Attorney General considers relevant, promulgate final guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this title.

(B) PERIODIC REVIEW.—The Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers and private entities described in subparagraph (A), periodically, but not less frequently than once every two years, review the guidelines promulgated under subparagraph (A).

(3) CONTENT.—The guidelines required by paragraphs (1) and (2) shall, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats—

(A) limit the effect on privacy and civil liberties of activities by the Federal Government under this title;

(B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information or information that identifies specific persons, including by establishing—

(i) a process for the timely destruction of such information that is known not to be directly related to uses authorized under this title; and

(ii) specific limitations on the length of any period in which a cyber threat indicator may be retained;

(C) include requirements to safeguard cyber threat indicators containing personal information or information that identifies specific persons from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines;

(D) include procedures for notifying entities and Federal entities if information received pursuant to this section is known or determined by a Federal entity receiving such information not to constitute a cyber threat indicator;

(E) protect the confidentiality of cyber threat indicators containing personal information or information that identifies specific persons to the greatest extent practicable and require recipients to be informed that such indicators may only be used for purposes authorized under this title; and

(F) include steps that may be needed so that dissemination of cyber threat indicators is consistent with the protection of classified and other sensitive national security information.

(c) CAPABILITY AND PROCESS WITHIN THE DEPARTMENT OF HOMELAND SECURITY.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the heads of the appropriate Federal entities, shall develop and implement a capability and process within the Department of Homeland Security that—

(A) shall accept from any entity in real time cyber threat indicators and defensive measures, pursuant to this section;

(B) shall, upon submittal of the certification under paragraph (2) that such capability and process fully and effectively operates as described in such paragraph, be the process by which the Federal Government receives cyber threat indicators and defensive measures under this title that are shared by a private entity with the Federal Government through electronic mail or media, an interactive form on an Internet website, or a real time, automated process between information systems except—

(i) consistent with section 104, communications between a Federal entity and a private entity regarding a previously shared cyber threat indicator to describe the relevant cybersecurity threat or develop a defensive measure based on such cyber threat indicator; and

(ii) communications by a regulated entity with such entity's Federal regulatory authority regarding a cybersecurity threat;

(C) ensures that all of the appropriate Federal entities receive in an automated manner such cyber threat indicators shared through the real-time process within the Department of Homeland Security;

(D) is in compliance with the policies, procedures, and guidelines required by this section; and

(E) does not limit or prohibit otherwise lawful disclosures of communications, records, or other information, including—

(i) reporting of known or suspected criminal activity, by an entity to any other entity or a Federal entity;

(ii) voluntary or legally compelled participation in a Federal investigation; and

(iii) providing cyber threat indicators or defensive measures as part of a statutory or authorized contractual requirement.

(2) CERTIFICATION.—Not later than 10 days prior to the implementation of the capability and process required by paragraph (1), the Secretary of Homeland Security shall, in consultation with the heads of the appropriate Federal entities, certify to Congress whether such capability and process fully and effectively operates—

(A) as the process by which the Federal Government receives from any entity a cyber threat indicator or defensive measure under this title; and

(B) in accordance with the policies, procedures, and guidelines developed under this section.

(3) PUBLIC NOTICE AND ACCESS.—The Secretary of Homeland Security shall ensure there is public notice of, and access to, the capability and process developed and implemented under paragraph (1) so that—

(A) any entity may share cyber threat indicators and defensive measures through such process with the Federal Government; and

(B) all of the appropriate Federal entities receive such cyber threat indicators and defensive measures in real time with receipt through the process within the Department of Homeland Security.

(4) OTHER FEDERAL ENTITIES.—The process developed and implemented under paragraph (1) shall ensure that other Federal entities receive in a timely manner any cyber threat indicators and defensive measures shared with the Federal Government through such process.

(5) REPORT ON DEVELOPMENT AND IMPLEMENTATION.—

(A) IN GENERAL.—Not later than 60 days after the date of the enactment of this Act, the Secretary of Homeland Security shall submit to Congress a report on the development and implementation of the capability and process required by paragraph (1), including a description of such capability and process and the public notice of, and access to, such process.

(B) CLASSIFIED ANNEX.—The report required by subparagraph (A) shall be submitted in unclassified form, but may include a classified annex.

(d) INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.—

(1) NO WAIVER OF PRIVILEGE OR PROTECTION.—The provision of cyber threat indicators and defensive measures to the Federal Government under this title shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

(2) PROPRIETARY INFORMATION.—Consistent with section 104(c)(2), a cyber threat indicator or defensive measure provided by an entity to the Federal Government under this title shall be considered the commercial, financial, and proprietary information of such entity when so designated by the originating entity or a third party acting in accordance with the written authorization of the originating entity.

(3) EXEMPTION FROM DISCLOSURE.—Cyber threat indicators and defensive measures provided to the Federal Government under this title shall be—

(A) deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records; and

(B) withheld, without discretion, from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local provision of law requiring disclosure of information or records.

(4) EX PARTE COMMUNICATIONS.—The provision of a cyber threat indicator or defensive measure to the Federal Government under this title shall not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

(5) DISCLOSURE, RETENTION, AND USE.—

(A) AUTHORIZED ACTIVITIES.—Cyber threat indicators and defensive measures provided to the Federal Government under this title may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

(i) a cybersecurity purpose;

(ii) the purpose of identifying a cybersecurity threat, including the source of such cybersecurity threat, or a security vulnerability;

(iii) the purpose of identifying a cybersecurity threat involving the use of an information system by a foreign adversary or terrorist;

(iv) the purpose of responding to, or otherwise preventing or mitigating, an imminent threat of death, serious bodily harm, or serious economic harm, including a terrorist act or a use of a weapon of mass destruction;

(v) the purpose of responding to, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(vi) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in clause (iv) or any of the offenses listed in—

(I) sections 1028 through 1030 of title 18, United States Code (relating to fraud and identity theft);

(II) chapter 37 of such title (relating to espionage and censorship); and

(III) chapter 90 of such title (relating to protection of trade secrets).

(B) PROHIBITED ACTIVITIES.—Cyber threat indicators and defensive measures provided to the Federal Government under this title shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under subparagraph (A).

(C) PRIVACY AND CIVIL LIBERTIES.—Cyber threat indicators and defensive measures provided to the Federal Government under this title shall be retained, used, and disseminated by the Federal Government—

(i) in accordance with the policies, procedures, and guidelines required by subsections (a) and (b);

(ii) in a manner that protects from unauthorized use or disclosure any cyber threat indicators that may contain personal information or information that identifies specific persons; and

(iii) in a manner that protects the confidentiality of cyber threat indicators containing personal information or information that identifies a specific person.

(D) FEDERAL REGULATORY AUTHORITY.—

(i) IN GENERAL.—Except as provided in clause (ii), cyber threat indicators and defensive measures provided to the Federal Government under this title shall not be directly used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any entity, including activities relating to monitoring, operating defensive measures, or sharing cyber threat indicators.

(ii) EXCEPTIONS.—

(I) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS.—Cyber threat indicators and defensive measures provided to the Federal Government under this title may, consistent with Federal or State regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such information systems.

(II) PROCEDURES DEVELOPED AND IMPLEMENTED UNDER THIS TITLE.—Clause (i) shall not apply to procedures developed and implemented under this title.

SEC. 106. PROTECTION FROM LIABILITY.

(a) MONITORING OF INFORMATION SYSTEMS.—No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of information systems and information under section 104(a) that is conducted in accordance with this title.

(b) SHARING OR RECEIPT OF CYBER THREAT INDICATORS.—No cause of action shall lie or be maintained in any court against any entity, and such action shall be promptly dismissed, for the sharing or receipt of cyber threat indicators or defensive measures under section 104(c) if—

(1) such sharing or receipt is conducted in accordance with this title; and

(2) in a case in which a cyber threat indicator or defensive measure is shared with the Federal Government, the cyber threat indicator or defensive measure is shared in a manner that is consistent with section 105(c)(1)(B) and the sharing or receipt, as the case may be, occurs after the earlier of—

(A) the date on which the interim policies and procedures are submitted to Congress under section 105(a)(1) and guidelines are submitted to Congress under section 105(b)(1); or

(B) the date that is 60 days after the date of the enactment of this Act.

(c) CONSTRUCTION.—Nothing in this section shall be construed—

(1) to require dismissal of a cause of action against an entity that has engaged in gross negligence or willful misconduct in the course of conducting activities authorized by this title; or

(2) to undermine or limit the availability of otherwise applicable common law or statutory defenses.

SEC. 107. OVERSIGHT OF GOVERNMENT ACTIVITIES.

(a) BIENNIAL REPORT ON IMPLEMENTATION.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, and not less frequently than once every 2 years thereafter, the heads of the appropriate Federal entities shall jointly submit and the Inspector General of the Department of Homeland Security, the Inspector General of the Intelligence Community, the Inspector General of the Department of Justice, the Inspector General of the Department of Defense, and the Inspector General of the Department of Energy, in consultation with the Council of Inspectors General on Financial Oversight, shall jointly submit to Congress a detailed report concerning the implementation of this title during—

(A) in the case of the first report submitted under this paragraph, the most recent 1-year period; and

(B) in the case of any subsequent report submitted under this paragraph, the most recent 2-year period.

(2) CONTENTS.—Each report submitted under paragraph (1) shall include, for the period covered by the report, the following:

(A) An assessment of the sufficiency of the policies, procedures, and guidelines required by section 105 in ensuring that cyber threat indicators are shared effectively and responsibly within the Federal Government.

(B) An evaluation of the effectiveness of real-time information sharing through the capability and process developed under section 105(c), including any impediments to such real-time sharing.

(C) An assessment of the sufficiency of the procedures developed under section 103 in ensuring that cyber threat indicators in the possession of the Federal Government are shared in a timely and adequate manner with appropriate entities, or, if appropriate, are made publicly available.

(D) An assessment of whether cyber threat indicators have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purposes of this title.

(E) A review of the type of cyber threat indicators shared with the appropriate Federal entities under this title, including the following:

(i) The number of cyber threat indicators received through the capability and process developed under section 105(c).

(ii) The number of times that information shared under this title was used by a Federal entity to prosecute an offense consistent with section 105(d)(5)(A).

(iii) The degree to which such information may affect the privacy and civil liberties of specific persons.

(iv) A quantitative and qualitative assessment of the effect of the sharing of such cyber threat indicators with the Federal Government on privacy and civil liberties of specific persons, including the number of notices that were issued with respect to a failure to remove personal information or information that identified a specific person not directly related to a cybersecurity threat in accordance with the procedures required by section 105(b)(3)(D).

(v) The adequacy of any steps taken by the Federal Government to reduce such effect.

(F) A review of actions taken by the Federal Government based on cyber threat indicators shared with the Federal Government under this title, including the appropriateness of any subsequent use or dissemination of such cyber threat indicators by a Federal entity under section 105.

(G) A description of any significant violations of the requirements of this title by the Federal Government.

(H) A summary of the number and type of entities that received classified cyber threat indicators from the Federal Government under this title and an evaluation of the risks and benefits of sharing such cyber threat indicators.

(3) RECOMMENDATIONS.—Each report submitted under paragraph (1) may include recommendations for improvements or modifications to the authorities and processes under this title.

(4) FORM OF REPORT.—Each report required by paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(b) REPORTS ON PRIVACY AND CIVIL LIBERTIES.—

(1) BIENNIAL REPORT FROM PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD.—Not later than 2 years after the date of the enactment of this Act and not less frequently than once every 2 years thereafter, the Privacy and Civil Liberties Oversight Board shall submit to Congress and the President a report providing—

(A) an assessment of the effect on privacy and civil liberties by the type of activities carried out under this title; and

(B) an assessment of the sufficiency of the policies, procedures, and guidelines established pursuant to section 105 in addressing concerns relating to privacy and civil liberties.

(2) BIENNIAL REPORT OF INSPECTORS GENERAL.—

(A) IN GENERAL.—Not later than 2 years after the date of the enactment of this Act and not less frequently than once every 2 years thereafter, the Inspector General of the Department of Homeland Security, the Inspector General of the Intelligence Community, the Inspector General of the Department of Justice, the Inspector General of the Department of Defense, and the Inspector General of the Department of Energy shall, in consultation with the Council of Inspectors General on Financial Oversight, jointly submit to Congress a report on the receipt, use, and dissemination of cyber threat indicators and defensive measures that have been shared with Federal entities under this title.

(B) CONTENTS.—Each report submitted under subparagraph (A) shall include the following:

(i) A review of the types of cyber threat indicators shared with Federal entities.

(ii) A review of the actions taken by Federal entities as a result of the receipt of such cyber threat indicators.

(iii) A list of Federal entities receiving such cyber threat indicators.

(iv) A review of the sharing of such cyber threat indicators among Federal entities to identify inappropriate barriers to sharing information.

(3) RECOMMENDATIONS.—Each report submitted under this subsection may include such recommendations as the Privacy and Civil Liberties Oversight Board, with respect to a report submitted under paragraph (1), or the Inspectors General referred to in paragraph (2)(A), with respect to a report submitted under paragraph (2), may have for improvements or modifications to the authorities under this title.

(4) FORM.—Each report required under this subsection shall be submitted in unclassified form, but may include a classified annex.

SEC. 108. CONSTRUCTION AND PREEMPTION.

(a) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this title shall be construed—

(1) to limit or prohibit otherwise lawful disclosures of communications, records, or other information, including reporting of known or suspected criminal activity, by an entity to any other entity or the Federal Government under this title; or

(2) to limit or prohibit otherwise lawful use of such disclosures by any Federal entity, even when such otherwise lawful disclosures duplicate or replicate disclosures made under this title.

(b) WHISTLE BLOWER PROTECTIONS.—Nothing in this title shall be construed to prohibit or limit the disclosure of information protected under section 2302(b)(8) of title 5, United States Code (governing disclosures of illegality, waste, fraud, abuse, or public health or safety threats), section 7211 of title 5, United States Code (governing disclosures to Congress), section 1034 of title 10, United States Code (governing disclosure to Congress by members of the military), section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) (governing disclosure by employees of elements of the intelligence community), or any similar provision of Federal or State law.

(c) PROTECTION OF SOURCES AND METHODS.—Nothing in this title shall be construed—

(1) as creating any immunity against, or otherwise affecting, any action brought by the Federal Government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, or use of classified information;

(2) to affect the conduct of authorized law enforcement or intelligence activities; or

(3) to modify the authority of a department or agency of the Federal Government to protect classified information and sources and methods and the national security of the United States.

(d) RELATIONSHIP TO OTHER LAWS.—Nothing in this title shall be construed to affect any requirement under any other provision of law for an entity to provide information to the Federal Government.

(e) PROHIBITED CONDUCT.—Nothing in this title shall be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.

(f) INFORMATION SHARING RELATIONSHIPS.—Nothing in this title shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any entity and another entity or a Federal entity; or

(4) to require the use of the capability and process within the Department of Homeland Security developed under section 105(c).

(g) PRESERVATION OF CONTRACTUAL OBLIGATIONS AND RIGHTS.—Nothing in this title shall be construed—

(1) to amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between any entities, or between any entity and a Federal entity; or

(2) to abrogate trade secret or intellectual property rights of any entity or Federal entity.

(h) ANTI-TASKING RESTRICTION.—Nothing in this title shall be construed to permit a Federal entity—

(1) to require an entity to provide information to a Federal entity or another entity;

(2) to condition the sharing of cyber threat indicators with an entity on such entity's provision of cyber threat indicators to a Federal entity or another entity; or

(3) to condition the award of any Federal grant, contract, or purchase on the provision of a cyber threat indicator to a Federal entity or another entity.

(i) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this title shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized in this title.

(j) USE AND RETENTION OF INFORMATION.—Nothing in this title shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal Government to retain or use any information shared under this title for any use other than permitted in this title.

(k) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This title supersedes any statute or other provision of law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this title.

(2) STATE LAW ENFORCEMENT.—Nothing in this title shall be construed to supersede any statute or other provision of law of a State or political subdivision of a State concerning the use of authorized law enforcement practices and procedures.

(l) REGULATORY AUTHORITY.—Nothing in this title shall be construed—

(1) to authorize the promulgation of any regulations not specifically authorized by this title;

(2) to establish or limit any regulatory authority not specifically established or limited under this title; or

(3) to authorize regulatory actions that would duplicate or conflict with regulatory requirements, mandatory standards, or related processes under another provision of Federal law.

(m) AUTHORITY OF SECRETARY OF DEFENSE TO RESPOND TO CYBER ATTACKS.—Nothing in this title shall be construed to limit the authority of the Secretary of Defense to develop, prepare, coordinate, or, when authorized by the President to do so, conduct a military cyber operation in response to a malicious cyber activity carried out against the United States or a United States person by a foreign government or an organization sponsored by a foreign government or a terrorist organization.

SEC. 109. REPORT ON CYBERSECURITY THREATS.

(a) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Director of National Intelligence, in coordination with the heads of other appropriate elements of the intelligence community, shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on cybersecurity threats, including cyber attacks, theft, and data breaches.

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

(1) An assessment of the current intelligence sharing and cooperation relationships of the United States with other countries regarding cybersecurity threats, including cyber attacks, theft, and data breaches, directed against the United States and which threaten the United States national security interests and economy and intellectual property, specifically identifying the relative utility of such relationships, which elements of the intelligence community participate in such relationships, and whether and how such relationships could be improved.

(2) A list and an assessment of the countries and nonstate actors that are the primary threats of carrying out a cybersecurity threat, including a cyber attack, theft, or data breach, against the United States and which threaten the United States national security, economy, and intellectual property.

(3) A description of the extent to which the capabilities of the United States Government to respond to or prevent cybersecurity threats, including cyber attacks, theft, or data breaches, directed against the United States private sector are degraded by a delay in the prompt notification by private entities of such threats or cyber attacks, theft, and breaches.

(4) An assessment of additional technologies or capabilities that would enhance the ability of the United States to prevent and to respond to cybersecurity threats, including cyber attacks, theft, and data breaches.

(5) An assessment of any technologies or practices utilized by the private sector that could be rapidly fielded to assist the intelligence community in preventing and responding to cybersecurity threats.

(c) ADDITIONAL REPORT.—At the time the report required by subsection (a) is submitted, the Director of National Intelligence shall submit to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives a report containing the information required by subsection (b)(2).

(d) FORM OF REPORT.—The report required by subsection (a) shall be made available in classified and unclassified forms.

(e) INTELLIGENCE COMMUNITY DEFINED.—In this section, the term ''intelligence community'' has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

SEC. 110. CONFORMING AMENDMENT.

Section 941(c)(3) of the National Defense Authorization Act for Fiscal Year 2013 (Public Law 112–239; 10 U.S.C. 2224 note) is amended by inserting at the end the following: ''The Secretary may share such information with other Federal entities if such information consists of cyber threat indicators and defensive measures and such information is shared consistent with the policies and procedures promulgated by the Attorney General and the Secretary of Homeland Security under section 105 of the Cybersecurity Information Sharing Act of 2015.''.

TITLE II—FEDERAL CYBERSECURITY ENHANCEMENT

SEC. 201. SHORT TITLE.

This title may be cited as the ''Federal Cybersecurity Enhancement Act of 2015''.

SEC. 202. DEFINITIONS.

In this title—

(1) the term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code;

(2) the term ''agency information system'' has the meaning given the term in section 228 of the Homeland Security Act of 2002, as added by section 203(a);

(3) the term ''appropriate congressional committees'' means—

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

(B) the Committee on Homeland Security of the House of Representatives;

(4) the terms ''cybersecurity risk'' and ''information system'' have the meanings given those terms in section 227 of the Homeland Security Act of 2002, as so redesignated by section 203(a);

(5) the term ''Director'' means the Director of the Office of Management and Budget;

(6) the term ''intelligence community'' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)); and

(7) the term ''Secretary'' means the Secretary of Homeland Security.

SEC. 203. IMPROVED FEDERAL NETWORK SECURITY.

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

(1) by redesignating section 228 as section 229;

(2) by redesignating section 227 as subsection (c) of section 228, as added by paragraph (4), and adjusting the margins accordingly;

(3) by redesignating the second section designated as section 226 (relating to the national cybersecurity and communications integration center) as section 227;

(4) by inserting after section 227, as so redesignated, the following:

''SEC. 228. CYBERSECURITY PLANS.

''(a) DEFINITIONS.—In this section—

''(1) the term 'agency information system' means an information system used or operated by an agency or by another entity on behalf of an agency;

''(2) the terms 'cybersecurity risk' and 'information system' have the meanings given those terms in section 227; and

''(3) the term 'intelligence community' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

''(b) INTRUSION ASSESSMENT PLAN.—

''(1) REQUIREMENT.—The Secretary, in coordination with the Director of the Office of Management and Budget, shall develop and implement an intrusion assessment plan to identify and remove intruders in agency information systems.

''(2) EXCEPTION.—The intrusion assessment plan required under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.'';

(5) in section 228(c), as so redesignated, by striking ''section 226'' and inserting ''section 227''; and

(6) by inserting after section 229, as so redesignated, the following:

''SEC. 230. FEDERAL INTRUSION DETECTION AND PREVENTION SYSTEM.

''(a) DEFINITIONS.—In this section—

''(1) the term 'agency' has the meaning given that term in section 3502 of title 44, United States Code;

''(2) the term 'agency information' means information collected or maintained by or on behalf of an agency;

''(3) the term 'agency information system' has the meaning given the term in section 228; and

''(4) the terms 'cybersecurity risk' and 'information system' have the meanings given those terms in section 227.

''(b) REQUIREMENT.—

''(1) IN GENERAL.—Not later than 1 year after the date of enactment of this section, the Secretary shall deploy, operate, and maintain, to make available for use by any agency, with or without reimbursement—

''(A) a capability to detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system; and

''(B) a capability to prevent network traffic associated with such cybersecurity risks from transiting or traveling to or from an agency information system or modify such network traffic to remove the cybersecurity risk.

''(2) REGULAR IMPROVEMENT.—The Secretary shall regularly deploy new technologies and modify existing technologies to the intrusion detection and prevention capabilities described in paragraph (1) as appropriate to improve the intrusion detection and prevention capabilities.

''(c) ACTIVITIES.—In carrying out subsection (b), the Secretary—

''(1) may access, and the head of an agency may disclose to the Secretary or a private entity providing assistance to the Secretary under paragraph (2), information transiting or traveling to or from an agency information system, regardless of the location from which the Secretary or a private entity providing assistance to the Secretary under paragraph (2) accesses such information, notwithstanding any other provision of law that would otherwise restrict or prevent the head of an agency from disclosing such information to the Secretary or a private entity providing assistance to the Secretary under paragraph (2);

''(2) may enter into contracts or other agreements with, or otherwise request and obtain the assistance of, private entities to deploy and operate technologies in accordance with subsection (b);

''(3) may retain, use, and disclose information obtained through the conduct of activities authorized under this section only to protect information and information systems from cybersecurity risks;

''(4) shall regularly assess through operational test and evaluation in real world or simulated environments available advanced protective technologies to improve detection and prevention capabilities, including commercial and non-commercial technologies and detection technologies beyond signature-based detection, and utilize such technologies when appropriate;

''(5) shall establish a pilot to acquire, test, and deploy, as rapidly as possible, technologies described in paragraph (4);

''(6) shall periodically update the privacy impact assessment required under section 208(b) of the E-Government Act of 2002 (44 U.S.C. 3501 note); and

''(7) shall ensure that—

''(A) activities carried out under this section are reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

''(B) information accessed by the Secretary will be retained no longer than reasonably necessary for the purpose of protecting agency information and agency information systems from a cybersecurity risk;

''(C) notice has been provided to users of an agency information system concerning access to communications of users of the agency information system for the purpose of protecting agency information and the agency information system; and

''(D) the activities are implemented pursuant to policies and procedures governing the operation of the intrusion detection and prevention capabilities.

''(d) PRIVATE ENTITIES.—

''(1) CONDITIONS.—A private entity described in subsection (c)(2) may not—

''(A) disclose any network traffic transiting or traveling to or from an agency information system to any entity without the consent of the Department or the agency that disclosed the information under subsection (c)(1); or

''(B) use any network traffic transiting or traveling to or from an agency information system to which the private entity gains access in accordance with this section for any purpose other than to protect agency information and agency information systems against cybersecurity risks or to administer a contract or other agreement entered into pursuant to subsection (c)(2) or as part of another contract with the Secretary.

''(2) LIMITATION ON LIABILITY.—No cause of action shall lie in any court against a private entity for assistance provided to the Secretary in accordance with this section and any contract or agreement entered into pursuant to subsection (c)(2).

''(3) RULE OF CONSTRUCTION.—Nothing in paragraph (2) shall be construed to authorize an Internet service provider to break a user agreement with a customer without the consent of the customer.

''(e) ATTORNEY GENERAL REVIEW.—Not later than 1 year after the date of enactment of this section, the Attorney General shall review the policies and guidelines for the program carried out under this section to ensure that the policies and guidelines are consistent with applicable law governing the acquisition, interception, retention, use, and disclosure of communications.''.

(b) PRIORITIZING ADVANCED SECURITY TOOLS.—The Director and the Secretary, in consultation with appropriate agencies, shall—

(1) review and update governmentwide policies and programs to ensure appropriate prioritization and use of network security monitoring tools within agency networks; and

(2) brief appropriate congressional committees on such prioritization and use.

(c) AGENCY RESPONSIBILITIES.—

(1) IN GENERAL.—Except as provided in paragraph (2)—

(A) not later than 1 year after the date of enactment of this Act or 2 months after the date on which the Secretary makes available the intrusion detection and prevention capabilities under section 230(b)(1) of the Homeland Security Act of 2002, as added by subsection (a), whichever is later, the head of each agency shall apply and continue to utilize the capabilities to all information traveling between an agency information system and any information system other than an agency information system; and

(B) not later than 6 months after the date on which the Secretary makes available improvements to the intrusion detection and prevention capabilities pursuant to section 230(b)(2) of the Homeland Security Act of 2002, as added by subsection (a), the head of each agency shall apply and continue to utilize the improved intrusion detection and prevention capabilities.

(2) EXCEPTION.—The requirements under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(3) DEFINITION.—Notwithstanding section 202, in this subsection, the term ''agency information system'' means an information system owned or operated by an agency.

(4) RULE OF CONSTRUCTION.—Nothing in this subsection shall be construed to limit an agency from applying the intrusion detection and prevention capabilities under section 230(b)(1) of the Homeland Security Act

of 2002, as added by subsection (a), at the discretion of the head of the agency or as provided in relevant policies, directives, and guidelines.

(d) TABLE OF CONTENTS 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 striking the items relating to the first section designated as section 226, the second section designated as section 226 (relating to the national cybersecurity and communications integration center), section 227, and section 228 and inserting the following:

''Sec. 226. Cybersecurity recruitment and retention.
''Sec. 227. National cybersecurity and communications integration center.
''Sec. 228. Cybersecurity plans.
''Sec. 229. Clearances.
''Sec. 230. Federal intrusion detection and prevention system.''.

SEC. 204. ADVANCED INTERNAL DEFENSES.

(a) ADVANCED NETWORK SECURITY TOOLS.—

(1) IN GENERAL.—The Secretary shall include in the Continuous Diagnostics and Mitigation Program advanced network security tools to improve visibility of network activity, including through the use of commercial and free or open source tools, to detect and mitigate intrusions and anomalous activity.

(2) DEVELOPMENT OF PLAN.—The Director shall develop and implement a plan to ensure that each agency utilizes advanced network security tools, including those described in paragraph (1), to detect and mitigate intrusions and anomalous activity.

(b) IMPROVED METRICS.—The Secretary, in collaboration with the Director, shall review and update the metrics used to measure security under section 3554 of title 44, United States Code, to include measures of intrusion and incident detection and response times.

(c) TRANSPARENCY AND ACCOUNTABILITY.—The Director, in consultation with the Secretary, shall increase transparency to the public on agency cybersecurity posture, including by increasing the number of metrics available on Federal Government performance websites and, to the greatest extent practicable, displaying metrics for department components, small agencies, and micro agencies.

(d) MAINTENANCE OF TECHNOLOGIES.—Section 3553(b)(6)(B) of title 44, United States Code, is amended by inserting '', operating, and maintaining'' after ''deploying''.

(e) EXCEPTION.—The requirements under this section shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

SEC. 205. FEDERAL CYBERSECURITY REQUIREMENTS.

(a) IMPLEMENTATION OF FEDERAL CYBERSECURITY STANDARDS.—Consistent with section 3553 of title 44, United States Code, the Secretary, in consultation with the Director, shall exercise the authority to issue binding operational directives to assist the Director in ensuring timely agency adoption of and compliance with policies and standards promulgated under section 11331 of title 40, United States Code, for securing agency information systems.

(b) CYBERSECURITY REQUIREMENTS AT AGENCIES.—

(1) IN GENERAL.—Consistent with policies, standards, guidelines, and directives on information security under subchapter II of chapter 35 of title 44, United States Code, and the standards and guidelines promulgated under section 11331 of title 40, United States Code, and except as provided in paragraph (2), not later than 1 year after the date of the enactment of this Act, the head of each agency shall—

(A) identify sensitive and mission critical data stored by the agency consistent with the inventory required under the first subsection (c) (relating to the inventory of major information systems) and the second subsection (c) (relating to the inventory of information systems) of section 3505 of title 44, United States Code;

(B) assess access controls to the data described in subparagraph (A), the need for readily accessible storage of the data, and individuals' need to access the data;

(C) encrypt or otherwise render indecipherable to unauthorized users the data described in subparagraph (A) that is stored on or transiting agency information systems;

(D) implement a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires user authentication, as developed by the Administrator of General Services in collaboration with the Secretary; and

(E) implement identity management consistent with section 504 of the Cybersecurity Enhancement Act of 2014 (Public Law 113–274; 15 U.S.C. 7464), including multi-factor authentication, for—

(i) remote access to an agency information system; and

(ii) each user account with elevated privileges on an agency information system.

(2) EXCEPTION.—The requirements under paragraph (1) shall not apply to an agency information system for which—

(A) the head of the agency has personally certified to the Director with particularity that—

(i) operational requirements articulated in the certification and related to the agency information system would make it excessively burdensome to implement the cybersecurity requirement;

(ii) the cybersecurity requirement is not necessary to secure the agency information system or agency information stored on or transiting it; and

(iii) the agency has all taken necessary steps to secure the agency information system and agency information stored on or transiting it; and

(B) the head of the agency or the designee of the head of the agency has submitted the certification described in subparagraph (A) to the appropriate congressional committees and the agency's authorizing committees.

(3) CONSTRUCTION.—Nothing in this section shall be construed to alter the authority of the Secretary, the Director, or the Director of the National Institute of Standards and Technology in implementing subchapter II of chapter 35 of title 44, United States Code. Nothing in this section shall be construed to affect the National Institute of Standards and Technology standards process or the requirement under section 3553(a)(4) of such title or to discourage continued improvements and advancements in the technology, standards, policies, and guidelines used to promote Federal information security.

(c) EXCEPTION.—The requirements under this section shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

SEC. 206. ASSESSMENT; REPORTS.

(a) DEFINITIONS.—In this section—

(1) the term ''intrusion assessments'' means actions taken under the intrusion assessment plan to identify and remove intruders in agency information systems;

(2) the term ''intrusion assessment plan'' means the plan required under section 228(b)(1) of the Homeland Security Act of 2002, as added by section 203(a) of this Act; and

(3) the term ''intrusion detection and prevention capabilities'' means the capabilities required under section 230(b) of the Homeland Security Act of 2002, as added by section 203(a) of this Act.

(b) THIRD PARTY ASSESSMENT.—Not later than 3 years after the date of enactment of this Act, the Government Accountability Office shall conduct a study and publish a report on the effectiveness of the approach and strategy of the Federal Government to securing agency information systems, including the intrusion detection and prevention capabilities and the intrusion assessment plan.

(c) REPORTS TO CONGRESS.—

(1) INTRUSION DETECTION AND PREVENTION CAPABILITIES.—

(A) SECRETARY OF HOMELAND SECURITY REPORT.—Not later than 6 months after the date of enactment of this Act, and annually thereafter, the Secretary shall submit to the appropriate congressional committees a report on the status of implementation of the intrusion detection and prevention capabilities, including—

(i) a description of privacy controls;

(ii) a description of the technologies and capabilities utilized to detect cybersecurity risks in network traffic, including the extent to which those technologies and capabilities include existing commercial and non-commercial technologies;

(iii) a description of the technologies and capabilities utilized to prevent network traffic associated with cybersecurity risks from transiting or traveling to or from agency information systems, including the extent to which those technologies and capabilities include existing commercial and non-commercial technologies;

(iv) a list of the types of indicators or other identifiers or techniques used to detect cybersecurity risks in network traffic transiting or traveling to or from agency information systems on each iteration of the intrusion detection and prevention capabilities and the number of each such type of indicator, identifier, and technique;

(v) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from agency information systems and the number of times the intrusion detection and prevention capabilities blocked network traffic associated with cybersecurity risk; and

(vi) a description of the pilot established under section 230(c)(5) of the Homeland Security Act of 2002, as added by section 203(a) of this Act, including the number of new technologies tested and the number of participating agencies.

(B) OMB REPORT.—Not later than 18 months after the date of enactment of this Act, and annually thereafter, the Director shall submit to Congress, as part of the report required under section 3553(c) of title 44, United States Code, an analysis of agency application of the intrusion detection and prevention capabilities, including—

(i) a list of each agency and the degree to which each agency has applied the intrusion detection and prevention capabilities to an agency information system; and

(ii) a list by agency of—

(I) the number of instances in which the intrusion detection and prevention capabilities detected a cybersecurity risk in network traffic transiting or traveling to or from an agency information system and the types of indicators, identifiers, and techniques used to detect such cybersecurity risks; and

(II) the number of instances in which the intrusion detection and prevention capabilities prevented network traffic associated with a cybersecurity risk from transiting or traveling to or from an agency information

system and the types of indicators, identifiers, and techniques used to detect such agency information systems.

(2) OMB REPORT ON DEVELOPMENT AND IMPLEMENTATION OF INTRUSION ASSESSMENT PLAN, ADVANCED INTERNAL DEFENSES, AND FEDERAL CYBERSECURITY BEST PRACTICES.—The Director shall—

(A) not later than 6 months after the date of enactment of this Act, and 30 days after any update thereto, submit the intrusion assessment plan to the appropriate congressional committees;

(B) not later than 1 year after the date of enactment of this Act, and annually thereafter, submit to Congress, as part of the report required under section 3553(c) of title 44, United States Code—

(i) a description of the implementation of the intrusion assessment plan;

(ii) the findings of the intrusion assessments conducted pursuant to the intrusion assessment plan;

(iii) advanced network security tools included in the Continuous Diagnostics and Mitigation Program pursuant to section 204(a)(1);

(iv) the results of the assessment of the Secretary of best practices for Federal cybersecurity pursuant to section 205(a); and

(v) a list by agency of compliance with the requirements of section 205(b); and

(C) not later than 1 year after the date of enactment of this Act, submit to the appropriate congressional committees—

(i) a copy of the plan developed pursuant to section 204(a)(2); and

(ii) the improved metrics developed pursuant to section 204(b).

SEC. 207. TERMINATION.

(a) IN GENERAL.—The authority provided under section 230 of the Homeland Security Act of 2002, as added by section 203(a) of this Act, and the reporting requirements under section 206(c) shall terminate on the date that is 7 years after the date of enactment of this Act.

(b) RULE OF CONSTRUCTION.—Nothing in subsection (a) shall be construed to affect the limitation of liability of a private entity for assistance provided to the Secretary under section 230(d)(2) of the Homeland Security Act of 2002, as added by section 203(a) of this Act, if such assistance was rendered before the termination date under subsection (a) or otherwise during a period in which the assistance was authorized.

SEC. 208. IDENTIFICATION OF INFORMATION SYSTEMS RELATING TO NATIONAL SECURITY.

(a) IN GENERAL.—Except as provided in subsection (c), not later than 180 days after the date of enactment of this Act—

(1) the Director of National Intelligence, in coordination with the heads of other agencies, shall—

(A) identify all unclassified information systems that provide access to information that may provide an adversary with the ability to derive information that would otherwise be considered classified;

(B) assess the risks that would result from the breach of each unclassified information system identified in subparagraph (A); and

(C) assess the cost and impact on the mission carried out by each agency that owns an unclassified information system identified in subparagraph (A) if the system were to be subsequently designated as a national security system, as defined in section 11103 of title 40, United States Code; and

(2) the Director of National Intelligence shall submit to the appropriate congressional committees, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives a report that includes the findings under paragraph (1).

(b) FORM.—The report submitted under subsection (a)(2) shall be in unclassified form, and shall include a classified annex.

(c) EXCEPTION.—The requirements under subsection (a)(1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

SEC. 209. DIRECTION TO AGENCIES.

(a) IN GENERAL.—Section 3553 of title 44, United States Code, is amended by adding at the end the following:

''(h) DIRECTION TO AGENCIES.—

''(1) AUTHORITY.—

''(A) IN GENERAL.—Subject to subparagraph (B), in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, the Secretary may issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems owned or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat.

''(B) EXCEPTION.—The authorities of the Secretary under this subsection shall not apply to a system described subsection (d) or to a system described in paragraph (2) or (3) of subsection (e).

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

''(A) in coordination with the Director, 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 a directive 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;

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

''(E) consult with the Director of the National Institute of Standards and Technology regarding any directive under this subsection that implements standards and guidelines developed by the National Institute of Standards and Technology;

''(F) ensure that directives issued under this subsection do not conflict with the standards and guidelines issued under section 11331 of title 40;

''(G) consider any applicable standards or guidelines developed by the National Institute of Standards and issued by the Secretary of Commerce under section 11331 of title 40; and

''(H) not later than February 1 of each year, submit to the appropriate congressional committees a report regarding the specific actions the Secretary has taken pursuant to paragraph (1)(A).

''(3) IMMINENT THREATS.—

''(A) IN GENERAL.—Notwithstanding section 3554, 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 for the purpose of ensuring the security of the information or information system or other agency information systems, if—

''(i) the Secretary determines there is an imminent threat to agency information systems;

''(ii) the Secretary determines a directive under subsection (b)(2)(C) or paragraph (1)(A) is not reasonably likely to result in a timely response to the threat;

''(iii) the Secretary determines the risk posed by the imminent threat outweighs any adverse consequences reasonably expected to result from the use of protective capabilities under the control of the Secretary;

''(iv) the Secretary provides prior notice to the Director, and the head and chief information officer (or equivalent official) of each agency to which specific actions will be taken pursuant to subparagraph (A), and notifies the appropriate congressional committees and authorizing committees of each such agencies within seven days of taking an action under this subsection of—

''(I) any action taken under this subsection; and

''(II) the reasons for and duration and nature of the action;

''(v) the action of the Secretary is consistent with applicable law; and

''(vi) the Secretary authorizes the use of protective capabilities in accordance with the advance procedures established under subparagraph (C).

''(B) LIMITATION ON DELEGATION.—The authority under this subsection may not be delegated by the Secretary.

''(C) ADVANCE PROCEDURES.—The Secretary shall, in coordination with the Director, and in consultation with the heads of Federal agencies, establish procedures governing the circumstances under which the Secretary may authorize the use of protective capabilities subparagraph (A). The Secretary shall submit the procedures to Congress.

''(4) LIMITATION.—The Secretary may direct or authorize lawful action or protective capability under this subsection only to—

''(A) protect agency information from unauthorized access, use, disclosure, disruption, modification, or destruction; or

''(B) require the remediation of or protect against identified information security risks with respect to—

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

''(ii) that portion of an information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

''(i) ANNUAL REPORT TO CONGRESS.—Not later than February 1 of each year, the Director shall submit to the appropriate congressional committees a report regarding the specific actions the Director has taken pursuant to subsection (a)(5), including any actions taken pursuant to section 11303(b)(5) of title 40.

''(j) APPROPRIATE CONGRESSIONAL COMMITTEES DEFINED.—In this section, the term 'appropriate congressional committees' means—

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

''(2) the Committee on Appropriations, the Committee on Homeland Security, the Committee on Oversight and Government Reform, and the Committee on Science, Space, and Technology of the House of Representatives.''.

(b) CONFORMING AMENDMENT.—Section 3554(a)(1)(B) of title 44, United States Code, is amended—

(1) in clause (iii), by striking ''and'' at the end; and

(2) by adding at the end the following:

''(v) emergency directives issued by the Secretary under section 3553(h); and''.

TITLE III—FEDERAL CYBERSECURITY WORKFORCE ASSESSMENT

SEC. 301. SHORT TITLE.

This title may be cited as the ''Federal Cybersecurity Workforce Assessment Act''.

SEC. 302. DEFINITIONS.

In this title:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Armed Services of the Senate;

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

(C) the Select Committee on Intelligence of the Senate;

(D) the Committee on Armed Services in the House of Representatives;

(E) the Committee on Homeland Security of the House of Representatives;

(F) the Committee on Oversight and Government Reform of the House of Representatives; and

(G) the Permanent Select Committee on Intelligence of the House of Representatives.

(2) DIRECTOR.—The term ''Director'' means the Director of the Office of Personnel Management.

(3) ROLES.—The term ''roles'' has the meaning given the term in the National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework.

SEC. 303. NATIONAL CYBERSECURITY WORKFORCE MEASUREMENT INITIATIVE.

(a) IN GENERAL.—The head of each Federal agency shall—

(1) identify all positions within the agency that require the performance of cybersecurity or other cyber-related functions; and

(2) assign the corresponding employment code, which shall be added to the National Initiative for Cybersecurity Education's National Cybersecurity Workforce Framework, in accordance with subsection (b).

(b) EMPLOYMENT CODES.—

(1) PROCEDURES.—

(A) CODING STRUCTURE.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Commerce, acting through the National Institute of Standards and Technology, shall update the National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework to include a corresponding coding structure.

(B) IDENTIFICATION OF CIVILIAN CYBER PERSONNEL.—Not later than 9 months after the date of enactment of this Act, the Director, in coordination with the Director of National Intelligence, shall establish procedures to implement the National Initiative for Cybersecurity Education's coding structure to identify all Federal civilian positions that require the performance of information technology, cybersecurity, or other cyber-related functions.

(C) IDENTIFICATION OF NONCIVILIAN CYBER PERSONNEL.—Not later than 18 months after the date of enactment of this Act, the Secretary of Defense shall establish procedures to implement the National Initiative for Cybersecurity Education's coding structure to identify all Federal noncivilian positions that require the performance of information technology, cybersecurity, or other cyber-related functions.

(D) BASELINE ASSESSMENT OF EXISTING CYBERSECURITY WORKFORCE.—Not later than 3 months after the date on which the procedures are developed under subparagraphs (B) and (C), respectively, the head of each Federal agency shall submit to the appropriate congressional committees of jurisdiction a report that identifies—

(i) the percentage of personnel with information technology, cybersecurity, or other cyber-related job functions who currently hold the appropriate industry-recognized certifications as identified in the National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework;

(ii) the level of preparedness of other civilian and non-civilian cyber personnel without existing credentials to take certification exams; and

(iii) a strategy for mitigating any gaps identified in clause (i) or (ii) with the appropriate training and certification for existing personnel.

(E) PROCEDURES FOR ASSIGNING CODES.—Not later than 3 months after the date on which the procedures are developed under subparagraphs (B) and (C), respectively, the head of each Federal agency shall establish procedures—

(i) to identify all encumbered and vacant positions with information technology, cybersecurity, or other cyber-related functions (as defined in the National Initiative for Cybersecurity Education's coding structure); and

(ii) to assign the appropriate employment code to each such position, using agreed standards and definitions.

(2) CODE ASSIGNMENTS.—Not later than 1 year after the date after the procedures are established under paragraph (1)(E), the head of each Federal agency shall complete assignment of the appropriate employment code to each position within the agency with information technology, cybersecurity, or other cyber-related functions.

(c) PROGRESS REPORT.—Not later than 180 days after the date of enactment of this Act, the Director shall submit a progress report on the implementation of this section to the appropriate congressional committees.

SEC. 304. IDENTIFICATION OF CYBER-RELATED ROLES OF CRITICAL NEED.

(a) IN GENERAL.—Beginning not later than 1 year after the date on which the employment codes are assigned to employees pursuant to section 203(b)(2), and annually through 2022, the head of each Federal agency, in consultation with the Director and the Secretary of Homeland Security, shall—

(1) identify information technology, cybersecurity, or other cyber-related roles of critical need in the agency's workforce; and

(2) submit a report to the Director that—

(A) describes the information technology, cybersecurity, or other cyber-related roles identified under paragraph (1); and

(B) substantiates the critical need designations.

(b) GUIDANCE.—The Director shall provide Federal agencies with timely guidance for identifying information technology, cybersecurity, or other cyber-related roles of critical need, including—

(1) current information technology, cybersecurity, and other cyber-related roles with acute skill shortages; and

(2) information technology, cybersecurity, or other cyber-related roles with emerging skill shortages.

(c) CYBERSECURITY NEEDS REPORT.—Not later than 2 years after the date of the enactment of this Act, the Director, in consultation with the Secretary of Homeland Security, shall—

(1) identify critical needs for information technology, cybersecurity, or other cyber-related workforce across all Federal agencies; and

(2) submit a progress report on the implementation of this section to the appropriate congressional committees.

SEC. 305. GOVERNMENT ACCOUNTABILITY OFFICE STATUS REPORTS.

The Comptroller General of the United States shall—

(1) analyze and monitor the implementation of sections 203 and 204; and

(2) not later than 3 years after the date of the enactment of this Act, submit a report to the appropriate congressional committees that describes the status of such implementation.

TITLE IV—OTHER CYBER MATTERS

SEC. 401. STUDY ON MOBILE DEVICE SECURITY.

(a) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Secretary of Homeland Security shall—

(1) complete a study on threats relating to the security of the mobile devices of the Federal Government; and

(2) submit an unclassified report to Congress, with a classified annex if necessary, that contains the findings of such study, the recommendations developed under paragraph (3) of subsection (b), the deficiencies, if any, identified under (4) of such subsection, and the plan developed under paragraph (5) of such subsection.

(b) MATTERS STUDIED.—In carrying out the study under subsection (a)(1), the Secretary shall—

(1) assess the evolution of mobile security techniques from a desktop-centric approach, and whether such techniques are adequate to meet current mobile security challenges;

(2) assess the effect such threats may have on the cybersecurity of the information systems and networks of the Federal Government (except for national security systems or the information systems and networks of the Department of Defense and the intelligence community);

(3) develop recommendations for addressing such threats based on industry standards and best practices;

(4) identify any deficiencies in the current authorities of the Secretary that may inhibit the ability of the Secretary to address mobile device security throughout the Federal Government (except for national security systems and the information systems and networks of the Department of Defense and intelligence community); and

(5) develop a plan for accelerated adoption of secure mobile device technology by the Department of Homeland Security.

(c) INTELLIGENCE COMMUNITY DEFINED.—In this section, the term ''intelligence community'' has the meaning given such term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

SEC. 402. DEPARTMENT OF STATE INTERNATIONAL CYBERSPACE POLICY STRATEGY.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Secretary of State shall produce a comprehensive strategy relating to United States international policy with regard to cyberspace.

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

(1) A review of actions and activities undertaken by the Secretary of State to date to support the goal of the President's International Strategy for Cyberspace, released in May 2011, to ''work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation.''.

(2) A plan of action to guide the diplomacy of the Secretary of State, with regard to foreign countries, including conducting bilateral and multilateral activities to develop the norms of responsible international behavior in cyberspace, and status review of existing discussions in multilateral fora to obtain agreements on international norms in cyberspace.

(3) A review of the alternative concepts with regard to international norms in cyberspace offered by foreign countries that are prominent actors, including China, Russia, Brazil, and India.

(4) A detailed description of threats to United States national security in cyberspace from foreign countries, state-sponsored actors, and private actors to Federal and private sector infrastructure of the United States, intellectual property in the United States, and the privacy of citizens of the United States.

(5) A review of policy tools available to the President to deter foreign countries, state-sponsored actors, and private actors, including those outlined in Executive Order 13694, released on April 1, 2015.

(6) A review of resources required by the Secretary, including the Office of the Coordinator for Cyber Issues, to conduct activities to build responsible norms of international cyber behavior.

(c) CONSULTATION.—In preparing the strategy required by subsection (a), the Secretary of State shall consult, as appropriate, with other agencies and departments of the United States and the private sector and nongovernmental organizations in the United States with recognized credentials and expertise in foreign policy, national security, and cybersecurity.

(d) FORM OF STRATEGY.—The strategy required by subsection (a) shall be in unclassified form, but may include a classified annex.

(e) AVAILABILITY OF INFORMATION.—The Secretary of State shall—

(1) make the strategy required in subsection (a) available the public; and

(2) brief the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives on the strategy, including any material contained in a classified annex.

SEC. 403. APPREHENSION AND PROSECUTION OF INTERNATIONAL CYBER CRIMINALS.

(a) INTERNATIONAL CYBER CRIMINAL DEFINED.—In this section, the term ''international cyber criminal'' means an individual—

(1) who is believed to have committed a cybercrime or intellectual property crime against the interests of the United States or the citizens of the United States; and

(2) for whom—

(A) an arrest warrant has been issued by a judge in the United States; or

(B) an international wanted notice (commonly referred to as a ''Red Notice'') has been circulated by Interpol.

(b) CONSULTATIONS FOR NONCOOPERATION.—The Secretary of State, or designee, shall consult with the appropriate government official of each country from which extradition is not likely, due to the lack of an extradition treaty with the United States or other reasons, in which one or more international cyber criminals are physically present to determine what actions the government of such country has taken—

(1) to apprehend and prosecute such criminals; and

(2) to prevent such criminals from carrying out cybercrimes or intellectual property crimes against the interests of the United States or its citizens.

(c) ANNUAL REPORT.—

(1) IN GENERAL.—The Secretary of State shall submit to the appropriate congressional committees an annual report that includes—

(A) the number of international cyber criminals located in other countries, disaggregated by country, and indicating from which countries extradition is not likely due to the lack of an extradition treaty with the United States or other reasons;

(B) the nature and number of significant discussions by an official of the Department of State on ways to thwart or prosecute international cyber criminals with an official of another country, including the name of each such country; and

(C) for each international cyber criminal who was extradited to the United States during the most recently completed calendar year—

(i) his or her name;

(ii) the crimes for which he or she was charged;

(iii) his or her previous country of residence; and

(iv) the country from which he or she was extradited into the United States.

(2) FORM.—The report required by this subsection shall be in unclassified form to the maximum extent possible, but may include a classified annex.

(3) APPROPRIATE CONGRESSIONAL COMMITTEES.—For purposes of this subsection, the term ''appropriate congressional committees'' means—

(A) the Committee on Foreign Relations, the Committee on Appropriations, the Committee on Homeland Security and Governmental Affairs, the Committee on Banking, Housing, and Urban Affairs, the Select Committee on Intelligence, and the Committee on the Judiciary of the Senate; and

(B) the Committee on Foreign Affairs, the Committee on Appropriations, the Committee on Homeland Security, the Committee on Financial Services, the Permanent Select Committee on Intelligence, and the Committee on the Judiciary of the House of Representatives.

SEC. 404. ENHANCEMENT OF EMERGENCY SERVICES.

(a) COLLECTION OF DATA.—Not later than 90 days after the date of enactment of this Act, the Secretary of Homeland Security, acting through the National Cybersecurity and Communications Integration Center, in coordination with appropriate Federal entities and the Director for Emergency Communications, shall establish a process by which a Statewide Interoperability Coordinator may report data on any cybersecurity risk or incident involving any information system or network used by emergency response providers (as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101)) within the State.

(b) ANALYSIS OF DATA.—Not later than 1 year after the date of enactment of this Act, the Secretary of Homeland Security, acting through the Director of the National Cybersecurity and Communications Integration Center, in coordination with appropriate entities and the Director for Emergency Communications, and in consultation with the Director of the National Institute of Standards and Technology, shall conduct integration and analysis of the data reported under subsection (a) to develop information and recommendations on security and resilience measures for any information system or network used by State emergency response providers.

(c) BEST PRACTICES.—

(1) IN GENERAL.—Using the results of the integration and analysis conducted under subsection (b), and any other relevant information, the Director of the National Institute of Standards and Technology shall, on an ongoing basis, facilitate and support the development of methods for reducing cybersecurity risks to emergency response providers using the process described in section 2(e) of the National Institute of Standards and Technology Act (15 U.S.C. 272(e)).

(2) REPORT.—The Director of the National Institute of Standards and Technology shall submit a report to Congress on the methods developed under paragraph (1) and shall make such report publically available on the website of the National Institute of Standards and Technology.

(d) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to—

(1) require a State to report data under subsection (a); or

(2) require an entity to—

(A) adopt a recommended measure developed under subsection (b); or

(B) follow the best practices developed under subsection (c).

SEC. 405. IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY.

(a) DEFINITIONS.—In this section:

(1) BUSINESS ASSOCIATE.—The term ''business associate'' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(2) COVERED ENTITY.—The term ''covered entity'' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(3) HEALTH CARE CLEARINGHOUSE; HEALTH CARE PROVIDER; HEALTH PLAN.—The terms ''health care clearinghouse'', ''health care provider'', and ''health plan'' have the meanings given the terms in section 160.103 of title 45, Code of Federal Regulations.

(4) HEALTH CARE INDUSTRY STAKEHOLDER.—The term ''health care industry stakeholder'' means any—

(A) health plan, health care clearinghouse, or health care provider;

(B) patient advocate;

(C) pharmacist;

(D) developer of health information technology;

(E) laboratory;

(F) pharmaceutical or medical device manufacturer; or

(G) additional stakeholder the Secretary determines necessary for purposes of subsection (d)(1), (d)(3), or (e).

(5) SECRETARY.—The term ''Secretary'' means the Secretary of Health and Human Services.

(b) REPORT.—Not later than 1 year after the date of enactment of this Act, the Secretary shall submit, to the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Energy and Commerce of the House of Representatives, a report on the preparedness of the health care industry in responding to cybersecurity threats.

(c) CONTENTS OF REPORT.—With respect to the internal response of the Department of Health and Human Services to emerging cybersecurity threats, the report shall include—

(1) a clear statement of the official within the Department of Health and Human Services to be responsible for leading and coordinating efforts of the Department regarding cybersecurity threats in the health care industry; and

(2) a plan from each relevant operating division and subdivision of the Department of Health and Human Services on how such division or subdivision will address cybersecurity threats in the health care industry, including a clear delineation of how each such division or subdivision will divide responsibility among the personnel of such division or subdivision and communicate with other such divisions and subdivisions regarding efforts to address such threats.

(d) HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE.—

(1) IN GENERAL.—Not later than 60 days after the date of enactment of this Act, the Secretary, in consultation with the Secretary of Homeland Security, shall convene health care industry stakeholders, cybersecurity experts, and any Federal agencies or entities the Secretary determines appropriate to establish a task force to—

(A) analyze how industries, other than the health care industry, have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries;

(B) analyze challenges and barriers private entities (notwithstanding section 2(15)(B),

excluding any State, tribal, or local government) in the health care industry face securing themselves against cyber attacks;

(C) review challenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record;

(D) provide the Secretary with information to disseminate to health care industry stakeholders for purposes of improving their preparedness for, and response to, cybersecurity threats affecting the health care industry;

(E) establish a plan for creating a single system for the Federal Government to share information on actionable intelligence regarding cybersecurity threats to the private sector in near real time, at no cost to the recipients of such information, including which Federal agency or other entity may be best suited to be the central conduit to facilitate the sharing of such information; and

(F) report to Congress on the findings and recommendations of the task force regarding carrying out subparagraphs (A) through (E).

(2) TERMINATION.—The task force established under this subsection shall terminate on the date that is 1 year after the date of enactment of this Act.

(3) DISSEMINATION.—Not later than 60 days after the termination of the task force established under this subsection, the Secretary shall disseminate the information described in paragraph (1)(D) to health care industry stakeholders in accordance with such paragraph.

(e) CYBERSECURITY FRAMEWORK.—The Secretary shall establish, through a collaborative process with the Secretary of Homeland Security, health care industry stakeholders, the National Institute of Standards and Technology, and any Federal agency or entity the Secretary determines appropriate, a single, voluntary, national health-specific cybersecurity framework that—

(1) establishes a common set of security practices and standards that specifically pertain to a range of health care organizations;

(2) supports voluntary adoption and implementation efforts to improve safeguards to address cybersecurity threats; and

(3) is consistently updated and applicable to the range of health care organizations described in paragraph (1).

SEC. 406. FEDERAL COMPUTER SECURITY.

(a) DEFINITIONS.—In this section:

(1) COVERED SYSTEM.—The term ''covered system'' shall mean a national security system as defined in section 11103 of title 40, United States Code, or a Federal computer system that provides access to personally identifiable information.

(2) COVERED AGENCY.—The term ''covered agency'' means an agency that operates a covered system.

(3) LOGICAL ACCESS CONTROL.—The term ''logical access control'' means a process of granting or denying specific requests to obtain and use information and related information processing services.

(4) MULTI-FACTOR LOGICAL ACCESS CONTROLS.—The term ''multi-factor logical access controls'' means a set of not less than 2 of the following logical access controls:

(A) Information that is known to the user, such as a password or personal identification number.

(B) An access device that is provided to the user, such as a cryptographic identification device or token.

(C) A unique biometric characteristic of the user.

(5) PRIVILEGED USER.—The term ''privileged user'' means a user who, by virtue of function or seniority, has been allocated powers within a covered system, which are significantly greater than those available to the majority of users.

(b) INSPECTOR GENERAL REPORTS ON COVERED SYSTEMS.—

(1) IN GENERAL.—Not later than 240 days after the date of enactment of this Act, the Inspector General of each covered agency shall each submit to each Comptroller General of the United States and the appropriate committees of jurisdiction in the Senate and the House of Representatives a report, which shall include information collected from the covered agency for the contents described in paragraph (2) regarding the Federal computer systems of the covered agency.

(2) CONTENTS.—The report submitted by each Inspector General of a covered agency under paragraph (1) shall include, with respect to the covered agency, the following:

(A) A description of the logical access standards used by the covered agency to access a covered system, including—

(i) in aggregate, a list and description of logical access controls used to access such a covered system; and

(ii) whether the covered agency is using multi-factor logical access controls to access such a covered system.

(B) A description of the logical access controls used by the covered agency to govern access to covered systems by privileged users.

(C) If the covered agency does not use logical access controls or multi-factor logical access controls to access a covered system, a description of the reasons for not using such logical access controls or multi-factor logical access controls.

(D) A description of the following data security management practices used by the covered agency:

(i) The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.

(ii) What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including—

(I) data loss prevention capabilities; or

(II) digital rights management capabilities.

(iii) A description of how the covered agency is using the capabilities described in clause (ii).

(iv) If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.

(E) A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the data security management practices described in subparagraph (D).

(3) EXISTING REVIEW.—The reports required under this subsection may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the covered agency, and may be submitted as part of another report, including the report required under section 3555 of title 44, United States Code.

(4) CLASSIFIED INFORMATION.—Reports submitted under this subsection shall be in unclassified form, but may include a classified annex.

(c) GAO ECONOMIC ANALYSIS AND REPORT ON FEDERAL COMPUTER SYSTEMS.—

(1) REPORT.—Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall submit to Congress a report examining, including an economic analysis of, any impediments to agency use of effective security software and security devices.

(2) CLASSIFIED INFORMATION.—A report submitted under this subsection shall be in unclassified form, but may include a classified annex.

SEC. 407. STRATEGY TO PROTECT CRITICAL INFRASTRUCTURE AT GREATEST RISK.

(a) DEFINITIONS.—In this section:

(1) APPROPRIATE AGENCY.—The term ''appropriate agency'' means, with respect to a covered entity—

(A) except as provided in subparagraph (B), the applicable sector-specific agency; or

(B) in the case of a covered entity that is regulated by a Federal entity, such Federal entity.

(2) APPROPRIATE AGENCY HEAD.—The term ''appropriate agency head'' means, with respect to a covered entity, the head of the appropriate agency.

(3) COVERED ENTITY.—The term ''covered entity'' means an entity identified under subsection (b).

(4) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Select Committee on Intelligence of the Senate;

(B) the Permanent Select Committee on Intelligence of the House of Representatives;

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

(D) the Committee on Homeland Security of the House of Representatives;

(E) the Committee on Energy and Natural Resources of the Senate; and

(F) the Committee on Energy and Commerce of the House of Representatives;

(5) SECRETARY.—The term ''Secretary'' means the Secretary of the Department of Homeland Security

(b) IDENTIFICATION OF CRITICAL INFRASTRUCTURE AT GREATEST RISK REQUIRED.—No later than 60 days after the date of the enactment of this Act, the Secretary shall identify critical infrastructure entities where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

(c) STATUS OF EXISTING CYBER INCIDENT REPORTING.—

(1) IN GENERAL.—No later than 120 days after the date of the enactment of this Act, the Secretary, in conjunction with the appropriate agency head (as the case may be), shall submit to the appropriate congressional committees describing the extent to which each covered entity reports significant intrusions of information systems essential to the operation of critical infrastructure to the Department of Homeland Security or the appropriate agency head in a timely manner.

(2) FORM.—The report submitted under paragraph (1) may include a classified annex.

(d) MITIGATION STRATEGY REQUIRED FOR CRITICAL INFRASTRUCTURE AT GREATEST RISK.—

(1) IN GENERAL.—No later than 180 days after the date of the enactment of this Act, the Secretary, in conjunction with the appropriate agency head (as the case may be), shall conduct an assessment and develop a strategy that addresses each of the covered entities, to ensure that, to the greatest extent feasible, a cyber security incident affecting such entity would no longer reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.

(2) ELEMENTS.—The strategy submitted by the Secretary with respect to a covered entity intrusion shall include the following:

(A) An assessment of whether each entity should be required to report cyber security incidents.

(B) A description of any identified security gaps that must be addressed.

(C) Additional statutory authority necessary to reduce the likelihood that a cyber incident could cause catastrophic regional or

national effects on public health or safety, economic security, or national security.

(3) SUBMITTAL.—The Secretary shall submit to the appropriate congressional committees the assessment and strategy required by paragraph (1).

(4) FORM.—The assessment and strategy submitted under paragraph (3) may each include a classified annex.

(e) SENATE OF CONGRESS.—To the extent that the Secretary proposes to require the reporting of significant cyber intrusions of any covered entity pursuant to a recommendation identified in subsection (d) it is the Sense of Congress that—

(1) the Secretary should ensure that the policies and procedures established for such reporting incorporate, to the greatest extent practicable, processes, roles, and responsibilities of appropriate agencies and entities, including sector specific information sharing and analysis centers, that were in effect on the day before the date of the enactment of this Act;

(2) no cause of action should lie or be maintained in any court against a covered entity, and such action should be promptly dismissed for sharing information with the Secretary or the appropriate agency head for sharing such information;

(3) the Secretary or appropriate agency head, as the case may be, should, under section 103 and to the greatest extent practicable, make available to any covered entity submitting a report such cyber threat indicators as the Secretary or appropriate agency head considers appropriate; and

(4) the Secretary or the appropriate agency head (as the case may be) should take such actions as the Secretary or the appropriate agency head (as the case may be) considers appropriate to protect from disclosure the identity of the covered entity.

SA 2717. Mr. UDALL (for himself, Mrs. SHAHEEN, Mr. TESTER, and Mr. MERKLEY) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

SEC. 11. EXTENSION OF LAND AND WATER CONSERVATION FUND.

Section 200302 of title 54, United States Code, is amended—

(1) in subsection (b), in the matter preceding paragraph (1), by striking ''September 30, 2015'' and inserting ''December 11, 2015''; and

(2) in subsection (c)(1), by striking ''September 30, 2015'' and inserting ''December 11, 2015''.

SA 2718. Mr. UDALL (for himself, Mrs. SHAHEEN, Mr. TESTER, and Mr. MERKLEY) submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. PERMANENT REAUTHORIZATION OF LAND AND WATER CONSERVATION FUND.

(a) IN GENERAL.—Section 200302 of title 54, United States Code, is amended—

(1) in subsection (b), in the matter preceding paragraph (1), by striking ''During the period ending September 30, 2015, there'' and inserting ''There''; and

(2) in subsection (c)(1), by striking ''through September 30, 2015''.

(b) PUBLIC ACCESS.—Section 200306 of title 54, United States Code, is amended by adding at the end the following:

''(c) PUBLIC ACCESS.—Not less than 1.5 percent of amounts made available for expenditure in any fiscal year under section 200303, or $10,000,000, whichever is greater, shall be used for projects that secure recreational public access to existing Federal public land for hunting, fishing, and other recreational purposes.''.

SA 2719. Mr. ALEXANDER submitted an amendment intended to be proposed by him to the bill S. 754, to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. ___. IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY.

(a) DEFINITIONS.—In this section:

(1) BUSINESS ASSOCIATE.—The term ''business associate'' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(2) COVERED ENTITY.—The term ''covered entity'' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

(3) HEALTH CARE CLEARINGHOUSE; HEALTH CARE PROVIDER; HEALTH PLAN.—The terms ''health care clearinghouse'', ''health care provider'', and ''health plan'' have the meanings given the terms in section 160.103 of title 45, Code of Federal Regulations.

(4) HEALTH CARE INDUSTRY STAKEHOLDER.—The term ''health care industry stakeholder'' means any—

(A) health plan, health care clearinghouse, or health care provider;

(B) patient advocate;

(C) pharmacist;

(D) developer of health information technology;

(E) laboratory;

(F) pharmaceutical or medical device manufacturer; or

(G) additional stakeholder the Secretary determines necessary for purposes of subsection (d)(1), (d)(3), or (e).

(5) SECRETARY.—The term ''Secretary'' means the Secretary of Health and Human Services.

(b) REPORT.—Not later than 1 year after the date of enactment of this Act, the Secretary shall submit, to the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Energy and Commerce of the House of Representatives, a report on the preparedness of the health care industry in responding to cybersecurity threats.

(c) CONTENTS OF REPORT.—With respect to the internal response of the Department of Health and Human Services to emerging cybersecurity threats, the report shall include—

(1) a clear statement of the official within the Department of Health and Human Services to be responsible for leading and coordinating efforts of the Department regarding cybersecurity threats in the health care industry; and

(2) a plan from each relevant operating division and subdivision of the Department of Health and Human Services on how such division or subdivision will address cybersecurity threats in the health care industry, including a clear delineation of how each such division or subdivision will divide responsibility among the personnel of such division or subdivision and communicate with other such divisions and subdivisions regarding efforts to address such threats.

(d) HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE.—

(1) IN GENERAL.—Not later than 60 days after the date of enactment of this Act, the Secretary, in consultation with the Secretary of Homeland Security, shall convene health care industry stakeholders, cybersecurity experts, and any Federal agencies or entities the Secretary determines appropriate to establish a task force to—

(A) analyze how industries, other than the health care industry, have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries;

(B) analyze challenges and barriers private entities (notwithstanding section 2(15)(B), excluding any State, tribal, or local government) in the health care industry face securing themselves against cyber attacks;

(C) review challenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record;

(D) provide the Secretary with information to disseminate to health care industry stakeholders for purposes of improving their preparedness for, and response to, cybersecurity threats affecting the health care industry;

(E) establish a plan for creating a single system for the Federal Government to share information on actionable intelligence regarding cybersecurity threats to the private sector in near real time, at no cost to the recipients of such information, including which Federal agency or other entity may be best suited to be the central conduit to facilitate the sharing of such information; and

(F) report to Congress on the findings and recommendations of the task force regarding carrying out subparagraphs (A) through (E).

(2) TERMINATION.—The task force established under this subsection shall terminate on the date that is 1 year after the date of enactment of this Act.

(3) DISSEMINATION.—Not later than 60 days after the termination of the task force established under this subsection, the Secretary shall disseminate the information described in paragraph (1)(D) to health care industry stakeholders in accordance with such paragraph.

(e) CYBERSECURITY FRAMEWORK.—The Secretary shall establish, through a collaborative process with the Secretary of Homeland Security, health care industry stakeholders, the National Institute of Standards and Technology, and any Federal agency or entity the Secretary determines appropriate, a single, voluntary, national health-specific cybersecurity framework that—

(1) establishes a common set of security practices and standards that specifically pertain to a range of health care organizations;

(2) supports voluntary adoption and implementation efforts to improve safeguards to address cybersecurity threats; and

(3) is consistently updated and applicable to the range of health care organizations described in paragraph (1).

AUTHORITY FOR COMMITTEES TO MEET

COMMITTEE ON ENERGY AND NATURAL RESOURCES

Mr. TOOMEY. Mr. President, I ask unanimous consent that the Committee on Energy and Natural Resources be authorized to meet during