resolution approving the renewal of import restrictions contained in the Burmese Freedom and Democracy Act of 2003.

At the request of Mr. MCCONNELL, the names of the Senator from Arizona (Mr. KYL) and the Senator from Texas (Mrs. HUTCHISON) were added as cosponsors of S.J. Res. 17, supra.

S. RES. 175

At the request of Mrs. SHAHEEN, the name of the Senator from Indiana (Mr. LUGAR) was added as a cosponsor of S. Res. 175, a resolution expressing the sense of the Senate with respect to ongoing violations of the territorial integrity and sovereignty of Georgia and the importance of a peaceful and just resolution to the conflict within Georgia's internationally recognized borders.

S. RES. 185

At the request of Mr. CARDIN, the names of the Senator from South Dakota (Mr. JOHNSON), the Senator from Nebraska (Mr. JOHANNS), the Senator from Nevada (Mr. HELLER), the Senator from Colorado (Mr. BENNET), the Senator from Mississippi (Mr. WICKER), the Senator from Georgia (Mr. ISAKSON), the Senator from New Hampshire (Mrs. SHAHEEN), the Senator from Montana (Mr. BAUCUS) and the Senator from Georgia (Mr. CHAMBLISS) were added as cosponsors of S. Res. 185, a resolution reaffirming the commitment of the United States to a negotiated settlement of the Israeli-Palestinian conflict through direct Israeli-Palestinian negotiations, reaffirming opposition to the inclusion of Hamas in a unity government unless it is willing to accept peace with Israel and renounce violence, and declaring that Palestinian efforts to gain recognition of a state outside direct negotiations demonstrates absence of a good faith commitment to peace negotiations, and will have implications for continued United States aid.

S. RES. 202

At the request of Mr. CONRAD, the names of the Senator from Maine (Ms. SNOWE) and the Senator from Minnesota (Mr. FRANKEN) were added as cosponsors of S. Res. 202, a resolution designating June 27, 2011, as ''National Post-Traumatic Stress Disorder Awareness Day''.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. WYDEN (for himself, Mr. CRAPO, Mr. RISCH, and Mr. MERKLEY):

S. 1149. A bill to expand geothermal production, and for other purposes; to the Committee on Energy and Natural Resources.

Mr. WYDEN. Mr. President, today Sen. CRAPO, Sen. RISCH, Sen. MERKLEY, and I are introducing the Geothermal Production Expansion Act of 2011. The bill is aimed at making improvements to the Geothermal Steam Act and is very similar to legislation introduced in the 111th Congress as S. 3993.

Both bills contain identical provisions to allow the Secretary of the Interior to lease a limited amount of public land adjacent to existing geothermal property at fair market value. The reason for this change is to allow the rapid expansion of already identified geothermal resources without the additional delays of competitive leasing and without opening up those adjacent properties to speculative bidders who have no interest in actually developing the resource, only in extracting as much money as they can from the existing geothermal lease holder. Current lease holders are understandably reluctant to nominate adjacent lands to proven resources for competitive leasing because doing so would immediately signal the value of those adjacent properties. As a result, existing geothermal developers will likely not realize the full potential of the geothermal energy resources that they have spent millions of dollars exploring, proving, and developing without these changes. And, the Treasury will not realize the economic value of those adjacent parcels, which go unleased and undeveloped as a result. For these reasons, the bill has the strong support of the Geothermal Energy Association.

I want to emphasize that this bill is not a giveaway. The amount of land that can be leased non-competitively is limited to less than 640 acres per lease. It can only be leased where there are already proven resources and thus more likely than not to increase overall Federal royalties paid to the Treasury as the adjacent parcels are incorporated into the developer's geothermal energy project. Third, the bidder must pay fair market value for the lease as determined by the Interior Department. Finally, this bill contains an additional provision, which was not included in the prior version, which will significantly increase the annual rental payments for the newly acquired adjacent land in order to ensure that the bill comes as close as possible to full economic recovery for the taxpayers.

Current law sets two different annual rental payment levels for geothermal leases. These are amounts that the lease-holder pays per year for every acre held in lease. The rental rate for non-competitive leases is $1 per acre per year. The rate for competitive leases begins at $2 per acre for the first year and increases to $3 for the next 9 years. The sole difference between the bill introduced in the prior Congress and the bill being introduced today is that the version being introduced today treats the new, adjacent lease as a competitive lease for determining the annual rental even though it is being acquired as a non-competitive lease. This will have the clear effect of raising the annual rental payments on the newly acquired adjacent lands to the higher rate of $2 and then $3 per acre and increase revenue to the Treasury. This change underscores our intent, as sponsors of the bill, to ensure that the result of these changes in the Geothermal Steam Act is truly to increase geothermal energy production on Federal lands without any overall loss of revenue to the taxpayers from noncompetitive award of these adjacent lands.

Geothermal energy is, by definition, a domestic renewable energy resource with enormous potential, but developers face high costs and economic risks of finding the right location to extract energy. These changes will help ensure that once those resources have been proven on Federal lands, they can be fully developed as quickly and efficiently as possible.

Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the text of the bill was ordered to be printed in the RECORD, as follows:

S. 1149

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Geothermal Production Expansion Act of 2011''.

SEC. 2. FINDINGS.

Congress finds that—

(1) it is in the best interest of the United States to develop clean renewable geothermal energy;

(2) development of that energy should be promoted on appropriate Federal land;

(3) under the Energy Policy Act of 2005 (42 U.S.C. 15801 et seq.), the Bureau of Land Management is authorized to issue 3 different types of noncompetitive leases for production of geothermal energy on Federal land, including—

(A) noncompetitive geothermal leases to mining claim holders that have a valid operating plan;

(B) direct use leases; and

(C) leases on parcels that do not sell at a competitive auction;

(4) Federal geothermal energy leasing activity should be directed toward persons seeking to develop the land as opposed to persons seeking to speculate on geothermal resources and artificially raising the cost of legitimate geothermal energy development;

(5) developers of geothermal energy on Federal land that have invested substantial capital and made high risk investments should be allowed to secure a discovery of geothermal energy resources; and

(6) successful geothermal development on Federal land will provide increased revenue to the Federal Government, with the payment of production royalties over decades.

SEC. 3. NONCOMPETITIVE LEASING OF ADJOINING AREAS FOR DEVELOPMENT OF GEOTHERMAL RESOURCES.

Section 4(b) of the Geothermal Steam Act of 1970 (30 U.S.C. 1003(b)) is amended by adding at the end the following:

''(4) ADJOINING LAND.—

''(A) DEFINITIONS.—In this paragraph:

''(i) FAIR MARKET VALUE PER ACRE.—The term 'fair market value per acre' means a dollar amount per acre that—

''(I) except as provided in this clause, shall be equal to the market value per acre as determined by the Secretary under regulations issued under this paragraph;

''(II) shall be determined by the Secretary with respect to a lease under this paragraph, by not later than the end of the 90-day period beginning on the date the Secretary receives an application for the lease; and

''(III) shall be not less than the greater of—

''(aa) 4 times the median amount paid per acre for all land leased under this Act during the preceding year; or

''(bb) $50.

''(ii) INDUSTRY STANDARDS.—The term 'industry standards' means the standards by which a qualified geothermal professional assesses whether downhole or flowing temperature measurements with indications of permeability are sufficient to produce energy from geothermal resources, as determined through flow or injection testing or measurement of lost circulation while drilling.

''(iii) QUALIFIED FEDERAL LAND.—The term 'qualified Federal land' means land that is otherwise available for leasing under this Act.

''(iv) QUALIFIED GEOTHERMAL PROFESSIONAL.—The term 'qualified geothermal professional' means an individual who is an engineer or geoscientist in good professional standing with at least 5 years of experience in geothermal exploration, development, or project assessment.

''(v) QUALIFIED LESSEE.—The term 'qualified lessee' means a person that may hold a geothermal lease under this Act (including applicable regulations).

''(vi) VALID DISCOVERY.—The term 'valid discovery' means a discovery of a geothermal resource by a new or existing slim hole or production well, that exhibits downhole or flowing temperature measurements with indications of permeability that are sufficient to meet industry standards.

''(B) AUTHORITY.—An area of qualified Federal land that adjoins other land for which a qualified lessee holds a legal right to develop geothermal resources may be available for a noncompetitive lease under this section to the qualified lessee at the fair market value per acre, if—

''(i) the area of qualified Federal land—

''(I) consists of not less than 1 acre and not more than 640 acres; and

''(II) is not already leased under this Act or nominated to be leased under subsection (a);

''(ii) the qualified lessee has not previously received a noncompetitive lease under this paragraph in connection with the valid discovery for which data has been submitted under clause (iii)(I); and

''(iii) sufficient geological and other technical data prepared by a qualified geothermal professional has been submitted by the qualified lessee to the applicable Federal land management agency that would lead individuals who are experienced in the subject matter to believe that—

''(I) there is a valid discovery of geothermal resources on the land for which the qualified lessee holds the legal right to develop geothermal resources; and

''(II) that thermal feature extends into the adjoining areas.

''(C) DETERMINATION OF FAIR MARKET VALUE.—

''(i) IN GENERAL.—The Secretary shall—

''(I) publish a notice of any request to lease land under this paragraph;

''(II) determine fair market value for purposes of this paragraph in accordance with procedures for making those determinations that are established by regulations issued by the Secretary;

''(III) provide to a qualified lessee and publish, with an opportunity for public comment for a period of 30 days, any proposed determination under this subparagraph of the fair market value of an area that the qualified lessee seeks to lease under this paragraph; and

''(IV) provide to the qualified lessee and any adversely affected party the opportunity to appeal the final determination of fair market value in an administrative proceeding before the applicable Federal land management agency, in accordance with applicable law (including regulations).

''(ii) LIMITATION ON NOMINATION.—After publication of a notice of request to lease land under this paragraph, the Secretary may not accept under subsection (a) any nomination of the land for leasing unless the request has been denied or withdrawn.

''(iii) ANNUAL RENTAL.—For purposes of section 5(a)(3), a lease awarded under this paragraph shall be considered a lease awarded in a competitive lease sale.

''(D) REGULATIONS.—Not later than 180 days after the date of enactment of the Geothermal Production Expansion Act of 2011, the Secretary shall issue regulations to carry out this paragraph.''.

By Mr. LEAHY (for himself, Mr. SCHUMER, Mr. CARDIN, and Mr. FRANKEN):

S. 1151. A bill to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information; to the Committee on the Judiciary.

Mr. LEAHY. Mr. President, today, I am pleased to reintroduce the Personal Data Privacy and Security Act. The recent and troubling data breaches at Sony, Epsilon and Lockheed Martin on U.S. Government computers is clear evidence that developing a comprehensive national strategy to protect data privacy and cybersecurity is one of the most challenging and important issues facing our Nation. The Personal Data Privacy and Security Act will help to meet this challenge, by better protecting Americans from the growing threats of data breaches and identity theft. I thank Senators SCHUMER and CARDIN for cosponsoring this important privacy legislation.

When I first introduced this bill six years ago, I had high hopes of bringing urgently needed data privacy reforms to the American people. Although the Judiciary Committee favorably reported this bill three times—in 2005, 2007, and again in 2009—the legislation languished on the Senate calendar.

While the Congress has waited to act, the dangers to our privacy, economic prosperity and national security posed by data breaches have not gone away. According to the Privacy Rights Clearinghouse, more than 533 million records have been involved in data security breaches since 2005. Just last week, Google announced that the Gmail accounts for hundreds of its users, including senior U.S. Government officials, have been hacked in an apparent state-sponsored cyberattack. As The Washington Post editorial board recently observed, ''[n]ow there is a need for legislative action. As the recent high-profile leaks of personal data at Google, Sony and the data-collecting company Epsilon suggest, this issue is a ticking bomb.''

In May, the Obama administration released several proposals to enhance cybersecurity, including a data breach proposal that adopts the carefully balanced framework of this bill. I am pleased that many of the sound privacy principles in this bill have been embraced by the President and his administration.

The Personal Data Privacy and Security Act requires that data brokers let consumers know what sensitive personal information they have about them, and to allow individuals to correct inaccurate information. The bill also requires that companies that have databases with sensitive personal information on Americans establish and implement data privacy and security programs.

The bill would also establish a single nationwide standard for data breach notification. The bill requires notice to consumers when their sensitive personal information has been compromised.

This bill also provides for tough criminal penalties for anyone who would intentionally and willfully conceal the fact that a data breach has occurred when the breach causes economic damage to consumers. The bill also includes the administration's recent proposal to update the Computer Fraud and Abuse Act, so that attempted computer hacking and conspiracy to commit computer hacking offenses are subject to the same criminal penalties, as the underlying offense.

Finally, the bill addresses the important issue of the Government's use of personal data by requiring that Federal agencies notify affected individuals when Government data breaches occur, and by placing privacy and security front and center when Federal agencies evaluate whether data brokers can be trusted with Government contracts that involve sensitive information about the American people.

Of course, no one has a monopoly on good ideas to solve the serious problems of identity theft and lax cybersecurity. But, this bill puts forth some meaningful solutions to this vexing problem.

I have drafted this bill after long and thoughtful consultation with many of the stakeholders on this issue, including the privacy, consumer protection and business communities. I have also consulted with the Departments of Justice and Homeland Security, and with the Federal Trade Commission. I have worked closely with other Senators, including Senators Feinstein and Schumer.

This is a comprehensive bill that not only deals with the need to provide Americans with notice when they have been victims of a data breach, but that also deals with the underlying problem of lax security and lack of accountability to help prevent data breaches from occurring in the first place. Enacting this comprehensive data privacy legislation remains one of my legislative priorities as Chairman of the Judiciary Committee.

This bill has always garnered strong bipartisan support. Protecting privacy

rights is of critical importance to all of us, regardless of party or ideology. I hope that all Senators will support this measure to better protect Americans' privacy.

Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the text of the bill was ordered to be printed in the RECORD, as follows:

S. 1151

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Personal Data Privacy and Security Act of 2011''.

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

SEC. 2. FINDINGS.

Congress finds that—

(1) databases of personally identifiable information are increasingly prime targets of hackers, identity thieves, rogue employees, and other criminals, including organized and sophisticated criminal operations;

(2) identity theft is a serious threat to the Nation's economic stability, homeland security, the development of e-commerce, and the privacy rights of Americans;

(3) over 9,300,000 individuals were victims of identity theft in America last year;

(4) security breaches are a serious threat to consumer confidence, homeland security, e-commerce, and economic stability;

(5) it is important for business entities that own, use, or license personally identifiable information to adopt reasonable procedures to ensure the security, privacy, and confidentiality of that personally identifiable information;

(6) individuals whose personal information has been compromised or who have been victims of identity theft should receive the necessary information and assistance to mitigate their damages and to restore the integrity of their personal information and identities;

(7) data brokers have assumed a significant role in providing identification, authentication, and screening services, and related data collection and analyses for commercial, nonprofit, and government operations;

(8) data misuse and use of inaccurate data have the potential to cause serious or irreparable harm to an individual's livelihood, privacy, and liberty and undermine efficient and effective business and government operations;

(9) there is a need to ensure that data brokers conduct their operations in a manner that prioritizes fairness, transparency, accuracy, and respect for the privacy of consumers;

(10) government access to commercial data can potentially improve safety, law enforcement, and national security; and

(11) because government use of commercial data containing personal information potentially affects individual privacy, and law enforcement and national security operations, there is a need for Congress to exercise oversight over government use of commercial data.

SEC. 3. DEFINITIONS.

In this Act, the following definitions shall apply:

(1) AGENCY.—The term ''agency'' has the same meaning given such term in section 551 of title 5, United States Code.

(2) AFFILIATE.—The term ''affiliate'' means persons related by common ownership or by corporate control.

(3) BUSINESS ENTITY.—The term ''business entity'' means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture established to make a profit, or nonprofit.

(4) IDENTITY THEFT.—The term ''identity theft'' means a violation of section 1028(a)(7) of title 18, United States Code.

(5) DATA BROKER.—The term ''data broker'' means a business entity which for monetary fees or dues regularly engages in the practice of collecting, transmitting, or providing access to sensitive personally identifiable information on more than 5,000 individuals who are not the customers or employees of that business entity or affiliate primarily for the purposes of providing such information to nonaffiliated third parties on an interstate basis.

(6) DATA FURNISHER.—The term ''data furnisher'' means any agency, organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or nonprofit that serves as a source of information for a data broker.

(7) ENCRYPTION.—The term ''encryption''—

(A) means the protection of data in electronic form, in storage or in transit, using an encryption technology that has been adopted by a widely accepted standards setting body or, has been widely accepted as an effective industry practice which renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; and

(B) includes appropriate management and safeguards of such cryptographic keys so as to protect the integrity of the encryption.

(8) PERSONAL ELECTRONIC RECORD.—

(A) IN GENERAL.—The term ''personal electronic record'' means data associated with an individual contained in a database, networked or integrated databases, or other data system that is provided by a data broker to nonaffiliated third parties and includes personally identifiable information about that individual.

(B) EXCLUSIONS.—The term ''personal electronic record'' does not include—

(i) any data related to an individual's past purchases of consumer goods; or

(ii) any proprietary assessment or evaluation of an individual or any proprietary assessment or evaluation of information about an individual.

(9) PERSONALLY IDENTIFIABLE INFORMATION.—The term ''personally identifiable information'' means any information, or compilation of information, in electronic or digital form that is a means of identification, as defined by section 1028(d)(7) of title 18, United States Code.

(10) PUBLIC RECORD SOURCE.—The term ''public record source'' means the Congress, any agency, any State or local government agency, the government of the District of Columbia and governments of the territories or possessions of the United States, and Federal, State or local courts, courts martial and military commissions, that maintain personally identifiable information in records available to the public.

(11) SECURITY BREACH.—

(A) IN GENERAL.—The term ''security breach'' means compromise of the security, confidentiality, or integrity of computerized data through misrepresentation or actions—

(i) that result in, or that there is a reasonable basis to conclude has resulted in—

(I) the unauthorized acquisition of sensitive personally identifiable information; and

(II) access to sensitive personally identifiable information that is for an unauthorized purpose, or in excess of authorization; and

(ii) which present a significant risk of harm or fraud to any individual.

(B) EXCLUSION.—The term ''security breach'' does not include—

(i) a good faith acquisition of sensitive personally identifiable information by a business entity or agency, or an employee or agent of a business entity or agency, if the sensitive personally identifiable information is not subject to further unauthorized disclosure;

(ii) the release of a public record not otherwise subject to confidentiality or nondisclosure requirements; or

(iii) any lawfully authorized investigative, protective, or intelligence activity of a law enforcement or intelligence agency of the United States.

(12) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term ''sensitive personally identifiable information'' means any information or compilation of information, in electronic or digital form that includes—

(A) an individual's first and last name or first initial and last name in combination with any 1 of the following data elements:

(i) A non-truncated social security number, driver's license number, passport number, or alien registration number.

(ii) Any 2 of the following:

(I) Home address or telephone number.

(II) Mother's maiden name.

(III) Month, day, and year of birth.

(iii) Unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation.

(iv) A unique account identifier, electronic identification number, user name, or routing code in combination with any associated security code, access code, or password if the code or password is required for an individual to obtain money, goods, services, or any other thing of value; or

(B) a financial account number or credit or debit card number in combination with any security code, access code, or password that is required for an individual to obtain credit, withdraw funds, or engage in a financial transaction.

TITLE I—ENHANCING PUNISHMENT FOR IDENTITY THEFT AND OTHER VIOLATIONS OF DATA PRIVACY AND SECURITY

SEC. 101. ORGANIZED CRIMINAL ACTIVITY IN CONNECTION WITH UNAUTHORIZED ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION.

Section 1961(1) of title 18, United States Code, is amended by inserting ''section 1030 (relating to fraud and related activity in connection with computers) if the act is a felony,'' before ''section 1084''.

SEC. 102. CONCEALMENT OF SECURITY BREACHES INVOLVING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.

(a) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by adding at the end the following:

''§ 1041. Concealment of security breaches involving sensitive personally identifiable information

''(a) Whoever, having knowledge of a security breach and having the obligation to provide notice of such breach to individuals under title III of the Personal Data Privacy and Security Act of 2011, and having not otherwise qualified for an exemption from providing notice under section 312 of such Act, intentionally and willfully conceals the fact of such security breach and which breach causes economic damage to 1 or more persons, shall be fined under this title or imprisoned not more than 5 years, or both.

''(b) For purposes of subsection (a), the term 'person' has the same meaning as in section 1030(e)(12) of title 18, United States Code.

''(c) Any person seeking an exemption under section 312(b) of the Personal Data Privacy and Security Act of 2011 shall be immune from prosecution under this section if the United States Secret Service does not indicate, in writing, that such notice be given under section 312(b)(3) of such Act.''.

(b) CONFORMING AND TECHNICAL AMENDMENTS.—The table of sections for chapter 47 of title 18, United States Code, is amended by adding at the end the following:

''1041. Concealment of security breaches involving personally identifiable information.''.

(c) ENFORCEMENT AUTHORITY.—

(1) IN GENERAL.—The United States Secret Service shall have the authority to investigate offenses under this section.

(2) NONEXCLUSIVITY.—The authority granted in paragraph (1) shall not be exclusive of any existing authority held by any other Federal agency.

SEC. 103. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030(c) of title 18, United States Code, is amended—

(1) by inserting ''or conspiracy'' after ''or an attempt'' each place it appears, except for paragraph (4);

(2) in paragraph (2)(B)—

(A) in clause (i), by inserting '', or attempt or conspiracy or conspiracy to commit an offense,'' after ''the offense'';

(B) in clause (ii), by inserting '', or attempt or conspiracy or conspiracy to commit an offense,'' after ''the offense''; and

(C) in clause (iii), by inserting ''(or, in the case of an attempted offense, would, if completed, have obtained)'' after ''information obtained''; and

(3) in paragraph (4)—

(A) in subparagraph (A)—

(i) by striking clause (ii);

(ii) by striking ''in the case of—'' and all that follows through ''an offense under subsection (a)(5)(B)'' and inserting ''in the case of an offense, or an attempt or conspiracy to commit an offense, under subsection (a)(5)(B)'';

(iii) by inserting ''or conspiracy'' after ''if the offense'';

(iv) by redesignating subclauses (I) through (VI) as clauses (i) through (vi), respectively, and adjusting the margin accordingly; and

(v) in clause (vi), as so redesignated, by striking ''; or'' and inserting a semicolon;

(B) in subparagraph (B)—

(i) by striking clause (ii);

(ii) by striking ''in the case of—'' and all that follows through ''an offense under subsection (a)(5)(A)'' and inserting ''in the case of an offense, or an attempt or conspiracy to commit an offense, under subsection (a)(5)(A)'';

(iii) by inserting ''or conspiracy'' after ''if the offense''; and

(iv) by striking ''; or'' and inserting a semicolon;

(C) in subparagraph (C)—

(i) by striking clause (ii);

(ii) by striking ''in the case of—'' and all that follows through ''an offense or an attempt to commit an offense'' and inserting ''in the case of an offense, or an attempt or conspiracy to commit an offense,''; and

(iii) by striking ''; or'' and inserting a semicolon;

(D) in subparagraph (D)—

(i) by striking clause (ii);

(ii) by striking ''in the case of—'' and all that follows through ''an offense or an attempt to commit an offense'' and inserting ''in the case of an offense, or an attempt or conspiracy to commit an offense,''; and

(iii) by striking ''; or'' and inserting a semicolon;

(E) in subparagraph (E), by inserting ''or conspires'' after ''offender attempts'';

(F) in subparagraph (F), by inserting ''or conspires'' after ''offender attempts''; and

(G) in subparagraph (G)(ii), by inserting ''or conspiracy'' after ''an attempt''.

TITLE II—DATA BROKERS

SEC. 201. TRANSPARENCY AND ACCURACY OF DATA COLLECTION.

(a) IN GENERAL.—Data brokers engaging in interstate commerce are subject to the requirements of this title for any product or service offered to third parties that allows access or use of personally identifiable information.

(b) LIMITATION.—Notwithstanding any other provision of this section, this section shall not apply to—

(1) any product or service offered by a data broker engaging in interstate commerce where such product or service is currently subject to, and in compliance with, access and accuracy protections similar to those under subsections (c) through (e) of this section under the Fair Credit Reporting Act (Public Law 91–508);

(2) any data broker that is subject to regulation under the Gramm-Leach-Bliley Act (Public Law 106–102);

(3) any data broker currently subject to and in compliance with the data security requirements for such entities under the Health Insurance Portability and Accountability Act (Public Law 104–191), and its implementing regulations;

(4) any data broker subject to, and in compliance with, the privacy and data security requirements under sections 13401 and 13404 of division A of the American Reinvestment and Recovery Act of 2009 (42 U.S.C. 17931 and 17934) and implementing regulations promulgated under such sections;

(5) information in a personal electronic record that—

(A) the data broker has identified as inaccurate, but maintains for the purpose of aiding the data broker in preventing inaccurate information from entering an individual's personal electronic record; and

(B) is not maintained primarily for the purpose of transmitting or otherwise providing that information, or assessments based on that information, to nonaffiliated third parties;

(6) information concerning proprietary methodologies, techniques, scores, or algorithms relating to fraud prevention not normally provided to third parties in the ordinary course of business ; and

(7) information that is used for legitimate governmental or fraud prevention purposes that would be compromised by disclosure to the individual.

(c) DISCLOSURES TO INDIVIDUALS.—

(1) IN GENERAL.—A data broker shall, upon the request of an individual, disclose to such individual for a reasonable fee all personal electronic records pertaining to that individual maintained or accessed by the data broker specifically for disclosure to third parties that request information on that individual in the ordinary course of business in the databases or systems of the data broker at the time of such request.

(2) INFORMATION ON HOW TO CORRECT INACCURACIES.—The disclosures required under paragraph (1) shall also include guidance to individuals on procedures for correcting inaccuracies.

(d) DISCLOSURE TO INDIVIDUALS OF ADVERSE ACTIONS TAKEN BY THIRD PARTIES.—

(1) IN GENERAL.—If a person takes any adverse action with respect to any individual that is based, in whole or in part, on any information contained in a personal electronic record, the person, at no cost to the affected individual, shall provide—

(A) written or electronic notice of the adverse action to the individual;

(B) to the individual, in writing or electronically, the name, address, and telephone number of the data broker (including a toll-free telephone number established by the data broker, if the data broker complies and maintains data on individuals on a nationwide basis) that furnished the information to the person;

(C) a copy of the information such person obtained from the data broker; and

(D) information to the individual on the procedures for correcting any inaccuracies in such information.

(2) ACCEPTED METHODS OF NOTICE.—A person shall be in compliance with the notice requirements under paragraph (1) if such person provides written or electronic notice in the same manner and using the same methods as are required under section 313(1) of this Act.

(e) ACCURACY RESOLUTION PROCESS.—

(1) INFORMATION FROM A PUBLIC RECORD OR LICENSOR.—

(A) IN GENERAL.—If an individual notifies a data broker of a dispute as to the completeness or accuracy of information disclosed to such individual under subsection (c) that is obtained from a public record source or a license agreement, such data broker shall determine within 30 days whether the information in its system accurately and completely records the information available from the licensor or public record source.

(B) DATA BROKER ACTIONS.—If a data broker determines under subparagraph (A) that the information in its systems does not accurately and completely record the information available from a public record source or licensor, the data broker shall—

(i) correct any inaccuracies or incompleteness, and provide to such individual written notice of such changes; and

(ii) provide such individual with the contact information of the public record or licensor.

(2) INFORMATION NOT FROM A PUBLIC RECORD SOURCE OR LICENSOR.—If an individual notifies a data broker of a dispute as to the completeness or accuracy of information not from a public record or licensor that was disclosed to the individual under subsection (c), the data broker shall, within 30 days of receiving notice of such dispute—

(A) review and consider free of charge any information submitted by such individual that is relevant to the completeness or accuracy of the disputed information; and

(B) correct any information found to be incomplete or inaccurate and provide notice to such individual of whether and what information was corrected, if any.

(3) EXTENSION OF REVIEW PERIOD.—The 30-day period described in paragraph (1) may be extended for not more than 30 additional days if a data broker receives information from the individual during the initial 30-day period that is relevant to the completeness or accuracy of any disputed information.

(4) NOTICE IDENTIFYING THE DATA FURNISHER.—If the completeness or accuracy of any information not from a public record source or licensor that was disclosed to an individual under subsection (c) is disputed by such individual, the data broker shall provide, upon the request of such individual, the contact information of any data furnisher that provided the disputed information.

(5) DETERMINATION THAT DISPUTE IS FRIVOLOUS OR IRRELEVANT.—

(A) IN GENERAL.—Notwithstanding paragraphs (1) through (3), a data broker may decline to investigate or terminate a review of information disputed by an individual under those paragraphs if the data broker reasonably determines that the dispute by the individual is frivolous or intended to perpetrate fraud.

(B) NOTICE.—A data broker shall notify an individual of a determination under subparagraph (A) within a reasonable time by any means available to such data broker.

SEC. 202. ENFORCEMENT.

(a) CIVIL PENALTIES.—

(1) PENALTIES.—Any data broker that violates the provisions of section 201 shall be subject to civil penalties of not more than $1,000 per violation per day while such violations persist, up to a maximum of $250,000 per violation.

(2) INTENTIONAL OR WILLFUL VIOLATION.—A data broker that intentionally or willfully violates the provisions of section 201 shall be subject to additional penalties in the amount of $1,000 per violation per day, to a maximum of an additional $250,000 per violation, while such violations persist.

(3) EQUITABLE RELIEF.—A data broker engaged in interstate commerce that violates this section may be enjoined from further violations by a court of competent jurisdiction.

(4) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this subsection are cumulative and shall not affect any other rights and remedies available under law.

(b) FEDERAL TRADE COMMISSION AUTHORITY.—Any data broker shall have the provisions of this title enforced against it by the Federal Trade Commission.

(c) STATE ENFORCEMENT.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the acts or practices of a data broker that violate this title, the State may bring a civil action on behalf of the residents of that State in a district court of the United States of appropriate jurisdiction, or any other court of competent jurisdiction, to—

(A) enjoin that act or practice;

(B) enforce compliance with this title; or

(C) obtain civil penalties of not more than $1,000 per violation per day while such violations persist, up to a maximum of $250,000 per violation.

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under this subsection, the attorney general of the State involved shall provide to the Federal Trade Commission—

(i) a written notice of that action; and

(ii) a copy of the complaint for that action.

(B) EXCEPTION.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general of a State determines that it is not feasible to provide the notice described in subparagraph (A) before the filing of the action.

(C) NOTIFICATION WHEN PRACTICABLE.—In an action described under subparagraph (B), the attorney general of a State shall provide the written notice and the copy of the complaint to the Federal Trade Commission as soon after the filing of the complaint as practicable.

(3) FEDERAL TRADE COMMISSION AUTHORITY.—Upon receiving notice under paragraph (2), the Federal Trade Commission shall have the right to—

(A) move to stay the action, pending the final disposition of a pending Federal proceeding or action as described in paragraph (4);

(B) intervene in an action brought under paragraph (1); and

(C) file petitions for appeal.

(4) PENDING PROCEEDINGS.—If the Federal Trade Commission has instituted a proceeding or civil action for a violation of this title, no attorney general of a State may, during the pendency of such proceeding or civil action, bring an action under this subsection against any defendant named in such civil action for any violation that is alleged in that civil action.

(5) RULE OF CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this title shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(A) conduct investigations;

(B) administer oaths and affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(6) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under this subsection may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(B) SERVICE OF PROCESS.—In an action brought under this subsection, process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

(d) NO PRIVATE CAUSE OF ACTION.—Nothing in this title establishes a private cause of action against a data broker for violation of any provision of this title.

SEC. 203. RELATION TO STATE LAWS.

No requirement or prohibition may be imposed under the laws of any State with respect to any subject matter regulated under section 201, relating to individual access to, and correction of, personal electronic records held by data brokers.

SEC. 204. EFFECTIVE DATE.

This title shall take effect 180 days after the date of enactment of this Act.

TITLE III—PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION

Subtitle A—A Data Privacy and Security Program

SEC. 301. PURPOSE AND APPLICABILITY OF DATA PRIVACY AND SECURITY PROGRAM.

(a) PURPOSE.—The purpose of this subtitle is to ensure standards for developing and implementing administrative, technical, and physical safeguards to protect the security of sensitive personally identifiable information.

(b) IN GENERAL.—A business entity engaging in interstate commerce that involves collecting, accessing, transmitting, using, storing, or disposing of sensitive personally identifiable information in electronic or digital form on 10,000 or more United States persons is subject to the requirements for a data privacy and security program under section 302 for protecting sensitive personally identifiable information.

(c) LIMITATIONS.—Notwithstanding any other obligation under this subtitle, this subtitle does not apply to:

(1) FINANCIAL INSTITUTIONS.—Financial institutions—

(A) subject to the data security requirements and implementing regulations under the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.); and

(B) subject to—

(i) examinations for compliance with the requirements of this Act by a Federal Functional Regulator or State Insurance Authority (as those terms are defined in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809)); or

(ii) compliance with part 314 of title 16, Code of Federal Regulations.

(2) HIPPA REGULATED ENTITIES.—

(A) COVERED ENTITIES.—Covered entities subject to the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.), including the data security requirements and implementing regulations of that Act.

(B) BUSINESS ENTITIES.—A Business entity shall be deemed in compliance with this Act if the business entity—

(i) is acting as a business associate, as that term is defined under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.) and is in compliance with the requirements imposed under that Act and implementing regulations promulgated under that Act; and

(ii) is subject to, and currently in compliance, with the privacy and data security requirements under sections 13401 and 13404 of division A of the American Reinvestment and Recovery Act of 2009 (42 U.S.C. 17931 and

17934) and implementing regulations promulgated under such sections.

(3) PUBLIC RECORDS.—Public records not otherwise subject to a confidentiality or nondisclosure requirement, or information obtained from a news report or periodical.

(d) SAFE HARBORS.—

(1) IN GENERAL.—A business entity shall be deemed in compliance with the privacy and security program requirements under section 302 if the business entity complies with or provides protection equal to industry standards or standards widely accepted as an effective industry practice, as identified by the Federal Trade Commission, that are applicable to the type of sensitive personally identifiable information involved in the ordinary course of business of such business entity.

(2) LIMITATION.—Nothing in this subsection shall be construed to permit, and nothing does permit, the Federal Trade Commission to issue regulations requiring, or according greater legal status to, the implementation of or application of a specific technology or technological specifications for meeting the requirements of this title.

SEC. 302. REQUIREMENTS FOR A PERSONAL DATA PRIVACY AND SECURITY PROGRAM.

(a) PERSONAL DATA PRIVACY AND SECURITY PROGRAM.—A business entity subject to this subtitle shall comply with the following safeguards and any other administrative, technical, or physical safeguards identified by the Federal Trade Commission in a rulemaking process pursuant to section 553 of title 5, United States Code, for the protection of sensitive personally identifiable information:

(1) SCOPE.—A business entity shall implement a comprehensive personal data privacy and security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the business entity and the nature and scope of its activities.

(2) DESIGN.—The personal data privacy and security program shall be designed to—

(A) ensure the privacy, security, and confidentiality of sensitive personally identifying information;

(B) protect against any anticipated vulnerabilities to the privacy, security, or integrity of sensitive personally identifying information; and

(C) protect against unauthorized access to use of sensitive personally identifying information that could create a significant risk of harm or fraud to any individual.

(3) RISK ASSESSMENT.—A business entity shall—

(A) identify reasonably foreseeable internal and external vulnerabilities that could result in unauthorized access, disclosure, use, or alteration of sensitive personally identifiable information or systems containing sensitive personally identifiable information;

(B) assess the likelihood of and potential damage from unauthorized access, disclosure, use, or alteration of sensitive personally identifiable information;

(C) assess the sufficiency of its policies, technologies, and safeguards in place to control and minimize risks from unauthorized access, disclosure, use, or alteration of sensitive personally identifiable information; and

(D) assess the vulnerability of sensitive personally identifiable information during destruction and disposal of such information, including through the disposal or retirement of hardware.

(4) RISK MANAGEMENT AND CONTROL.—Each business entity shall—

(A) design its personal data privacy and security program to control the risks identified under paragraph (3); and

(B) adopt measures commensurate with the sensitivity of the data as well as the size, complexity, and scope of the activities of the business entity that—

(i) control access to systems and facilities containing sensitive personally identifiable information, including controls to authenticate and permit access only to authorized individuals;

(ii) detect, record, and preserve information relevant to actual and attempted fraudulent, unlawful, or unauthorized access, disclosure, use, or alteration of sensitive personally identifiable information, including by employees and other individuals otherwise authorized to have access;

(iii) protect sensitive personally identifiable information during use, transmission, storage, and disposal by encryption, redaction, or access controls that are widely accepted as an effective industry practice or industry standard, or other reasonable means (including as directed for disposal of records under section 628 of the Fair Credit Reporting Act (15 U.S.C. 1681w) and the implementing regulations of such Act as set forth in section 682 of title 16, Code of Federal Regulations);

(iv) ensure that sensitive personally identifiable information is properly destroyed and disposed of, including during the destruction of computers, diskettes, and other electronic media that contain sensitive personally identifiable information;

(v) trace access to records containing sensitive personally identifiable information so that the business entity can determine who accessed or acquired such sensitive personally identifiable information pertaining to specific individuals; and

(vi) ensure that no third party or customer of the business entity is authorized to access or acquire sensitive personally identifiable information without the business entity first performing sufficient due diligence to ascertain, with reasonable certainty, that such information is being sought for a valid legal purpose.

(b) TRAINING.—Each business entity subject to this subtitle shall take steps to ensure employee training and supervision for implementation of the data security program of the business entity.

(c) VULNERABILITY TESTING.—

(1) IN GENERAL.—Each business entity subject to this subtitle shall take steps to ensure regular testing of key controls, systems, and procedures of the personal data privacy and security program to detect, prevent, and respond to attacks or intrusions, or other system failures.

(2) FREQUENCY.—The frequency and nature of the tests required under paragraph (1) shall be determined by the risk assessment of the business entity under subsection (a)(3).

(d) RELATIONSHIP TO SERVICE PROVIDERS.—In the event a business entity subject to this subtitle engages service providers not subject to this subtitle, such business entity shall—

(1) exercise appropriate due diligence in selecting those service providers for responsibilities related to sensitive personally identifiable information, and take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the security, privacy, and integrity of the sensitive personally identifiable information at issue; and

(2) require those service providers by contract to implement and maintain appropriate measures designed to meet the objectives and requirements governing entities subject to section 301, this section, and subtitle B.

(e) PERIODIC ASSESSMENT AND PERSONAL DATA PRIVACY AND SECURITY MODERNIZATION.—Each business entity subject to this subtitle shall on a regular basis monitor, evaluate, and adjust, as appropriate its data privacy and security program in light of any relevant changes in—

(1) technology;

(2) the sensitivity of personally identifiable information;

(3) internal or external threats to personally identifiable information; and

(4) the changing business arrangements of the business entity, such as—

(A) mergers and acquisitions;

(B) alliances and joint ventures;

(C) outsourcing arrangements;

(D) bankruptcy; and

(E) changes to sensitive personally identifiable information systems.

(f) IMPLEMENTATION TIMELINE.—Not later than 1 year after the date of enactment of this Act, a business entity subject to the provisions of this subtitle shall implement a data privacy and security program pursuant to this subtitle.

SEC. 303. ENFORCEMENT.

(a) CIVIL PENALTIES.—

(1) IN GENERAL.—Any business entity that violates the provisions of sections 301 or 302 shall be subject to civil penalties of not more than $5,000 per violation per day while such a violation exists, with a maximum of $500,000 per violation.

(2) INTENTIONAL OR WILLFUL VIOLATION.—A business entity that intentionally or willfully violates the provisions of sections 301 or 302 shall be subject to additional penalties in the amount of $5,000 per violation per day while such a violation exists, with a maximum of an additional $500,000 per violation.

(3) EQUITABLE RELIEF.—A business entity engaged in interstate commerce that violates this section may be enjoined from further violations by a court of competent jurisdiction.

(4) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this section are cumulative and shall not affect any other rights and remedies available under law.

(b) FEDERAL TRADE COMMISSION AUTHORITY.—Any business entity shall have the provisions of this subtitle enforced against it by the Federal Trade Commission.

(c) STATE ENFORCEMENT.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the acts or practices of a business entity that violate this subtitle, the State may bring a civil action on behalf of the residents of that State in a district court of the United States of appropriate jurisdiction, or any other court of competent jurisdiction, to—

(A) enjoin that act or practice;

(B) enforce compliance with this subtitle; or

(C) obtain civil penalties of not more than $5,000 per violation per day while such violations persist, up to a maximum of $500,000 per violation.

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under this subsection, the attorney general of the State involved shall provide to the Federal Trade Commission—

(i) a written notice of that action; and

(ii) a copy of the complaint for that action.

(B) EXCEPTION.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, if the attorney general of a State determines that it is not feasible to

provide the notice described in this subparagraph before the filing of the action.

(C) NOTIFICATION WHEN PRACTICABLE.—In an action described under subparagraph (B), the attorney general of a State shall provide the written notice and the copy of the complaint to the Federal Trade Commission as soon after the filing of the complaint as practicable.

(3) FEDERAL TRADE COMMISSION AUTHORITY.—Upon receiving notice under paragraph (2), the Federal Trade Commission shall have the right to—

(A) move to stay the action, pending the final disposition of a pending Federal proceeding or action as described in paragraph (4);

(B) intervene in an action brought under paragraph (1); and

(C) file petitions for appeal.

(4) PENDING PROCEEDINGS.—If the Federal Trade Commission has instituted a proceeding or action for a violation of this subtitle or any regulations thereunder, no attorney general of a State may, during the pendency of such proceeding or action, bring an action under this subsection against any defendant named in such criminal proceeding or civil action for any violation that is alleged in that proceeding or action.

(5) RULE OF CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1) nothing in this subtitle shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(A) conduct investigations;

(B) administer oaths and affirmations; or

(C) compel the attendance of witnesses or the production of documentary and other evidence.

(6) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under this subsection may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

(B) SERVICE OF PROCESS.—In an action brought under this subsection, process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

(d) NO PRIVATE CAUSE OF ACTION.—Nothing in this subtitle establishes a private cause of action against a business entity for violation of any provision of this subtitle.

SEC. 304. RELATION TO OTHER LAWS.

(a) IN GENERAL.—No State may require any business entity subject to this subtitle to comply with any requirements with respect to administrative, technical, and physical safeguards for the protection of sensitive personally identifying information.

(b) LIMITATIONS.—Nothing in this subtitle shall be construed to modify, limit, or supersede the operation of the Gramm-Leach-Bliley Act or its implementing regulations, including those adopted or enforced by States.

Subtitle B—Security Breach Notification

SEC. 311. NOTICE TO INDIVIDUALS.

(a) IN GENERAL.—Any agency, or business entity engaged in interstate commerce, that uses, accesses, transmits, stores, disposes of or collects sensitive personally identifiable information shall, following the discovery of a security breach of such information, notify any resident of the United States whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed, or acquired.

(b) OBLIGATION OF OWNER OR LICENSEE.—

(1) NOTICE TO OWNER OR LICENSEE.—Any agency, or business entity engaged in interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information that the agency or business entity does not own or license shall notify the owner or licensee of the information following the discovery of a security breach involving such information.

(2) NOTICE BY OWNER, LICENSEE OR OTHER DESIGNATED THIRD PARTY.—Nothing in this subtitle shall prevent or abrogate an agreement between an agency or business entity required to give notice under this section and a designated third party, including an owner or licensee of the sensitive personally identifiable information subject to the security breach, to provide the notifications required under subsection (a).

(3) BUSINESS ENTITY RELIEVED FROM GIVING NOTICE.—A business entity obligated to give notice under subsection (a) shall be relieved of such obligation if an owner or licensee of the sensitive personally identifiable information subject to the security breach, or other designated third party, provides such notification.

(c) TIMELINESS OF NOTIFICATION.—

(1) IN GENERAL.—All notifications required under this section shall be made without unreasonable delay following the discovery by the agency or business entity of a security breach.

(2) REASONABLE DELAY.—Reasonable delay under this subsection may include any time necessary to determine the scope of the security breach, prevent further disclosures, conduct the risk assessment described in section 302(a)(3), and restore the reasonable integrity of the data system and provide notice to law enforcement when required.

(3) BURDEN OF PRODUCTION.—The agency, business entity, owner, or licensee required to provide notice under this subtitle shall, upon the request of the Attorney General, provide records or other evidence of the notifications required under this subtitle, including to the extent applicable, the reasons for any delay of notification.

(d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT PURPOSES.—

(1) IN GENERAL.—If a Federal law enforcement or intelligence agency determines that the notification required under this section would impede a criminal investigation, such notification shall be delayed upon written notice from such Federal law enforcement or intelligence agency to the agency or business entity that experienced the breach.

(2) EXTENDED DELAY OF NOTIFICATION.—If the notification required under subsection (a) is delayed pursuant to paragraph (1), an agency or business entity shall give notice 30 days after the day such law enforcement delay was invoked unless a Federal law enforcement or intelligence agency provides written notification that further delay is necessary.

(3) LAW ENFORCEMENT IMMUNITY.—No cause of action shall lie in any court against any law enforcement agency for acts relating to the delay of notification for law enforcement purposes under this subtitle.

SEC. 312. EXEMPTIONS.

(a) EXEMPTION FOR NATIONAL SECURITY AND LAW ENFORCEMENT.—

(1) IN GENERAL.—Section 311 shall not apply to an agency or business entity if the agency or business entity certifies, in writing, that notification of the security breach as required by section 311 reasonably could be expected to—

(A) cause damage to the national security; or

(B) hinder a law enforcement investigation or the ability of the agency to conduct law enforcement investigations.

(2) LIMITS ON CERTIFICATIONS.—An agency or business entity may not execute a certification under paragraph (1) to—

(A) conceal violations of law, inefficiency, or administrative error;

(B) prevent embarrassment to a business entity, organization, or agency; or

(C) restrain competition.

(3) NOTICE.—In every case in which an agency or business agency issues a certification under paragraph (1), the certification, accompanied by a description of the factual basis for the certification, shall be immediately provided to the United States Secret Service and the Federal Bureau of Investigation.

(4) SECRET SERVICE AND FBI REVIEW OF CERTIFICATIONS.—

(A) IN GENERAL.—The United States Secret Service or the Federal Bureau of Investigation may review a certification provided by an agency under paragraph (3), and shall review a certification provided by a business entity under paragraph (3), to determine whether an exemption under paragraph (1) is merited. Such review shall be completed not later than 10 business days after the date of receipt of the certification, except as provided in paragraph (5)(C).

(B) NOTICE.—Upon completing a review under subparagraph (A) the United States Secret Service or the Federal Bureau of Investigation shall immediately notify the agency or business entity, in writing, of its determination of whether an exemption under paragraph (1) is merited.

(C) EXEMPTION.—The exemption under paragraph (1) shall not apply if the United States Secret Service or the Federal Bureau of Investigation determines under this paragraph that the exemption is not merited.

(5) ADDITIONAL AUTHORITY OF THE SECRET SERVICE AND FBI.—

(A) IN GENERAL.—In determining under paragraph (4) whether an exemption under paragraph (1) is merited, the United States Secret Service or the Federal Bureau of Investigation may request additional information from the agency or business entity regarding the basis for the claimed exemption, if such additional information is necessary to determine whether the exemption is merited.

(B) REQUIRED COMPLIANCE.—Any agency or business entity that receives a request for additional information under subparagraph (A) shall cooperate with any such request.

(C) TIMING.—If the United States Secret Service or the Federal Bureau of Investigation requests additional information under subparagraph (A), the United States Secret Service or the Federal Bureau of Investigation shall notify the agency or business entity not later than 10 business days after the date of receipt of the additional information whether an exemption under paragraph (1) is merited.

(b) SAFE HARBOR.—An agency or business entity will be exempt from the notice requirements under section 311, if—

(1) a risk assessment concludes that—

(A) there is no significant risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach, with the encryption of such information establishing a presumption that no significant risk exists; or

(B) there is no significant risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach, with the rendering of such sensitive personally identifiable information indecipherable through the use of best practices or methods, such as redaction, access controls, or other such mechanisms, which are widely accepted as an effective industry practice, or an effective industry standard, establishing a presumption that no significant risk exists;

(2) without unreasonable delay, but not later than 45 days after the discovery of a security breach, unless extended by the United States Secret Service or the Federal Bureau of Investigation, the agency or business entity notifies the United States Secret Service and the Federal Bureau of Investigation, in writing, of—

(A) the results of the risk assessment; and

(B) its decision to invoke the risk assessment exemption; and

(3) the United States Secret Service or the Federal Bureau of Investigation does not indicate, in writing, within 10 business days from receipt of the decision, that notice should be given.

(c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

(1) IN GENERAL.—A business entity will be exempt from the notice requirement under section 311 if the business entity utilizes or participates in a security program that—

(A) is designed to block the use of the sensitive personally identifiable information to initiate unauthorized financial transactions before they are charged to the account of the individual; and

(B) provides for notice to affected individuals after a security breach that has resulted in fraud or unauthorized transactions.

(2) LIMITATION.—The exemption by this subsection does not apply if—

(A) the information subject to the security breach includes sensitive personally identifiable information, other than a credit card or credit card security code, of any type of the sensitive personally identifiable information identified in section 3; or

(B) the security breach includes both the individual's credit card number and the individual's first and last name.

SEC. 313. METHODS OF NOTICE.

An agency or business entity shall be in compliance with section 311 if it provides both:

(1) INDIVIDUAL NOTICE.—Notice to individuals by 1 of the following means:

(A) Written notification to the last known home mailing address of the individual in the records of the agency or business entity.

(B) Telephone notice to the individual personally.

(C) E-mail notice, if the individual has consented to receive such notice and the notice is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001).

(2) MEDIA NOTICE.—Notice to major media outlets serving a State or jurisdiction, if the number of residents of such State whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person exceeds 5,000.

SEC. 314. CONTENT OF NOTIFICATION.

(a) IN GENERAL.—Regardless of the method by which notice is provided to individuals under section 313, such notice shall include, to the extent possible—

(1) a description of the categories of sensitive personally identifiable information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person;

(2) a toll-free number—

(A) that the individual may use to contact the agency or business entity, or the agent of the agency or business entity; and

(B) from which the individual may learn what types of sensitive personally identifiable information the agency or business entity maintained about that individual; and

(3) the toll-free contact telephone numbers and addresses for the major credit reporting agencies.

(b) ADDITIONAL CONTENT.—Notwithstanding section 319, a State may require that a notice under subsection (a) shall also include information regarding victim protection assistance provided for by that State.

SEC. 315. COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGENCIES.

If an agency or business entity is required to provide notification to more than 5,000 individuals under section 311(a), the agency or business entity shall also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis (as defined in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)) of the timing and distribution of the notices. Such notice shall be given to the consumer credit reporting agencies without unreasonable delay and, if it will not delay notice to the affected individuals, prior to the distribution of notices to the affected individuals.

SEC. 316. NOTICE TO LAW ENFORCEMENT.

(a) SECRET SERVICE AND FBI.—Any business entity or agency shall notify the United States Secret Service and the Federal Bureau of Investigation of the fact that a security breach has occurred if—

(1) the number of individuals whose sensitive personally identifying information was, or is reasonably believed to have been accessed or acquired by an unauthorized person exceeds 10,000;

(2) the security breach involves a database, networked or integrated databases, or other data system containing the sensitive personally identifiable information of more than 1,000,000 individuals nationwide;

(3) the security breach involves databases owned by the Federal Government; or

(4) the security breach involves primarily sensitive personally identifiable information of individuals known to the agency or business entity to be employees and contractors of the Federal Government involved in national security or law enforcement.

(b) FTC REVIEW OF THRESHOLDS.—The Federal Trade Commission may review and adjust the thresholds for notice to law enforcement under subsection (a), after notice and the opportunity for public comment, in a manner consistent with this section.

(c) ADVANCE NOTICE TO LAW ENFORCEMENT.—Not later than 48 hours before notifying an individual of a security breach under section 311, a business entity or agency that is required to provide notice under this section shall notify the United States Secret Service and the Federal Bureau of Investigation of the fact that the business entity or agency intends to provide the notice.

(d) NOTICE TO OTHER LAW ENFORCEMENT AGENCIES.—The United States Secret Service and the Federal Bureau of Investigation shall be responsible for notifying—

(1) the United States Postal Inspection Service, if the security breach involves mail fraud;

(2) the attorney general of each State affected by the security breach; and

(3) the Federal Trade Commission, if the security breach involves consumer reporting agencies subject to the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), or anticompetitive conduct.

(e) TIMING OF NOTICES.—The notices required under this section shall be delivered as follows:

(1) Notice under subsection (a) shall be delivered as promptly as possible, but not later than 14 days after discovery of the events requiring notice.

(2) Notice under subsection (d) shall be delivered not later than 14 days after the Service receives notice of a security breach from an agency or business entity.

SEC. 317. ENFORCEMENT.

(a) CIVIL ACTIONS BY THE ATTORNEY GENERAL.—The Attorney General may bring a civil action in the appropriate United States district court against any business entity that engages in conduct constituting a violation of this subtitle and, upon proof of such conduct by a preponderance of the evidence, such business entity shall be subject to a civil penalty of not more than $1,000 per day per individual whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of $1,000,000 per violation, unless such conduct is found to be willful or intentional. In determining the amount of a civil penalty under this subsection, the court shall take into account the degree of culpability of the business entity, any prior violations of this subtitle by the business entity, the ability of the business entity to pay, the effect on the ability of the business entity to continue to do business, and such other matters as justice may require.

(b) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—

(1) IN GENERAL.—If it appears that a business entity has engaged, or is engaged, in any act or practice constituting a violation of this subtitle, the Attorney General may petition an appropriate district court of the United States for an order—

(A) enjoining such act or practice; or

(B) enforcing compliance with this subtitle.

(2) ISSUANCE OF ORDER.—A court may issue an order under paragraph (1), if the court finds that the conduct in question constitutes a violation of this subtitle.

(c) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this subtitle are cumulative and shall not affect any other rights and remedies available under law.

(d) FRAUD ALERT.—Section 605A(b)(1) of the Fair Credit Reporting Act (15 U.S.C. 1681c–1(b)(1)) is amended by inserting '', or evidence that the consumer has received notice that the consumer's financial information has or may have been compromised,'' after ''identity theft report''.

SEC. 318. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) IN GENERAL.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of a business entity in a practice that is prohibited under this subtitle, the State or the State or local law enforcement agency on behalf of the residents of the agency's jurisdiction, may bring a civil action on behalf of the residents of the State or jurisdiction in a district court of the United States of appropriate jurisdiction or any other court of competent jurisdiction, including a State court, to—

(A) enjoin that practice;

(B) enforce compliance with this subtitle; or

(C) civil penalties of not more than $1,000 per day per individual whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of $1,000,000 per violation, unless such conduct is found to be willful or intentional.

(2) NOTICE.—

(A) IN GENERAL.—Before filing an action under paragraph (1), the attorney general of the State involved shall provide to the Attorney General of the United States—

(i) written notice of the action; and

(ii) a copy of the complaint for the action.

(B) EXEMPTION.—

(i) IN GENERAL.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this subtitle, if the State attorney general determines that it is not feasible to provide the notice described in such subparagraph before the filing of the action.

(ii) NOTIFICATION.—In an action described in clause (i), the attorney general of a State shall provide notice and a copy of the complaint to the Attorney General at the time the State attorney general files the action.

(b) FEDERAL PROCEEDINGS.—Upon receiving notice under subsection (a)(2), the Attorney General shall have the right to—

(1) move to stay the action, pending the final disposition of a pending Federal proceeding or action;

(2) initiate an action in the appropriate United States district court under section 317 and move to consolidate all pending actions, including State actions, in such court;

(3) intervene in an action brought under subsection (a)(2); and

(4) file petitions for appeal.

(c) PENDING PROCEEDINGS.—If the Attorney General has instituted a proceeding or action for a violation of this subtitle or any regulations thereunder, no attorney general of a State may, during the pendency of such proceeding or action, bring an action under this subtitle against any defendant named in such criminal proceeding or civil action for any violation that is alleged in that proceeding or action.

(d) CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this subtitle regarding notification shall be construed to prevent an attorney general of a State from exercising the powers conferred on such attorney general by the laws of that State to—

(1) conduct investigations;

(2) administer oaths or affirmations; or

(3) compel the attendance of witnesses or the production of documentary and other evidence.

(e) VENUE; SERVICE OF PROCESS.—

(1) VENUE.—Any action brought under subsection (a) may be brought in—

(A) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(B) another court of competent jurisdiction.

(2) SERVICE OF PROCESS.—In an action brought under subsection (a), process may be served in any district in which the defendant—

(A) is an inhabitant; or

(B) may be found.

(f) NO PRIVATE CAUSE OF ACTION.—Nothing in this subtitle establishes a private cause of action against a business entity for violation of any provision of this subtitle.

SEC. 319. EFFECT ON FEDERAL AND STATE LAW.

The provisions of this subtitle shall supersede any other provision of Federal law or any provision of law of any State relating to notification by a business entity engaged in interstate commerce or an agency of a security breach, except as provided in section 314(b).

SEC. 320. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated such sums as may be necessary to cover the costs incurred by the United States Secret Service to carry out investigations and risk assessments of security breaches as required under this subtitle.

SEC. 321. REPORTING ON RISK ASSESSMENT EXEMPTIONS.

The United States Secret Service and the Federal Bureau of Investigation shall report to Congress not later than 18 months after the date of enactment of this Act, and upon the request by Congress thereafter, on—

(1) the number and nature of the security breaches described in the notices filed by those business entities invoking the risk assessment exemption under section 312(b) and the response of the United States Secret Service and the Federal Bureau of Investigation to such notices; and

(2) the number and nature of security breaches subject to the national security and law enforcement exemptions under section 312(a), provided that such report may not disclose the contents of any risk assessment provided to the United States Secret Service and the Federal Bureau of Investigation pursuant to this subtitle.

SEC. 322. EFFECTIVE DATE.

This subtitle shall take effect on the expiration of the date which is 90 days after the date of enactment of this Act.

TITLE IV—GOVERNMENT ACCESS TO AND USE OF COMMERCIAL DATA

SEC. 401. GENERAL SERVICES ADMINISTRATION REVIEW OF CONTRACTS.

(a) IN GENERAL.—In considering contract awards totaling more than $500,000 and entered into after the date of enactment of this Act with data brokers, the Administrator of the General Services Administration shall evaluate—

(1) the data privacy and security program of a data broker to ensure the privacy and security of data containing personally identifiable information, including whether such program adequately addresses privacy and security threats created by malicious software or code, or the use of peer-to-peer file sharing software;

(2) the compliance of a data broker with such program;

(3) the extent to which the databases and systems containing personally identifiable information of a data broker have been compromised by security breaches; and

(4) the response by a data broker to such breaches, including the efforts by such data broker to mitigate the impact of such security breaches.

(b) COMPLIANCE SAFE HARBOR.—The data privacy and security program of a data broker shall be deemed sufficient for the purposes of subsection (a), if the data broker complies with or provides protection equal to industry standards, as identified by the Federal Trade Commission, that are applicable to the type of personally identifiable information involved in the ordinary course of business of such data broker.

(c) PENALTIES.—In awarding contracts with data brokers for products or services related to access, use, compilation, distribution, processing, analyzing, or evaluating personally identifiable information, the Administrator of the General Services Administration shall—

(1) include monetary or other penalties—

(A) for failure to comply with subtitles A and B of title III; or

(B) if a contractor knows or has reason to know that the personally identifiable information being provided is inaccurate, and provides such inaccurate information; and

(2) require a data broker that engages service providers not subject to subtitle A of title III for responsibilities related to sensitive personally identifiable information to—

(A) exercise appropriate due diligence in selecting those service providers for responsibilities related to personally identifiable information;

(B) take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the security, privacy, and integrity of the personally identifiable information at issue; and

(C) require such service providers, by contract, to implement and maintain appropriate measures designed to meet the objectives and requirements in title III.

(d) LIMITATION.—The penalties under subsection (c) shall not apply to a data broker providing information that is accurately and completely recorded from a public record source or licensor.

SEC. 402. REQUIREMENT TO AUDIT INFORMATION SECURITY PRACTICES OF CONTRACTORS AND THIRD PARTY BUSINESS ENTITIES.

Section 3544(b) of title 44, United States Code, is amended—

(1) in paragraph (7)(C)(iii), by striking ''and'' after the semicolon;

(2) in paragraph (8), by striking the period and inserting ''; and''; and

(3) by adding at the end the following:

''(9) procedures for evaluating and auditing the information security practices of contractors or third party business entities supporting the information systems or operations of the agency involving personally identifiable information (as that term is defined in section 3 of the Personal Data Privacy and Security Act of 2011) and ensuring remedial action to address any significant deficiencies.''.

SEC. 403. PRIVACY IMPACT ASSESSMENT OF GOVERNMENT USE OF COMMERCIAL INFORMATION SERVICES CONTAINING PERSONALLY IDENTIFIABLE INFORMATION.

(a) IN GENERAL.—Section 208(b)(1) of the E-Government Act of 2002 (44 U.S.C. 3501 note) is amended—

(1) in subparagraph (A)(i), by striking ''or''; and

(2) in subparagraph (A)(ii), by striking the period and inserting ''; or''; and

(3) by inserting after clause (ii) the following:

''(iii) purchasing or subscribing for a fee to personally identifiable information from a data broker (as such terms are defined in section 3 of the Personal Data Privacy and Security Act of 2011).''.

(b) LIMITATION.—Notwithstanding any other provision of law, commencing 1 year after the date of enactment of this Act, no Federal agency may enter into a contract with a data broker to access for a fee any database consisting primarily of personally identifiable information concerning United States persons (other than news reporting or telephone directories) unless the head of such department or agency—

(1) completes a privacy impact assessment under section 208 of the E-Government Act of 2002 (44 U.S.C. 3501 note), which shall subject to the provision in that Act pertaining to sensitive information, include a description of—

(A) such database;

(B) the name of the data broker from whom it is obtained; and

(C) the amount of the contract for use;

(2) adopts regulations that specify—

(A) the personnel permitted to access, analyze, or otherwise use such databases;

(B) standards governing the access, analysis, or use of such databases;

(C) any standards used to ensure that the personally identifiable information accessed, analyzed, or used is the minimum necessary to accomplish the intended legitimate purpose of the Federal agency;

(D) standards limiting the retention and redisclosure of personally identifiable information obtained from such databases;

(E) procedures ensuring that such data meet standards of accuracy, relevance, completeness, and timeliness;

(F) the auditing and security measures to protect against unauthorized access, analysis, use, or modification of data in such databases;

(G) applicable mechanisms by which individuals may secure timely redress for any adverse consequences wrongly incurred due to the access, analysis, or use of such databases;

(H) mechanisms, if any, for the enforcement and independent oversight of existing or planned procedures, policies, or guidelines; and

(I) an outline of enforcement mechanisms for accountability to protect individuals and the public against unlawful or illegitimate access or use of databases; and

(3) incorporates into the contract or other agreement totaling more than $500,000, provisions—

(A) providing for penalties—

(i) for failure to comply with title III of this Act; or

(ii) if the entity knows or has reason to know that the personally identifiable information being provided to the Federal department or agency is inaccurate, and provides such inaccurate information; and

(B) requiring a data broker that engages service providers not subject to subtitle A of title III for responsibilities related to sensitive personally identifiable information to—

(i) exercise appropriate due diligence in selecting those service providers for responsibilities related to personally identifiable information;

(ii) take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the security, privacy, and integrity of the personally identifiable information at issue; and

(iii) require such service providers, by contract, to implement and maintain appropriate measures designed to meet the objectives and requirements in title III.

(c) LIMITATION ON PENALTIES.—The penalties under subsection (b)(3)(A) shall not apply to a data broker providing information that is accurately and completely recorded from a public record source.

(d) STUDY OF GOVERNMENT USE.—

(1) SCOPE OF STUDY.—Not later than 180 days after the date of enactment of this Act, the Comptroller General of the United States shall conduct a study and audit and prepare a report on Federal agency actions to address the recommendations in the Government Accountability Office's April 2006 report on agency adherence to key privacy principles in using data brokers or commercial databases containing personally identifiable information.

(2) REPORT.—A copy of the report required under paragraph (1) shall be submitted to Congress.

TITLE V—COMPLIANCE WITH STATUTORY PAY-AS-YOU-GO ACT

SEC. 501. BUDGET COMPLIANCE.

The budgetary effects of this Act, for the purpose of complying with the Statutory Pay-As-You-Go-Act of 2010, shall be determined by reference to the latest statement titled ''Budgetary Effects of PAYGO Legislation'' for this Act, submitted for printing in the Congressional Record by the Chairman of the Senate Budget Committee, provided that such statement has been submitted prior to the vote on passage.

By Mr. BAUCUS:

S. 1154. A bill to require transparency for Executive departments in meeting the Government-wide goals for contracting with small business concerns owned and controlled by service-disabled veterans, and for other purposes; to the Committee on Small Business and Entrepreneurship.

Mr. BAUCUS. Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the text of the bill was ordered to be printed in the RECORD, as follows:

S. 1154

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Honoring Promises to Service-Disabled Veterans Act of 2011''.

SEC. 2. FINDINGS.

Congress finds the following:

(1) Federal agencies have an obligation to comply with the Veterans Entrepreneurship and Small Business Development Act of 1999 (Public Law 106–50; 113 Stat. 233), and the amendments made by that Act, which established a Government-wide goal that not less than 3 percent of the total value of all prime contracts and subcontracts be awarded to small business concerns owned and controlled by service-disabled veterans each fiscal year (referred to in this section as the ''Government-wide goal for service-disabled veterans'').

(2) Progress in meeting the Government-wide goal for service-disabled veterans has been unacceptably slow.

(3) Prime contractors doing business with the United States Government have an obligation to do their part to meet the Government-wide goal for service-disabled veterans.

(4) The public has a right to know whether the Executive departments (as defined in section 101 of title 5, United States Code) and prime contractors are meeting the Government-wide goal for service-disabled veterans.

SEC. 3. TRANSPARENCY IN CONTRACTING GOALS FOR SMALL BUSINESS CONCERNS OWNED AND CONTROLLED BY SERVICE-DISABLED VETERANS.

Section 15 of the Small Business Act (15 U.S.C. 644) is amended by adding at the end the following:

''(s) TRANSPARENCY IN CONTRACTING GOALS FOR SMALL BUSINESS CONCERNS OWNED AND CONTROLLED BY SERVICE-DISABLED VETERANS.—

''(1) DEFINITIONS.—In this subsection—

''(A) the term 'covered contractor' means a contractor that is required to submit a subcontracting plan under section 8(d) to an Executive department; and

''(B) the term 'Executive department' has the meaning given that term in section 101 of title 5, United States Code.

''(2) REPORTS TO ADMINISTRATOR.—Three months after the date of enactment of this subsection, and quarterly thereafter, the head of each Executive department shall submit to the Administrator a report that contains—

''(A) the percentage of the total value of all prime contracts awarded by the Executive department to small business concerns owned and controlled by service-disabled veterans during the 3-month period ending on the date of the report;

''(B) the name of each covered contractor to which the Executive department awards a contract;

''(C) for each contract awarded to a covered contractor by the Executive department—

''(i) the percentage goal negotiated under section 8(d)(6)(A) for the utilization as subcontractors of small business concerns owned and controlled by service-disabled veterans; and

''(ii) if the contract is completed during the 3-month period ending on the date of the report, the percentage of the total value of subcontracts entered into by the covered contractor awarded to small business concerns owned and controlled by service-disabled veterans;

''(D) the weighted average percentage goal negotiated by each covered contractor under section 8(d)(6)(A) for the utilization as subcontractors of small business concerns owned and controlled by service-disabled veterans for all contracts awarded by the Executive department to the covered contractor; and

''(E) for all contracts awarded to covered contractors by the Executive department that are completed during the 3-month period ending on the date of the report, the percentage of the total value of all subcontracts awarded by covered contractors that were awarded to small business concerns owned and controlled by service-disabled veterans.

''(3) RANKINGS.—For the first full fiscal year following the date of enactment of this subsection, and each fiscal year thereafter, the Administrator shall rank—

''(A) the Executive departments, based on—

''(i) the percentage of the total value of prime contracts awarded by the Executive departments to small business concerns owned and controlled by service-disabled veterans; and

''(ii) the percentage of the total value of subcontracts awarded by covered contractors that are awarded contracts by the Executive departments to small business concerns owned and controlled by service-disabled veterans; and

''(B) covered contractors, based on the percentage of the total value of subcontracts awarded by the covered contractors to small business concerns owned and controlled by service-disabled veterans.

''(4) PUBLICATION.—

''(A) WEBSITE.—Except as provided in subparagraph (B), the Administrator shall publish on a website accessible to the public a user-friendly, electronically searchable report containing—

''(i) the information submitted to the Administrator under paragraph (2); and

''(ii) the rankings made by the Administrator under paragraph (3).

''(B) EXCEPTION FOR NATIONAL SECURITY.—If the head of an Executive department determines that publication of information contained in a report submitted under paragraph (2) would be detrimental to national security, the Administrator shall not publish the information on the website described in subparagraph (A).

''(C) UPDATING.—The Administrator shall update the contents of the website described in subparagraph (A) not less frequently than quarterly.

''(5) REPORTS TO CONGRESS.—

''(A) ANNUAL REPORT.—The Administrator shall submit to Congress an annual report on the progress of each Executive department toward meeting the Government-wide goals for contracting and subcontracting established under subsection (g).

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

''(i) a statement of whether the website described in paragraph (4) contains the latest data reported to the Administrator by the Executive departments; and

''(ii) a recommendation of a prime contractor that should be recognized by Congress for outstanding progress in contracting with small business concerns owned and controlled by service-disabled veterans.

''(6) RULE OF CONSTRUCTION.—Nothing in this subsection may be construed to affect any other reporting requirement under Federal law.''.

AMENDMENTS SUBMITTED AND PROPOSED

SA 389. Mr. KOHL submitted an amendment intended to be proposed by him to the bill S. 782, to amend the Public Works and Economic Development Act of 1965 to reauthorize that Act, and for other purposes; which was ordered to lie on the table.

SA 390. Ms. SNOWE (for herself, Mr. COBURN, Mr. MCCONNELL, Mr. BARRASSO, Mr. BROWN of Massachusetts, Mr. MORAN, Mr. THUNE, Mr. ENZI, Ms. AYOTTE, and Mr. ISAKSON) submitted an amendment intended to be proposed by her to the bill S. 782, supra; which was ordered to lie on the table.

SA 391. Mr. MORAN submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 392. Mr. TESTER (for himself, Mr. CORKER, Mrs. HAGAN, Mr. CRAPO, Mr. BENNET, Mr. BLUNT, Mr. CARPER, Mr. KYL, and Mr. COONS) proposed an amendment to the bill S. 782, supra.

SA 393. Mr. DURBIN proposed an amendment to amendment SA 392 proposed by Mr. TESTER (for himself, Mr. CORKER, Mrs. HAGAN, Mr. CRAPO, Mr. BENNET, Mr. BLUNT, Mr. CARPER, Mr. KYL, and Mr. COONS) to the bill S. 782, supra.

SA 394. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 395. Mr. CORNYN submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 396. Mr. CORNYN (for himself and Mr. KYL) submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 397. Mr. CORNYN submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 398. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 399. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 400. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 401. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 402. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 403. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 404. Mr. DEMINT submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 405. Mr. BROWN of Massachusetts (for himself and Ms. SNOWE) submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 406. Mrs. HUTCHISON (for herself and Ms. LANDRIEU) submitted an amendment intended to be proposed by her to the bill S. 782, supra; which was ordered to lie on the table.

SA 407. Mr. CARDIN submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 408. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 409. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 410. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 411. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 412. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 413. Mr. MCCAIN submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

SA 414. Mr. PAUL submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table .

SA 415. Mr. BARRASSO (for himself and Mr. GRAHAM) submitted an amendment intended to be proposed by him to the bill S. 782, supra; which was ordered to lie on the table.

TEXT OF AMENDMENTS

SA 389. Mr. KOHL submitted an amendment intended to be proposed by him to the bill S. 782, to amend the Public Works and Economic Development Act of 1965 to reauthorize that Act, and for other purposes; which was ordered to lie on the table; as follows:

At the end of the bill, insert the following:

SEC. _____. NOPEC.

(a) SHORT TITLE.—This section may be cited as the ''No Oil Producing and Exporting Cartels Act of 2011'' or ''NOPEC''.

(b) SHERMAN ACT.—The Sherman Act (15 U.S.C. 1 et seq.) is amended by adding after section 7 the following:

''SEC. 7A. OIL PRODUCING CARTELS.

''(a) IN GENERAL.—It shall be illegal and a violation of this Act for any foreign state, or any instrumentality or agent of any foreign state, to act collectively or in combination with any other foreign state, any instrumentality or agent of any other foreign state, or any other person, whether by cartel or any other association or form of cooperation or joint action—

''(1) to limit the production or distribution of oil, natural gas, or any other petroleum product;

''(2) to set or maintain the price of oil, natural gas, or any petroleum product; or

''(3) to otherwise take any action in restraint of trade for oil, natural gas, or any petroleum product;

when such action, combination, or collective action has a direct, substantial, and reasonably foreseeable effect on the market, supply, price, or distribution of oil, natural gas, or other petroleum product in the United States.

''(b) SOVEREIGN IMMUNITY.—A foreign state engaged in conduct in violation of subsection (a) shall not be immune under the doctrine of sovereign immunity from the jurisdiction or judgments of the courts of the United States in any action brought to enforce this section.

''(c) INAPPLICABILITY OF ACT OF STATE DOCTRINE.—No court of the United States shall decline, based on the act of state doctrine, to make a determination on the merits in an action brought under this section.

''(d) ENFORCEMENT.—

''(1) IN GENERAL.—The Attorney General of the United States may bring an action to enforce this section in any district court of the United States as provided under the antitrust laws.

''(2) NO PRIVATE RIGHT OF ACTION.—No private right of action is authorized under this section.''.

(c) SOVEREIGN IMMUNITY.—Section 1605(a) of title 28, United States Code, is amended—

(1) in paragraph (5), by striking ''or'' after the semicolon;

(2) in paragraph (6), by striking the period and inserting ''; or''; and

(3) by adding at the end the following:

''(7) in which the action is brought under section 7A of the Sherman Act.''.

SA 390. Ms. SNOWE (for herself, Mr. COBURN, Mr. MCCONNELL, Mr. BARRASSO, Mr. BROWN of Massachusetts, Mr. MORAN, Mr. THUNE, Mr. ENZI, Ms. AYOTTE, and Mr. ISAKSON) submitted an amendment intended to be proposed by her to the bill S. 782, to amend the Public Works and Economic Development Act of 1965 to reauthorize that Act, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

TITLE _____—FREEDOM FROM RESTRICTIVE EXCESSIVE EXECUTIVE DEMANDS AND ONEROUS MANDATES

SEC. _____1. SHORT TITLE.

This title may be cited as the ''Freedom from Restrictive Excessive Executive Demands and Onerous Mandates Act of 2011''.

SEC. _____2. FINDINGS.

Congress finds the following:

(1) A vibrant and growing small business sector is critical to the recovery of the economy of the United States.

(2) Regulations designed for application to large-scale entities have been applied uniformly to small businesses and other small entities, sometimes inhibiting the ability of small entities to create new jobs.

(3) Uniform Federal regulatory and reporting requirements in many instances have imposed on small businesses and other small entities unnecessary and disproportionately burdensome demands, including legal, accounting, and consulting costs, thereby threatening the viability of small entities and the ability of small entities to compete and create new jobs in a global marketplace.

(4) Since 1980, Federal agencies have been required to recognize and take account of the differences in the scale and resources of regulated entities, but in many instances have failed to do so.

(5) In 2009, there were nearly 70,000 pages in the Federal Register, and, according to research by the Office of Advocacy of the Small Business Administration, the annual cost of Federal regulations totals $1,750,000,000,000. Small firms bear a disproportionate burden, paying approximately 36 percent more per employee than larger firms in annual regulatory compliance costs.

(6) All agencies in the Federal Government should fully consider the costs, including indirect economic impacts and the potential for job loss, of proposed rules, periodically review existing regulations to determine their impact on small entities, and repeal regulations that are unnecessarily duplicative or have outlived their stated purpose.

(7) It is the intention of Congress to amend chapter 6 of title 5, United States Code, to