The programs authorized under this Act and the amendments made by this Act, including the extent to which such programs have been funded and implemented and have contributed to the job creation among small business concerns.

SUBMITTED RESOLUTIONS

SENATE CONCURRENT RESOLUTION 54—STATING THAT IT IS THE POLICY OF THE UNITED STATES TO OPPOSE THE SALE, SHIPMENT, PERFORMANCE OF MAINTENANCE, REFURBISHMENT, MODIFICATION, REPAIR, AND UPGRADE OF ANY MILITARY EQUIPMENT FROM OR BY THE RUSSIAN FEDERATION TO OR FOR THE SYRIAN ARAB REPUBLIC

Mr. HATCH (for himself and Mr. CORNYN) submitted the following concurrent resolution; which was referred to the Committee on Foreign Relations:

S. CON. RES. 54

Whereas the General Director of Rosoboronexport, the largest Russian arms exporter, recently announced that his company was transferring anti-aircraft and anti-ship missile systems to Syria;

Whereas the Government of the Russian Federation has deployed 11 warships, including amphibious ships designed to carry naval infantry, to the eastern Mediterranean, and it is expected that some of those ships will dock at the Syrian port of Tartus;

Whereas Secretary of State Hillary Clinton recently stated, "What can every nation and group represented here do? . . . I ask you to reach out to Russia and China, and to not only urge but demand that they get off the sidelines and begin to support the legitimate aspirations of the Syrian people.";

Whereas Secretary of State Clinton further stated on July 17, 2012, "[O]ur commitment is to try to get Russia to cooperate. So we want the West to put pressure on Russia . . . as long as he [Bashar al-Assad] has Russia uncertain about whether or not to side against him in any more dramatic way that it already has, he [Assad] feels like he can keep going.";

Whereas the Government of the Russian Federation recently refurbished at least three Syrian Mi-25 helicopters; and

Whereas the Government of the Russian Federation has taken a tentative positive step of expounding a new policy that it will not enter into new arms agreements with the Government of the Syrian Arab Republic: Now, therefore, be it

Resolved by the Senate (the House of Representatives concurring), That it is the policy of the United States—

(1) to oppose the sale, shipment, performance of maintenance, refurbishment, modification, repair, and upgrade of any military equipment, including parts that can be used in military equipment, from or by the Government of the Russian Federation to or for the Government of the Syrian Arab Republic; and

(2) to oppose any effort by the Government of the Russian Federation to increase, maintain, or support the military readiness of the military capabilities of the Government of the Syrian Arab Republic.

AMENDMENTS SUBMITTED AND PROPOSED

SA 2573. Mr. HATCH (for himself, Mr. MCCONNELL, Mr. JOHANNS, Mr. ROBERTS, Mr. BURR, Mr. THUNE, Mr. CORNYN, Mr. KLY, Mr. BOOZMAN, Mr. BLUNT, Mr. RUBIO, Mr. MCCAIN, Mr. GRASSLEY, Mr. BARRELL, Mr. KIRK, Mrs. HUTCHISON, Mr. HOEVEN, Mr. SHEPHERD, and Mr. ISAKSON) proposed an amendment to the bill S. 3412, to amend the Internal Revenue Code of 1986 to provide tax relief to middle-class families.

SA 2574. Mrs. HUTCHISON submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table.

SA 2575. Mr. LAUTENBERG (for himself, Mrs. BOXER, Mr. REED, Mr. MENendez, Mrs. GILLIBRAND, Mr. SCHUMER, and Mrs. FRIEDBERG) submitted an amendment intended to be proposed by him to the bill S. 3414, supra, which was ordered to lie on the table.

SA 2576. Mr. LEAHY submitted an amendment intended to be proposed by him to the bill S. 3414, supra, which was ordered to lie on the table.

SA 2577. Mr. LEAHY submitted an amendment intended to be proposed by him to the bill S. 3414, supra, which was ordered to lie on the table.

SA 2578. Mr. LEAHY submitted an amendment intended to be proposed by him to the bill S. 3414, supra, which was ordered to lie on the table.

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

SA 2580. Mr. LEAHY submitted an amendment intended to be proposed by him to the bill S. 3414, supra, which was ordered to lie on the table.

TEXT OF AMENDMENTS

SA 2573. Mr. HATCH (for himself, Mr. MCCONNELL, Mr. JOHANNS, Mr. ROBERTS, Mr. BURR, Mr. THUNE, Mr. CORNYN, Mr. KLY, Mr. BOOZMAN, Mr. BLUNT, Mr. RUBIO, Mr. MCCAIN, Mr. GRASSLEY, Mr. BARRELL, Mr. KIRK, Mrs. HUTCHISON, Mr. HOEVEN, Mr. SHEPHERD, and Mr. ISAKSON) proposed an amendment to the bill S. 3412, to amend the Internal Revenue Code of 1986 to provide tax relief to middle-class families; as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE. This Act may be cited as the “Tax Hike Prevention Act of 2012”.

SEC. 2. TEMPORARY EXTENSION OF 2001 TAX RELIEF.

(a) IN GENERAL.—Section 901 of the Economic Growth and Tax Relief Reconciliation Act of 2001 is amended by striking “December 31, 2012” both places it appears and inserting “December 31, 2013”.

(b) EFFECTIVE DATE.—The amendment made by this section shall take effect as if included in the enactment of the Economic Growth and Tax Relief Reconciliation Act of 2001.

SEC. 3. TEMPORARY EXTENSION OF 2003 TAX RELIEF.

(a) IN GENERAL.—Section 303 of the Jobs and Growth Tax Relief Reconciliation Act of 2003 is amended by striking “December 31, 2013” both places it appears and inserting “December 31, 2014”.

(b) EFFECTIVE DATE.—The amendment made by this section shall take effect as if
made by this section shall apply to taxable

QUALIFIED REAL PROPERTY.—

AMOUNT.—

striking paragraph (6).

SEC. 6. INSTRUCTIONS FOR TAX REFORM.

on Finance shall report legislation not later

than 12 months after the date of the enactment
of this Act that consists of changes in laws within its jurisdiction which meet the requirements of subsection (b).

(b) Regulations issued under this section meet the requirements of this subsection if the legis-
lation—

(1) simplifies the Internal Revenue Code of 1986 by reducing the number of tax prefer-
ences and reducing individual tax rates proportionally, with the highest individual tax rate significantly below 35 percent;

(2) permanently repeals the alternative minimum tax;

(3) is projected, when compared to the cur-
rent tax policy baseline, to stimulate economic growth and lead to in-
creased revenue;

(4) applies any increased revenue from stimu-
lated economic growth to additional rate reductions and does not permit any such increased revenue to be used for additional Federal spending;

(5) retains a progressive tax code; and

(6) provides for revenue-neutral reform of the taxation of corporations and businesses by—

(A) providing a top tax rate on corpora-
tions of no more than 25 percent; and

(B) implementing a competitive territorial tax system.

SA 2574. Mrs. HUTCHISON submitted an amendment intended to be proposed by her to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end of the bill, add the following:

TITLE VIII—MISCELLANEOUS

SEC. 801. COMPLIANCE WITH OR VIOLATION OF ENVIRONMENTAL LAWS WHILE UNDER EMERGENCY ORDER.

(a) IN GENERAL.—Section 202(c) of the Federal Power Act (16 U.S.C. 824a(c)) is amended—

(1) by striking “(c) During” and inserting the following:

(c) TEMPORARY CONNECTION OR CONSTRUCTION OF CERTAIN REAL PROPERTY AS SECTION 179 PROPERTY.

(b) Temporary Extension of Increased Alternative Minimum Tax Exemption Amount.

(1) IN GENERAL.—Paragraph (1) of section 55(d) of the Internal Revenue Code of 1986 is amended—

(A) by striking “$72,450” and all that follows through “2011” in subparagraph (A) and inserting “$70,750 in the case of taxable years beginning in 2012 and $79,850 in the case of taxable years beginning in 2013”, and

(B) by striking “$45,000” and all that follows through “2011” in subparagraph (B) and inserting “$50,600 in the case of taxable years beginning in 2012 and $51,150 in the case of taxable years beginning in 2013”.

(b) Temporary Extension of Alternative Minimum Tax Relief for Nonrefundable Personal Credits.

(1) IN GENERAL.—Paragraph (2) of section 26(a) of the Internal Revenue Code of 1986 is amended—

(A) by striking “or 2011” and inserting “2011, 2012, or 2013”, and

(B) by striking “2011” in the heading thereof and inserting “2013”.

(c) EFFECTIVE.—The amendments made by this section shall apply to taxable years beginning after December 31, 2011.

SEC. 5. EXTENSION OF INCREASED EXPENSING LIMITATIONS AND TREATMENT OF CERTAIN REAL PROPERTY AS SECTION 179 PROPERTY.

(a) IN GENERAL.—Section 179(b)(1) of the Internal Revenue Code of 1986 is amended—

(A) by striking “2010 or 2011,” in subpara-
graph (B) and inserting “2010, 2011, 2012, or 2013,” and

(B) by striking subparagraph (C), (D) or redesignating subparagraph (D) as subpara-
graph (C), and

(D) in subparagraph (C), as so redesignated, by striking “2012” and inserting “2013”.

(b) REDUCTION IN LIMITATION.—Section 179(b)(2) of such Code is amended—

(A) by striking “2010 or 2011,” in subpara-
graph (B) and inserting “2010, 2011, 2012, or 2013,” and

(B) by striking subparagraph (C), (D) or redesignating subparagraph (D) as subpara-
graph (C), and

(D) in subparagraph (C), as so redesignated, by striking “2012” and inserting “2013”.

(c) CONFORMING AMENDMENT.—Subsection (b) of section 179 of such Code is amended by striking paragraph (6).

(d) COMPUTER SOFTWARE.—Section 179(d)(1)(A)(vi) of the Internal Revenue Code of 1986 is amended by striking “2013” and inserting “2014”.

(e) ELECTION.—Section 179(d)(2) of the Internal Revenue Code of 1986 is amended by striking “2013” and inserting “2014”.

(f) SPECIAL RULES FOR TREATMENT OF QUALIFIED REAL PROPERTY.


(2) CARRYOVER LIMITATION.—

(A) IN GENERAL.—Section 179(f)(4) of such Code is amended by striking “2011” each place it appears and inserting “2013”.

(B) CONFORMING AMENDMENT.—The heading for subparagraph (C) of section 179(f)(4) of such Code is amended by striking “2010” and inserting “2013”.

(C) EFFECTIVE DATE.—The amendments made by this section shall apply to taxable years beginning after December 31, 2011.

SEC. 6. INCOME TAX REFORM.

(a) IN GENERAL.—The Senate Committee on Finance shall report legislation not later

than 12 months after the date of the enactment of this Act that consists of changes in laws within its jurisdiction which meet the requirements of subsection (b).

(b) Regulations issued under this section meet the requirements of this subsection if the legis-
lation—

(1) simplifies the Internal Revenue Code of 1986 by reducing the number of tax pref-
erences and reducing individual tax rates proportionally, with the highest individual tax rate significantly below 35 percent;

(2) permanently repeals the alternative minimum tax;

(3) is projected, when compared to the cur-
rent tax policy baseline, to stimulate economic growth and lead to in-
creased revenue;

(4) applies any increased revenue from stimu-
lated economic growth to additional rate reductions and does not permit any such increased revenue to be used for additional Federal spending;

(5) retains a progressive tax code; and

(6) provides for revenue-neutral reform of the taxation of corporations and businesses by—

(A) providing a top tax rate on corpora-
tions of no more than 25 percent; and

(B) implementing a competitive territorial tax system.

SA 2575. Mr. LAUTENBERG (for himself, Mrs. BOXER, Mr. REED, Mr. MENEN-dez, Mrs. GILLIBRAND, Mr. SCHUMER, and Mrs. FEINSTEIN) submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the appropriate place, insert the follow-

SEC. 3. PROHIBITION ON TRANSFER OR POSSESSION OF LARGE CAPACITY AMMUNITION FEEDING DEVICES.

(a) DEFINITION.—Section 921(a) of title 18, United States Code, is amended by inserting after paragraph (29) the following:

“(30) The term ‘large capacity ammunition feeding device’—

(A) means a magazine, belt, drum, feed strip, or similar device that has a capacity of, or that can be readily restored or con-
verted to accept, more than 10 rounds of am-
munition; but

(B) does not include an attached tubular device designed to accept, and capable of op-
erating only with .22 caliber rimfire ammu-
nition;

(b) PROHIBITIONS.—Section 922 of such title is amended by inserting after subsection (a) the following:

“(v)(A)(i) Except as provided in clause (ii), any person who transfers or possesses a large capacity ammun-
ition feeding device.
(ii) Clause (i) shall not apply to the possession of a large capacity ammunition feeding device otherwise lawfully possessed within the United States on or before the date of the enactment of this Act.

(B) It shall be unlawful for any person to import or bring into the United States a large capacity ammunition feeding device.

(C) (A) A manufacture for, transfer to, or possession by the United States or a department or agency of the United States of a State or a department, agency, or political subdivision of a State, or a transfer to or possession by a law enforcement officer employed by such a State or a department, agency, or political subdivision of a State, or a department, agency, or political subdivision of a State, of a large capacity ammunition feeding device transferred to the individual by the agency upon that requirement; or

(D) A manufacture, transfer, or possession of a large capacity ammunition feeding device transferred to the individual by the agency upon that requirement.

SEC. 2576. Mr. LEAHY submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

- TABLE VIII—DATA SECURITY

SEC. 801. DEFINITIONS.

In this title, the following definitions shall apply:

(A) 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.

(B) A non-truncated social security number.

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

(D) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code.

(E) Any combination of the following data elements:

- An individual’s first and last name or initial and last name.
- A non-truncated social security number.
- A university issued unique identification number or other government-issued unique identification number.
- A unique biometric data such as a fingerprint, voice print, a retina or iris image, or any other unique physical representation.
- A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code.

(F) Any combination of the following data elements:

- An individual’s first and last name or initial and last name.
- An account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code.

III. Any security code, access code, or password, or source code that could be used to generate such codes or passwords.

SEC. 802. PURPOSE AND APPLICABILITY OF DATA PRIVACY AND SECURITY PROGRAM.

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

(b) APPLICABILITY.—A business entity engaging in interstate commerce that involves collecting, accessing, 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 803 for protecting sensitive personally identifiable information.

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

- Financial institutions.

- Financial institutions.

- Financial institutions.

- Financial institutions.

- Financial institutions.

- Financial institutions.

- Financial institutions.

- Financial institutions.

- Financial institutions.
obtained from a public record, including informa-
tion obtained from a news report or peri-
drical.

(d) SAFE HARBORS.—

(1) A business entity shall be deemed to be in compliance with the privacy and security program requirements under section 803 if the business entity complies with or provides a comprehensive personal data privacy and security program that includes administrative, technical, or physical safeguards 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 deemed to permit, and nothing does permit, the Federal Trade Commission to issue regulations requiring, or according any decisional status to, the implementation of or application of a specific technology or technological specifications for meeting the provisions of this title.

SEC. 803. REQUIREMENTS FOR A PERSONAL DATA PRIVACY AND SECURITY PROGRAM.

(a) PERSONAL DATA PRIVACY AND SECURITY PROGRAM.—A business entity subject to this title shall comply with the following safeguards that are administered administratively, technical, or physical safeguards identified by the Federal Trade Commission in a rule-making process pursuant to section 553 of title 5, United States Code, for the protection of sensitive personally identifiable information:

(1) PRIVACY.—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:

(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) prevent 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 from 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 or systems containing 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 or systems containing 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) VULNERABILITY TESTING.—Each business entity shall:

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

(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 to authenticate and permit access only to authorized individuals;

(ii) detect, record, and preserve information pertaining to unauthorized and attempted fraud, 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, or 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 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 altered 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; and

(C) establish a plan and procedures for minimizing the amount of sensitive personally identifiable information maintained by such business entity, which shall provide for the retention of sensitive personally identifiable information only as reasonably needed for the business purposes of such business entity or as necessary to comply with any legal obligation.

(5) RISK MANAGEMENT AND CONTROL.—Each business entity subject to this title 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 title 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 assessed to the business entity under subsection (a)(3).

(d) RELATIONSHIP TO CERTAIN PROVIDERS OF SERVICES.—In the event a business entity subject to this title engages a person or entity not subject to this title (other than a service provider) to perform functions on behalf of and under the instruction of such business entity, such business entity shall—

(1) exercise appropriate due diligence in selecting the person or entity, including the responsibilities related to sensitive personally identifiable information, and take reasonable steps to select and retain a person or entity that is capable of maintaining appropriate safeguards for the security, privacy, and integrity of the sensitive personally identifiable information involved at issue and any provisions governing entities subject to this section.

(2) require the person or entity by contract to implement and maintain appropriate measures designed to meet the objectives and any provisions governing entities subject to this section.

(e) PERIODIC ASSESSMENT AND PERSONAL DATA PRIVACY AND SECURITY MODERNIZATION.—Each business entity subject to this title 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.

SEC. 804. ENFORCEMENT.

(a) CIVIL PENALTIES.—

(1) IN GENERAL.—Any business entity that violates the provisions of section 803 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 section 803 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) PENALTY LIMITS.—

(A) IN GENERAL.—Notwithstanding any other provision of this title, the total sum of civil penalties assessed against a business entity for all violations of the provisions of this title resulting from the same or related acts and omissions shall not exceed $500,000, unless such conduct is found to be willful or intentional.

(B) DETERMINATIONS.—The determination of whether a violation of this title has occurred, and if so, the amount of the penalty to be imposed, if any, shall be made by the court sitting as the finder of fact.

(C) ADDITIONAL PENALTY LIMIT.—If a court determines under subparagraph (B) that a violation of this title was willful or intentional and imposes an additional penalty, the court may not impose an additional penalty in an amount that exceeds $500,000.

(d) EQUITABLE RELIEF.—A business entity engaged in interstate commerce that violates a provision of this title may be enjoined by a court, from further violations by a United States district court.

(e) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this section are cumulative and shall in no way affect or prevent any other rights and remedies available under law.
(b) Federal Trade Commission Authority.—Any business entity shall have the provisions of this title enforced against it by the Federal Trade Commission.

(c) Other Enforcement Agency.—

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 threatened or is threatened or adversely affected by the acts or practices of a business entity that violate this title, the State may bring a civil action against the resident of that State in a district court of the United States of appropriate jurisdiction to—

(A) enjoin that act or practice;

(B) provide the notice described in this subsection; and

(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) Penalties Limit.—

(A) In General.—Notwithstanding any other provision of law, the total sum of civil penalties assessed against a business entity for all violations of the provisions of this title resulting from the same or related acts or omissions shall not exceed $500,000, unless such conduct is found to be willful or intentional.

(B) Determinations.—The determination of whether a violation of a provision of this title has occurred, and if so, the amount of the penalty to be imposed, if any, shall be made by the court sitting as the finder of fact. No court determination of whether a violation of a provision of this title was willful or intentional, and if so, the amount of the additional penalty to be imposed, if any, shall be made by the court sitting as the finder of fact.

(C) Additional Penalty Limit.—If a court determines under subparagraph (B) that a violation of a provision of this title was willful or intentional and imposes an additional penalty, the court may not impose an additional penalty in an amount that exceeds $500,000.

(3) Notice.—

(A) In General.—Before filing an action under this section, 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.

(4) Federal Trade Commission Authority.—Upon receiving notice under paragraph (3), the Federal Trade Commission shall have the right to—

(A) move to stay the action, pending the final determination of whether a business professional proceeding or action described in paragraph (5);

(B) intervene in an action brought under paragraph (3) as an interested party;

(C) file petitions for appeal.

(5) Pending Proceedings.—If the Federal Trade Commission initiates a Federal civil action in any case under this title, any regulatory proceedings thereunder, no attorney general of a State may bring an action for a violation of this title that resulted from the same or related acts or omissions against a defendant named in the Federal civil action initiated by the Federal Trade Commission.

(6) 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 in good faith the powers and responsibilities of 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.

(7) 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 shall create a private cause of action for a business entity for violation of any provision of this title.

SEC. 805. RELATION TO OTHER LAWS.

(a) In General.—No business entity shall require any business entity subject to this title to comply with any requirements with respect to administrative, technical, and physical safeguards for the protection of personal information.

(b) Limitations.—Nothing in this title 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.

SA 2578. Mr. LEAHY submitted an amendment intended to be proposed by him to the bill S. 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end, add the following:

DIVISION —DATA BREACHES

SECTION 1. SHORT TITLE.

This division may be cited as the “Personal Data Privacy and Security Act of 2012”.

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, national security, homeland security, cybersecurity, the development of commerce, and the privacy rights of Americans;

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

(4) 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;

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

(6) 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;

(7) government access to commercial data can potentially improve safety, law enforcement and national security operations, and there is a need for Congress to exercise oversight over government use of commercial data.

SEC. 3. DEFINITIONS.

In this division, the following definitions shall apply:

(1) AFFILIATE.—The term “affiliate” means persons related by common ownership or by corporate control.

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

(3) BUSINESS ENTITY.—The term “business entity” means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture entity designated by the Secretary of Homeland Security under section 206(a).

(4) DATA SYSTEM COMMUNICATION INFORMATION.—The term “data system communication information” means information that identifies the origin, direction, destination, processing, transmission, or termination of each communication initiated, attempted, or received.

(5) DESIGNATED ENTITY.—The term “designated entity” means the Federal Government entity designated by the Secretary of Homeland Security under section 206(a).

(6) 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 generally accepted by experts in the field of information security that renders such data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data; and

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

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

(8) PERSONALLY IDENTIFIABLE INFORMATION.—The term “personally identifiable information” means any information, or combination of information, in electronic or physical form, that can be used, alone or in combination with other information, to identify or contact a particular individual, including but not limited to—

(A) personally identifiable information to adopt reasonable procedures to ensure the security, privacy, and confidentiality of that personally identifiable information;

(B) information to adopt reasonable procedures to ensure the security, privacy, and confidentiality of that personally identifiable information;

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

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


SEC. 101. 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)(2) SERVICE PROVIDER.—The term "service provider", means any information or compilation of information, in electronic or digital form that includes the following:

(i) An individual's first and last name or first initial and last name.

(ii) A unique account identifier, including any resident of the United States whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed, or acquired.

(iii) Any security code, access code, or password, or source code that could be used to generate such codes or passwords.

(2) NONEXCLUSIVITY.—The authority granted under subsection (a) shall have the authority to investigate offenses under this section.

(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 sensitive personally identifiable information."

TITLE II—SECURITY BREACH NOTIFICATION

SEC. 201. NOTICE TO INDIVIDUALS.

(a) In General.—Any agency, or business entity engaged in interstate commerce, other than a service provider, that uses, accesses, transmits, stores, transmits, stores, or provides access, transmit, stores, or provides of or collects sensitive personally identifiable information, shall, upon notification that sensitive personally identifiable information subject to the security breach 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, other than a service provider, that uses, accesses, transmits, stores, or provides access, transmit, stores, or provides 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 sensitive personally identifiable information subject to the security breach, to provide the notifications required under subsection (a)."
(3) Law enforcement immunity.—No nonconstitutional cause of action shall lie in any court against any agency for acts relating to the delay of notification for law enforcement or national security purposes under this title.

(e) Limitations.—Notwithstanding any other obligation under this title, this title does not apply to the following:

(1) Financial institutions.—Financial institutions—

(A) subject to the data security requirements under section 503(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6803(b)); and

(B) subject to the jurisdiction of an agency or authority described in section 503(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6805(a)).

(2) HIPAA 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 division if the business entity—

(i) acting as a covered entity and as a business associate, as those terms are defined under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.), including the data security requirements imposed under that Act and implementing regulations promulgated under that Act; and

(ii) subject to, and currently in compliance with, the data breach notification, privacy and data security requirements under the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17922) and implementing regulations promulgated thereunder; or

(2) HIPAA regulated entities.—

(A) Covered entities.—Covered entities subject to section 501(b) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.), including the data security requirements imposed under that Act and implementing regulations promulgated under that Act; and

(B) Business entities.—A business entity shall be deemed in compliance with this division if the business entity—

(i) acting as a covered entity and as a business associate, as those terms are defined under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.), including the data security requirements imposed under that Act and implementing regulations promulgated under that Act; and

(ii) subject to, and currently in compliance with, the data breach notification, privacy and data security requirements under the Health Information Technology for Economic and Clinical Health (HITECH) Act (42 U.S.C. 17001), including the data breach notification requirements and implementing regulations of that Act.

SEC. 202. Exemptions

(a) Exemption for national security and law enforcement purposes.—

(1) In general.—Section 201 shall not apply to an agency or business entity if—

(A) the United States Secret Service or the Federal Bureau of Investigation determines that notification of the security breach could be expected to reveal sensitive sources and methods or similarly impair the ability of the United States to conduct law enforcement investigations; or

(B) the Federal Bureau of Investigation determines that notification of the security breach could be expected to cause damage to the national security.

(2) Immunity.—No nonconstitutional cause of action shall lie in any court against any Federal agency for acts relating to the exemption from notification for law enforcement or national security purposes under this title.

(b) Sunny Harbor.—

(1) In general.—An agency or business entity shall be exempt from the notification requirements under section 201 if—

(A) a risk assessment conducted by the agency or business entity concludes that, based upon the information available, there is no significant risk that a security breach has occurred in, or will result in, identity theft, economic loss or harm, or physical harm to the individuals whose sensitive personally identifiable information was subject to the breach;

(B) without unreasonable delay, but not later than 45 days after the discovery of a security breach, unless extended by the Federal Trade Commission, the agency or business entity notifies the Federal Trade Commission, in writing, of—

(i) the receipt of the risk assessment; and

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

(C) the Federal Trade Commission does not indicate, within 10 business days from receipt of the decision, that notice should be given.

(2) Rebuttable presumptions.—For purposes of paragraph (1), the following shall apply:

(A) the encryption of sensitive personally identifiable information described in paragraph (1)(A) shall establish a rebuttable presumption that no significant risk exists; and

(B) the rendering of sensitive personally identifiable information described in paragraph (1)(A) unusable, unreadable, or indecipherable through data security technology or methodology that is generally accepted by experts in the field of information security, such as reduction or access controls shall establish a rebuttable presumption that no significant risk exists.

(3) Violation.—It shall be a violation of this section to—

(A) fail to conduct the risk assessment in a reasonable manner, or according to standards generally accepted by experts in the field of information security; or

(B) submit a false or misleading risk assessment that contains fraudulent or deliberately misleading information.

(c) Financial fraud prevention exemptions.—

(1) In general.—A business entity will be exempt from the notice requirement under section 201 if the business entity utilizes or participates in a financial fraud prevention program that—

(A) effectively blocks the use of the sensitive personally identifiable information to initiate unauthorized financial transactions or to otherwise cause harm 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 in paragraph (1) does not apply if the information subject to the security breach includes an individual’s first and last name, or any other type of sensitive personally identifiable information as defined in section 3, unless that information is maintained about that individual; and

(3) Financial fraud prevention exemptions.—

(a) Designation of government entity to receive notice.—

(1) In general.—Not later than 60 days after the date of enactment of this Act, the Secretary of Health and Human Services shall designate a Federal Government entity to receive the notices required under section 201 and this section, and any other reports and information about security incidents, threats, and vulnerabilities.

(b) Responsibilities of the designated entity.—The designated entity shall—

(1) promptly provide the information that it receives to the United States Secret Service and the Federal Bureau of Investigation; and

(2) Designation of government entity to receive notice.—

(a) In general.—An agency or business entity that has a direct relationship with the individual being notified shall be responsible for providing the information to the Federal Trade Commission for civil law enforcement purposes; and

(b) Provide the information described in subparagraph (A) as appropriate to other consumers reporting agencies that compile and maintain files on consumers on a nationwide basis (as defined in section 6803(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)) of the personal credit information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person exceeds 5,000.

(2) The security breach involves a database, networked or integrated databases, or other data systems containing a sensitive personally identifiable information of more than 500,000 individuals nationwide.

(3) The security breach involves databases owned or controlled by the Federal Deposit Insurance Corporation.

(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.
(c) INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.—
(1) IN GENERAL.—If it appears that a business entity has engaged in conduct constituting a violation of this title, 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 title.
(2) ISSUANCE OF ORDER.—A court may issue an order under paragraph (1), if after a hearing and findings of fact, finds that the conduct in question constitutes a violation of this title.
(d) CIVIL ACTIONS BY THE FEDERAL TRADE COMMISSION.—
(1) IN GENERAL.—Compliance with the requirements imposed under this title may be enforced by the Federal Trade Commission (15 U.S.C. 41 et seq.) by the Federal Trade Commission with respect to business entities subject to this division. All of the civil penalties and powers under the Federal Trade Commission Act under this title are enforceable by the Federal Trade Commission under the Federal Trade Commission Act are available to the Federal Trade Commission to enforce compliance by any person with the requirements imposed under this title.
(2) PENALTY LIMITATION.—(A) In determining whether a violation of a provision of this title has occurred, and if so, the amount of the penalty to be imposed, any, shall be made by the court sitting as the finder of fact. The determination of whether a violation of a provision of this title was willful or intentional, and if so, the amount of the additional penalty in an amount that exceeds $1,000,000, unless such conduct is found to be willful or intentional.
(B) DETERMINATIONS.—The determination of whether a violation of a provision of this title has occurred, and if so, the amount of the penalty to be imposed, if any, shall be made by the court sitting as the finder of fact.
(3) ADDITIONAL PENALTY LIMIT.—If a court determines under subparagraph (B) that a violation of a provision of this title was willful or intentional and imposes an additional penalty, the court may not impose an additional penalty in an amount that exceeds $1,000,000.
(4) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—The Federal Trade Commission may enforce civil violations of the Federal Trade Commission Act (15 U.S.C. 41a et seq.) regarding unfair or deceptive acts or practices and shall be subject to enforcement by the Federal Trade Commission under this division, not later than 180 days after the enactment of this Act, the Attorney General, issue such other regulations as it determines to be necessary to carry out this title. All regulations promulgated under this division shall be issued in accordance with section 553 of title 5, United States Code. Such regulations may relate to customer proprietary network information, the promulgation of such regulations will be coordinated with the Federal Communications Commission.
(g) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this title are cumulative and shall not affect any other rights and remedies available under law.

SEC. 208. 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 of 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 title, the Attorney General of the United States, in consultation with the Attorney General of the State or local law enforcement agency or 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 any court of the United States of appropriate jurisdiction to—
(A) enjoin that practice;
(B) enforce compliance with this title; or
(C) civil penalties of not more than $11,000 per day per security breach up to a maximum of $1,000,000 per violation, unless such conduct is found to be willful or intentional.
(b) PENALTY LIMITATION.—
(A) IN GENERAL.—Notwithstanding any other provision of law, the total amount of the civil penalties assessed against a business entity for any violation of this title resulting from the same or related acts or omissions may not exceed $1,000,000, unless such conduct is found to be willful or intentional.
(2) DETERMINATIONS.—The determination of whether a violation of a provision of this title has occurred, and if so, the amount of the penalty to be imposed, if any, shall be made by the court sitting as the finder of fact.
(3) ADDITIONAL PENALTY LIMIT.—If a court determines under subparagraph (B) that a violation of a provision of this title was willful or intentional and imposes an additional penalty, the court may not impose an additional penalty in an amount that exceeds $1,000,000.
(4) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—The Federal Trade Commission may initiate investigations under this division, not later than 180 days after the enactment of this Act, the Attorney General, issue such other regulations as it determines to be necessary to carry out this title. All regulations promulgated under this division shall be issued in accordance with section 553 of title 5, United States Code. Such regulations may relate to customer proprietary network information, the promulgation of such regulations will be coordinated with the Federal Communications Commission.

SEC. 209. ENFORCEMENT.—
(a) NOTICE.—
(1) 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—
(A) written notice of the action; and
(B) a copy of the complaint for the action.
(B) EXEMPTION.—
In General.—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under this title, 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) Notice Under Subsection.—Upon receiving notice under subsection (a)(3), 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 207 and move to consolidate all pending actions, including State actions, in such court;

(3) intervene in an action brought under subsection (a)(1); and

(4) file petitions for appeal.

(c) Pending Proceedings.—If the Attorney General or the Federal Trade Commission initiate a criminal proceeding or civil action for a violation of a provision of this title, or any regulations thereunder, no attorney general of a State may bring an action for a violation of a provision of this title against a defendant named in the Federal criminal proceeding or civil action.

(d) Construction.—For purposes of bringing an action under subsection (a), nothing in this title 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) require the testimony of witnesses or the production of documentary and other evidence.

(e) Venue.—Service of Process.—(1) 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 title establishes a private cause of action against a business entity for violation of any provision of this title.

SEC. 209. EFFECT ON FEDERAL AND STATE LAW.

For any entity, or agency that is subject to this title, the provisions of this title shall supersede, to the extent that they provide greater protection of personal information than any provision of Federal law, or any provisions of the law of any State, relating to notification of a security breach, except as provided in section 204(b). Nothing in this title shall be construed to modify, limit, or supersede the operation of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) or its implementing regulations, including any regulations adopted or enforced by States, the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d, including its implementing regulations, or the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17971) or its implementing regulations.

SEC. 210. REPORTING ON EXEMPTIONS.

(a) FTC Report.—Not later than 18 months after the date of enactment of this Act, and upon request by Congress thereafter, the Federal Trade Commission shall submit a report to Congress on the number and nature of the security breaches described in the notices of noncompliance inviolation of the risk assessment exemption under section 202(b) and their response to such notices.

(b) Law Enforcement Report.—(1) In General.—Not later than 18 months after the date of enactment of this Act, and upon request by Congress thereafter, the Attorney General and the Federal Bureau of Investigation shall submit a report to Congress on the number and nature of security breaches subject to the national security and law enforcement exemptions under section 202(a).

(2) Requirement.—The report required under paragraph (1) shall include the contents of any risk assessment provided to the United States Secret Service and the Federal Bureau of Investigation under this title.

SEC. 211. EFFECTIVE DATE.

This title shall take effect 90 days after the date of enactment of this Act.

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

SEC. 301. BUDGET COMPLIANCE.

The budgetary effects of this division, for the purpose of complying with the Statutory Pay-As-You-Go Act of 2010, shall be determined by reference to the latest statement of deficit or surplus submitted by the President to the Congress. The budgetary effects for this division, submitted for printing in the Congressional Record by the Chairman of the Senate Budget Committee, were provided to Congress prior to the vote on passage.

SA 2579. Mr. LEAHY submitted an amendment (see page S5348) proposed by him to the bill S 3414, to enhance the security and resiliency of the cyber and communications infrastructure of the United States; which was ordered to lie on the table; as follows:

At the end, insert the following:

TITLE.—CYBER CRIME PROTECTION ACT

SEC. 303. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1028(e)(6) of title 18, United States Code, is amended by inserting “section 1030 (relating to fraud and related activity in connection with computers)” after “the act is a felony,” before “the invoice.

SEC. 304. TRAFFICKING IN PASSWORDS.

Section 1030(a) of title 18, United States Code, is amended by striking paragraph (6) and inserting the following:

“(f) knowingly and with intent to defraud traffic (as defined in section 1029) in—

“(A) any password or similar information or means of access through which a computer can be accessed; or

“(B) a computer password or similar information or means of access through which a computer can be accessed without authorization; and

“(C) any computer access covered by paragraph (1) or (2) of section 1029(c), or any password or similar information or means of access through which a computer can be accessed without authorization.”

SEC. 305. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD.

Section 1030(b) of title 18, United States Code, is amended by inserting “for the completed offense” after “punished as provided”.

SEC. 306. CRIMINAL ACTION FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030(c) of title 18, United States Code, is amended by striking sections (1) and (3) and inserting the following:

(i) the offense was committed in the furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States, or of any State; or

(ii) the offense was committed for financial gain;

(iii) the offense was committed in violation of the Constitution or laws of the United States, or of any State; or

(iv) the offense was committed for financial gain;

(v) the offense was committed in violation of the Constitution or laws of the United States, or of any State; or

(vi) the offense was committed for financial gain;

(vii) the offense was committed in violation of the Constitution or laws of the United States, or of any State; or

(viii) the offense was committed for financial gain;
"(i) CRIMINAL FORFEITURE.— 
"(1) The court, in imposing sentence on any person convicted of a violation of this section, or of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States— 
"(A) any interest in any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of any violation of this section, or a conspiracy to violate this section. 
"(B) any property, real or personal, constituting or derived from any gross proceeds, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of such violation. 
"(2) The criminal forfeiture of property under this subsection, including any seizure and disposition of the property, and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section. 
"(j) CIVIL FORFEITURE.— 
"(1) The following shall be subject to forfeiture to the United States and no property right, real or personal, shall exist in them: 
"(A) Any property, real or personal, that was used, or intended to be used, to commit or facilitate the commission of any violation of this section, or a conspiracy to violate this section. 
"(B) Any property, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, as a result of the commission of any violation of this section, or a conspiracy to violate this section. 
"(2) Forfeitures under this subsection shall be governed by the provisions in chapter 46 of title 18, United States Code, relating to civil forfeitures, except subsection (b) shall be fined under this title, in whole or in part, only with another term of imprisonment to be imposed for a violation of this section; and 
"(3) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any way reduce the term of imprisonment for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and 
"(d) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law— 
"(i) a court shall not place on probation any person convicted of a violation of this section; 
"(ii) except as provided in paragraph (4), no term of imprisonment imposed on a person under this subsection shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony violation section 1030; 
"(iii) in determining any term of imprisonment to be imposed for a felony violation of section 1030, a court shall not in any way reduce the term of imprisonment for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and 
"(v) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently with any other term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony violation section 1030; and 
"(vii) the video tape service provider has provided an opportunity, in a clear and conspicuous manner, for the purchaser to withdraw on a case-by-case basis or to withdraw for ongoing disclosures:"

Subtitle B—Electronic Communications Privacy

SEC. 841. SHORT TITLE. 
This subtitle may be cited as the “Electronic Communications Privacy Act Amendments Act of 2012.”

SEC. 842. CONFIDENTIALITY OF ELECTRONIC COMMUNICATIONS. 
Section 2703(a)(3) of title 18, United States Code, is amended to read as follows:

“(b) T ECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following: 

“Sec. 1030A. Aggravated damage to a critical infrastructure computer.”

SEC. 8. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE. 
Section 1030(e)(6) of title 18, United States Code, is amended by adding after “place for access;” the following:

“or electronic communication of a subscriber or customer of the provider or service, or a governmental entity receives the contents of a wire or electronic communication service, or remote computing service under subsection (a), the governmental entity shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, as specified by the court issuing the warrant, the subscriber or customer—

“(1) a copy of the warrant; and

“(2) a notice that includes the information referred to in section 2707(a)(5)(B)(i).”

SEC. 9. ELECTRONIC COMMUNICATIONS SERVICE, OR REMOTE COMPUTING SERVICE—

SEC. 10. GENERAL.—Subject to paragraph (2), a governmental entity may request the disclosure by a provider of electronic communication service, or remote computing service, of the contents of any wire or electronic communication that is in electronic storage with or otherwise stored, held, or maintained by the provider if the government entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using warrant procedures) that is issued by a court of competent jurisdiction directing the disclosure:

“(1) a copy of the warrant; and

“(2) a notice that includes the information referred to in section 2707(a)(5)(B)(i).”

SEC. 11. CONSUMER INFORMATION—

SEC. 12. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE.
Section 1030(e)(6) of title 18, United States Code, is amended by adding after “or electronic communication service, or remote computing service under subsection (a), the governmental entity shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, as specified by the court issuing the warrant, the subscriber or customer—

“(1) a copy of the warrant; and

“(2) a notice that includes the information referred to in section 2707(a)(5)(B)(i).”

SEC. 843. ELIMINATION OF 180-DAY RULE; SEARCH WARRANT REQUIREMENT; REQUIR...
SECTION 7065. DELAYED NOTICE

(a) DELAY OF NOTIFICATION.—

(1) In general.—A governmental entity that is seeking a warrant under section 2703(a) may include in the application for the warrant a request for an order directing the provider of an electronic communication service, or remote computing service, to which a warrant, order, subpoena, or other directive under section 2703 is directed to not notify the person of the existence of the warrant, order, subpoena, or other directive for a period of not more than 90 days.

(2) DETERMINATION.—A court shall grant a request for an order made under paragraph (1) if the court determines that there is reason to believe that notification of the existence of the warrant may result in—

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Section 2703(d) of title 18, United States Code, is amended—

(1) by striking ‘‘A court order for disclosure under subsection (b) or (c)’’ and inserting ‘‘(a) request for disclosure under subsection (c)’’; and

(2) by striking ‘‘the contents of a wire or electronic communication, or’’. SEC. 844. DELAYED NOTICE. Section 2705 of title 18, United States Code, is amended to read as follows:

SEC. 2705. DELAYED NOTICE

(a) DELAY OF NOTIFICATION.—

(1) In general.—A governmental entity that is seeking a warrant under section 2703(a) may include in the application for the warrant a request for an order directing the provider of an electronic communication service, or remote computing service, to which a warrant, order, subpoena, or other directive under section 2703 is directed to not notify the person of the existence of the warrant, order, subpoena, or other directive for a period of not more than 90 days.

(2) DETERMINATION.—A court shall grant a request for an order made under paragraph (1) if the court determines that there is reason to believe that notification of the existence of the warrant may result in—

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Section 2703(d) of title 18, United States Code, is amended—

(1) by striking ‘‘A court order for disclosure under subsection (b) or (c)’’ and inserting ‘‘(a) request for disclosure under subsection (c)’’; and

(2) by striking ‘‘the contents of a wire or electronic communication, or’’. NOTICES OF HEARINGS COMMITTEE ON HEALTH, EDUCATION, LABOR, AND PENSIONS

Mr. HARKIN. Mr. President, I wish to announce that the Committee on Health, Education, Labor, and Pensions will meet in open session on Thursday, July 26, 2012, at 10 a.m. in room SD–430 in the Dirksen Senate Office Building to conduct a hearing entitled ‘‘Short-Supply Prescription Drugs: Shining a Light on the Gray Market.’’ The PRESIDING OFFICER. Without objection, it is so ordered.

COMMITTEE ON ENVIRONMENT AND PUBLIC WORKS

Mr. BEGICH. Mr. President, I ask unanimous consent that the Committee on Environment and Public Works be authorized to meet during the session of the Senate on July 25, 2012, at 2:30 p.m. in room 253 of the Dirksen Senate Office Building.

The Committee will hold a hearing entitled, ‘‘Short-Supply Prescription Drugs: Shining a Light on the Gray Market’’.

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

COMMITTEE ON ENERGY AND NATURAL RESOURCES

Mr. BEGICH. Mr. President, I ask unanimous consent that the Committee on Energy and Natural Resources be authorized to meet during the session of the Senate on July 25, 2012, at 2:30 p.m. in room SD–430 of the Dirksen Senate Office Building.

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

COMMITTEE ON FINANCE

Mr. BEGICH. Mr. President, I ask unanimous consent that the Committee on Finance be authorized to...