(3) Period of Appointment.—Members of the Executive Committee shall be appointed for a term of 1 year.

(4) Vacancies.—A vacancy in the Executive Committee shall be filled in the same manner as the original appointment, not later than 30 days after the date on which the vacancy occurs.

(c) Meetings.—

(1) In General.—The Executive Committee shall meet at the call of the chairperson of the Executive Committee.

(2) Quorum.—A majority of the members of the Executive Committee shall constitute a quorum.

(3) First Meeting.—The first meeting of the Executive Committee shall take place not later than 30 days after the date of enactment of this subtitle.

(4) Public Meeting.—The Executive Committee shall hold at least 1 public meeting before the date described in subsection (d)(1) to receive comments from small business concerns and other interested parties.

(d) Duties.—

(1) Recommendations.—Not later than 270 days after the date of enactment of this Act, upon consultation with the majority of members of the Executive Committee then serving, the Executive Committee shall submit to the Administrator recommendations relating to the feasibility of establishing a small business common application and web portal in order to meet the goals described in section 612.

(2) Transmission to Executive Agencies.—The Executive Committee shall transmit to each Executive agency a complete copy of the recommendations submitted under paragraph (1).

(3) Transmission to Congress.—The Executive Committee shall transmit to each relevant committee of Congress a complete copy of the recommendations submitted under paragraph (1).

(4) Recommendations by Executive Agencies.—Not later than 30 days after the date on which the Executive Committee transmits recommendations to the Executive agency under paragraph (2), each Executive agency that provides federal assistance to small business concerns shall submit to Congress recommendations, if any, for legislative changes necessary for the Executive agency to carry out the recommendations under paragraph (1).

(e) Personnel Matters.—

(1) Compensation of Members.—The members of the Executive Committee shall serve without compensation.

(2) Detail of Employees.—The Administrator may detail to the Executive Committee any employee of the Economic Development Administration, and such detail shall be without interruption or loss of civil service status or tenure.

(f) Federal Advisory Committee Act.—Section 14 of the Federal Advisory Committee Act (5 U.S.C. App.) shall not apply with respect to the Executive Committee.

SEC. 614. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to the Administrator such sums as may be necessary to carry out this subtitle.

Subtitle B—Government Accountability Office Review

SEC. 621. GOVERNMENT ACCOUNTABILITY OFFICE REVIEW

Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall submit a report to the Committee on Small Business and Entrepreneurship and the Committee on Small Business of the House of Representatives that evaluates the status of 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 of 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 world 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 any 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, or 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 sustain the military readiness and or 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. KYL, Mr. BOOZMAN, Mr. BLUNT, Mr. RUBIO, Mr. MCCAIN, Mr. GRASSLEY, Mr. BARRASSO, Mr. KIRK, Mrs. HUTCHISON, Mr. HOEVEN, Mr. SHELEY, 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. FEINSTEIN) 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. KYL, Mr. BOOZMAN, Mr. BLUNT, Mr. RUBIO, Mr. MCCAIN, Mr. GRASSLEY, Mr. BARRASSO, Mr. KIRK, Mrs. HUTCHISON, Mr. HOEVEN, Mr. SHELEY, 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, 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 Jobs and Growth Tax Relief Reconciliation Act of

SEC. 4. ALTERNATIVE MINIMUM TAX RELIEF. (a) 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 “$78,750 in the case of taxable years beginning in 2012 and $87,850 in the case of taxable years beginning in 2013,” and

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

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

(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”;

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

(d) COMPUTER SOFTWARE.—Section 179 of such Code is amended by striking paragraph (3) and inserting—

(2) by adding at the end the following:

“(c) TEMPORARY EXTENSION OF ADDITI0NAL RESEARCH EXPENSES DEDUCTION FOR CATEGORIES OF QUALIFIED REAL PROPERTY.—


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

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

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

(A) by striking “$72,450” and all that follows through “2011” in the heading thereof and inserting “$78,750 in the case of taxable years beginning in 2012 and $87,850 in the case of taxable years beginning in 2013,” and

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

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

(b) TEMPORARY EXTENSION OF INCREASED STRATEGIC REPORTABLE TECHNOLOGY EXPENSING AMOUNT.—


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

(e) 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) Requirements.—Legislation meets the requirements of this subsection if the legislation—

(1) simplifies the Internal Revenue Code of 1986 by reducing the number of tax preferences 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 current policy baseline, to result in increased revenue or result in revenue losses;

(4) has a dynamic effect which is projected to stimulate economic growth and lead to increased revenue;

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

(6) retains a progressive tax code; and

(7) 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.

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

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)” and inserting “(c)”

(2) by striking “(c)” and inserting “(c)”

(b) TEMPORARY CONNECTION OR CONSTRUCTION OF FACILITIES DURING EMERGENCY.—

SEC. 802. TEMPORARY EXTENSION OF INCREASED STRATEGIC REPORTABLE TECHNOLOGY EXPENSING AMOUNT.

SEC. 802. TEMPORARY EXTENSION OF INCREASED STRATEGIC REPORTABLE TECHNOLOGY EXPENSING AMOUNT.


(b) 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) Requirements.—Legislation meets the requirements of this subsection if the legislation—

(1) simplifies the Internal Revenue Code of 1986 by reducing the number of tax preferences 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 current policy baseline, to result in increased revenue or result in revenue losses;

(4) has a dynamic effect which is projected to stimulate economic growth and lead to increased revenue;

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

(6) retains a progressive tax code; and

(7) 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.
“(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) The term ‘(A)’ a manufacturer, transfer, or possession by 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 engaged in such purposes of law enforcement (whether on or off duty); or

“(B) a transfer to a licensee under title I of the Atomic Energy Act of 1954 for purposes of establishing an on-site physical protection system and security organization required by Federal law, or possession by an employee or contractor of such a licensee on-site for such purposes or off-site for purposes of licensee-authorized training or transportation of nuclear materials;

“(C) the possession, by an individual who is retired from service with a law enforcement agency and is not otherwise prohibited from receiving ammunition, of a large capacity ammunition feeding device transferred to the individual by the agency upon that retirement; or

“(D) a manufacture, transfer, or possession of a large capacity ammunition feeding device transferred to a licensee by a licensed manufacturer or licensed importer for the purposes of testing or experimentation authorized by the Attorney General.

(c) PENALTIES.—Section 924(a) of such title is amended by adding at the end the following:

“(6) Whoever knowingly violates section 922(v) shall be fined under this title, imprisoned not more than 10 years, or both.”

(d) IDENTIFICATION MARKINGS.—Section 923(i) of such title is amended by adding at the end the following:

“A large capacity ammunition feeding device manufactured after the date of the enactment of this sentence shall be identified by a serial number that clearly shows that the device was manufactured after such date of enactment, and such other markings as the Attorney General may by regulation prescribe.”

SA 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:

Beginning on page 199, strike line 4 and all that follows through page 110, line 6, and insert the following:

(d) CYBERSECURITY MODELING AND TEST BEDS.

(1) REVIEW.—Not later than 1 year after the date of enactment of this Act, the Director shall conduct a review of cybersecurity test beds in existence on the date of enactment of this Act to inform the program established under paragraph (2).

(2) ESTABLISHMENT OF PROGRAM.—

(A) IN GENERAL.—The Director of the National Science Foundation, the Secretary, and the Secretary of Commerce shall establish a program for the appropriate Federal agencies to provide research grants to institutions of higher education or research and development nonprofit institutions to establish cybersecurity test beds capable of realistic modeling and cyber attacks and defenses. The test beds shall work to enhance the security of public systems and focus on enhancing the security of critical private sector systems such as those in the finance, energy, and other sectors.

(B) REQUIREMENTS.—

(i) SIZE.—The test beds established under this paragraph shall be sufficiently large in order to model the scale and complexity of real world environments.

(ii) USE OF EXISTING TEST BEDS.—The test bed program established under subparagraph (A) shall build upon and expand test beds and cyber attack simulation, experiment, and distributed gaming tools developed by the Under Secretary of Homeland Security for Science and Technology prior to the date of enactment of this Act.

(iii) PURPOSES.—The purposes of the program established under paragraph (2) shall be to—

(A) support the rapid development of new cybersecurity defenses, techniques, and processes by improving understanding and assessing the latest technologies in a real-world environment; and

(B) to improve understanding among private sector partners of the risk, magnitude, and consequences of cyber attacks.

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 ensure the confidentiality, integrity, and security of sensitive personally identifiable information.

(b) APPLICABILITY.—A business entity engaging in interstate commerce that involves collecting, accessing, identifying, 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:

(1) FINANCIAL INSTITUTIONS.—Financial institutions subject to the data security requirements and standards under section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)) and

(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 title 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

(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 that Act.

(3) SERVICE PROVIDERS.—A service provider for any electronic communication by a third-party, to the extent that the service provider is exclusively engaged in the transmission, routing, or temporary, intermediate, or transient storage of that communication.

DIGITAL RECORDS.—Public records not otherwise subject to a confidentiality or nondisclosure requirement, or information...
obtained from a public record, including information obtained from a news report or periodical.

(d) SAFE HARBORS.—(1) A financial business entity shall be deemed in compliance with the privacy and security program requirements under section 803 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 a 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 prevent a financial business entity from taking actions that may result in the loss or exposure of sensitive personally identifiable information or systems containing sensitive personally identifiable information, including protecting such information from unauthorized access, disclosure, use, or alteration of sensitive personally identifiable information or systems containing sensitive personally identifiable information.

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 to meet the objectives of this title:

(1) PERSONAL DATA PRIVACY AND SECURITY PROGRAM.—Each business entity shall implement a comprehensive personal data privacy and security program pursuant to this title, which shall provide for the protection of sensitive personally identifiable information, including controls to authenticate and permit access only to authorized individuals; and

(2) FREQUENCY.—The frequency and nature of the tests required under paragraph (1) shall be determined by the risk assessment of the business entity 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 at issue and who is authorized to access sensitive personally identifiable information, including controls to authenticate and permit access only to authorized individuals; and

(b) TRAINING.—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.—The personal data privacy and security program of a business entity subject to this title shall be designed to meet the objectives of this title, 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.

(2) FREQUENCY.—The frequency and nature of the tests required under paragraph (1) shall be determined by the risk assessment of the business entity 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 at issue and who is authorized to access sensitive personally identifiable information, including controls to authenticate and permit access only to authorized individuals; and

(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 handle sensitive personally identifiable information in performing services or functions (other than the services or functions provided by a service provider on behalf of and under the instruction of such business entity, such business entity shall—

(1) exercise appropriate due diligence in selecting such person or entity; and

(2) 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—

SEC. 804. ENFORCEMENT.

(a) CIVIL PENALTIES.—Any business entity that violates the provisions of this title 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 this title 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.

(c) PENALTY LIMITS.—(A) IN GENERAL.—Notwithstanding any other provisions 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 any other provision of law, the total sum of civil penalties assessed against any person or entity for all violations of this title shall not exceed $500,000,000, unless such conduct is found to be willful or intentional.

(d) BUREAU OF NEUTRALS.—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.

(e) 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.

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

(g) OTHER RIGHTS AND REMEDIES.—The rights and remedies available under this section are in addition to any other rights and remedies available under law.
July 25, 2012

CONGRESSIONAL RECORD — SENATE

(b) Federal Trade Commission Authority.—Any business entity 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 business entity 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 for all violations of the provisions of this title resulting from the same or related acts or ommissions and for penalties assessed against the business entity.

(2) Penalty Limits.—

(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 that resulted from the same or related acts or omissions, does 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 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. 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 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 (A) 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 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) NOTICE 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 outcome of the action before the court; and

(B) intervene in an action brought under paragraph (3).

(C) file petitions for appeal.

(5) Pending Proceedings.—If the Federal Trade Commission initiates a Federal civil action under this title, or any regulations 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) Relief.—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 authority to investigate and to exercise the authority to enforce the laws of the 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 establishes 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.—Any action brought by 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 and use 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 security breach on the identity, privacy, and confidentiality of their personal information and identities;

(6) Data misuse and use of inaccurate data have the potential to cause serious or irrevocable harm to an individual’s livelihood, privacy, and liberty and undermine efficient productive 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:

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

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

(2) 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.

(3) CRYPTOGRAPHIC KEYS.—The term “cryptographic keys” means any device or means by which data is rendered indecipherable in the absence of associated cryptographic keys necessary to enable decryption of such data.

(4) DATA BREACH.—The term “data breach” means a violation of section 1028(a)(7) of title 18, United States Code.

(D) DATA BREACHES.—The term “data breaches” means any unauthorized or unprivileged access, disclosure, use, or modification of personal information.

(E) DATA SECURITY.—The term “data security” means measures designed to protect personal information.

(F) FEDERAL TRADE COMMISSION.—The term “Federal Trade Commission” means the agency designated by the Secretary of Homeland Security under section 206(a).

(G) ELEMENT.—The term “element” means a provision 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.

(H) ENTITY.—The term “entity” means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture established to make a profit, or nonprofit.

(I) EXPIRATION.—The term “expiration” means the date the term “entity” will terminate.

(J) PERSON.—The term “person” means an individual.

(K) PERSONAL DATA PRIVACY AND SECURITY ACT OF 2012.—The term “Act” means this division.

(L) 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.

(M) SECURITY BREACH.—The term “security breach” means a violation of section 1028(d)(7) of title 18, United States Code.

(2) SECURITY BREACH.—The term “security breach” means a violation of section 1028(d)(7) of title 18, United States Code.


(4) TRACTION.—The term “traction” means measures designed to protect personal information.

(5) UNAUTHORISED ACQUISITION.—The term “unauthorised acquisition” means a violation of section 1028(d)(7) of title 18, United States Code.

(D) UNSECURED ACCESS.—The term “unsecured access” means access to sensitive personally identifiable information that is for an unauthorized purpose, or in excess of authorization.

(E) SECURITY BREACH.—The term “security breach” means a violation of section 1028(d)(7) of title 18, United States Code.
§1041. Concealment of security breaches involving sensitive personally identifiable information

(a) IN GENERAL.—Whoever, having knowledge of a security breach and of the fact that notice of such breach is required under title II of the Personal Data Privacy and Security Act of 2012, intentionally and willfully conceals the fact of such security breach shall be immune from prosecution for such security breach results in economic harm to any individual in the amount of $1,000 or more, be fined under this title or imprisoned for not more than 5 years, or both.

(b) PERSON DEFINED.—For purposes of subsection (a), the term ‘person’ has the same meaning as in title 18, section 1039.

(c) NOTICE REQUIREMENT.—Any person seeking an exemption under section 202(b) of the Personal Data Privacy and Security Act of 2012 shall be immune from prosecution under this title if the Federal Trade Commission does not indicate, in writing, that such notice shall be given under section 202(b)(1)(C) of such Act.

(d) CONFORMING AND TECHNICAL AMENDMENTS.—The table of sections for chapter 47 of title 18, section 1341, is amended by adding at the end the following:

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, disposal of, or collects sensitive personally identifiable information shall, following the discovery of a security breach of such information, notify any resident of the States whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed, acquired by, or disclosed to another person.

(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, disposal 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 TO INDIVIDUAL.—If the Federal Trade Commission determines in writing that additional time is reasonably necessary to determine the scope of the security breach, prevent further disclosures, conduct the risk assessment, or to restore the reasonable integrity of the data system, or to provide notice to the entity designated by the Secretary of Homeland Security pursuant to section 202, delay of notification shall not exceed 60 days following the discovery of the security breach, unless the business entity or agency request an extension of time and the Federal Trade Commission determines in writing that additional time is reasonably necessary to determine the scope of the security breach, prevent further disclosures, or conduct the risk assessment, restore the reasonable integrity of the data system, or to provide notice to the entity designated by the Secretary of Homeland Security pursuant to section 202.

(3) BURDEN OF PRODUCTION.—The agency, or business entity shall give notice under subsection (a) if the Federal Trade Commission determines that the notification required under this title shall prevent or abrogate an agreement between an agency or business entity required to give notice under this title 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).

(4) BUSINESS ENTITY RELIEVED FROM GIVING NOTICE.—A business entity obligated to give notice under subsection (a) shall be relieved from such obligation provided the Federal Trade Commission determines that such notice would be contrary to a law enforcement or national security purpose.

(5) SERVICE PROVIDERS.—If a service provider becomes aware of a security breach of data in electronic form containing sensitive personal information that is owned or possessed by another business entity that connects to or uses a system or network provided by the service provider for the purpose of transmitting, routing, or providing intermediate or transient storage of such data, the service provider shall be required to notify the business entity that is engaged in such connection, transmission, routing, or storage of the security breach if the business entity can reasonably be identified. Upon receiving such notification from the service provider, the business entity shall be required to provide the notification required under subsection (a).

(6) TIMELINESS OF NOTIFICATION.—

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

(2) REASONABLE DELAY.—

(a) IN GENERAL.—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 202, delay of notification required under section 202(b), delay of notification required under section 202(c), delay of notification required under section 202(d), delay of notification required under section 202(e), or delay of notification required under section 202(f).
(3) Law Enforcement Immunity.—No non-
constitutional cause of action shall lie in any
court against any agency for acts relating
to the delay of notification for law en-
forcement or national security purposes un-
der this title.

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

(1) Financial Institutions.—Financial in-
stitutions—

(A) subject to the data security require-
ments promulgated under section 561(b)
6801(b)); and
(B) subject to the jurisdiction of an agency
or authority described in section 505(a) 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 require-
ments and implementing regulations of that
Act.

(B) Business Entities.—A business entity
shall be deemed in compliance with this divi-
sion if the business entity—

(1) acts as a covered entity and as a
business associate, as those terms are de-
fined under the Health Insurance Portability
and Accountability Act of 1996 (42 U.S.C. 1301
et seq.), including the data security require-
ments imposed under that Act and im-
plementing regulations promulgated under
that Act; and

(2) subject to, and currently in compli-
ance with, the data breach notification, pri-
vacy and data security requirements under
the Health Information Technology for Eco-
nomic and Clinical Health Act (HITECH)
(42 U.S.C. 17902) and implementing regulations
promulgated thereunder; or

(i) is acting as a vendor of personal health
records on a service provider, sub-
ject to the Health Information Technology
for Economic and Clinical Health (HITECH)
Act (42 U.S.C. 17935), including the data
breach notification requirements and im-
plementing 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 impede the ability
of the Federal Government to conduct law enforce-
ment investigations; or

(B) the Federal Bureau of Investigation
determines that notification of the security breach
would 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 or agencies for acts relating to the ex-
ception from notification for law enforce-
ment or national security purposes under this
title.

b) Safe Harbor.—

(1) In General.—An agency or business en-
tity shall be exempt from the notice require-
ments 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 per-
sonally identifiable information was subject to
the breach;

(B) without unreasonable delay, but not
later than 45 days after the discovery of a se-
curity breach, unless extended by the Fed-
eral Trade Commission, the agency or busi-
ness entity notifies the Federal Trade Com-
misson, in writing, of—

(1) the receipt of the risk assessment; and
(ii) its decision to invoke the risk assess-
ment exemption; and

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

(2) Rebuttable Presumptions.—For pur-
poses of part A of subchapter V—

(A) the encryption of sensitive personally
identifiable information described in para-
graph (1)(A) shall establish a rebuttable pre-
sumption that no significant risk exists; and

(B) the rendering of sensitive personally
identifiable information described in para-
graph (1)(A) unusable, unreadable, or inec-
driverable 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 es-
tablish a rebuttable presumption that no sig-
nificant 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 stand-
ards generally accepted by experts in the
field of information security; or

(B) submit a false risk assessment that contains fraudulent or deliberately mis-
leading information.

(c) Financial Fraud Prevention Exemp-
tions.

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

(A) effectively blocks the use of the sen-
tive 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 individ-
uals after a security breach that has resulted in
fraud or unauthorized transactions.

(2) Limitation.—The exemption in para-
graph (1) does not apply if the informa-
tion subject to the security breach includes an in-
dividual’s first and last name, or any other
type of sensitive personally identifiable in-
formation as defined in section 3, unless that
information is accessed or acquired by
a credit card security code.

SEC. 203. Methods of Notice.

An agency or business entity shall be in
compliance with section 201 if it provides the
following:

(1) Individual Notice.—Notice to indivi-
duals 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 per-
sonally;

(C) E-mail notice, if the individual has con-
sented to receive such notice and the notice
is consistent with the provisions permitting
the electronic transmission of notices under sec-
tion 209 of the Electronic Signatures in Glob-
al 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 recipients of such State whose sen-
sitive personally identifiable information
was, or is reasonably believed to have been,
accessed or acquired by an unauthorized per-
son exceeds 5,000.

SEC. 204. CONTENT OF NOTIFICATION.

(a) In General.—Regardless of the method
by which the Federal Trade Commission
is required to provide to individuals under section 203, such notice shall include,
to the extent possible—

(1) a description of the categories of sen-
sitive personally identifiable information
that was, or is reasonably believed to have
been, accessed or acquired by an author-
ized 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 identifi-
cable information the agency or business enti-
ty maintained about that individual; and

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

(b) National Content.—Notwithstanding
section 209, a State may require that a no-
tice under subsection (a) shall also include
information regarding victim protection as-
sistance provided for by that State.

(c) Direct Business Relationship.—Re-

gardless of whether a business entity, agen-
cy, or a designated third party provides the
notice required pursuant to section 201(b),
such notice shall include the name of the
business entity or agency that has a direct
relationship with the individual being noti-

SEC. 205. COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGEN-
CIES.

If an agency or business entity is required
to provide notification to more than 5,000 in-
dividuals under section 201(a), the agency or
business entity shall also notify all con-
sumer reporting agencies that compile and
maintain files on consumers on a nationwide
basis (as defined in section 680(p) of the Fair
Credit Reporting Act (15 U.S.C. 1681p)) of the
name and addresses for the major credit reporting
agencies without unreasonable
delay and, if it will not delay notice to
affected individuals, prior to the dis-
tribution of notices to the affected individ-
uals.

SEC. 206. NOTICE TO LAW ENFORCEMENT.

(a) Designation of Government Entity to Re-
ceive Notice.

(1) In General.—Not later than 60 days
after the date of enactment of this Act, the
Commission or the Federal Bureau of Invest-
igation shall designate a Federal Government entity to re-
ceive the notices required under section 201 and
this section, and any other reports and
information about security inci-
dents, threats, and vulnerabilities.

(2) Responsibilities of the Designated En-
tity.—The designated entity shall—

(a) be responsible for promptly providing
the information that it receives to the
United States Secret Service and the Federal
Bureau of Investigation, and to the Federal
Trade Commission for civil law enforcement
purposes; and

(b) provide the information described in
paragraph (A) as appropriate to other
agencies for national security, or data security
purposes.

(b) Notice.—Any business entity or agency
shall notify the designated entity of the fact
that a security breach has occurred if—

(1) the number of individuals whose sen-
sitive personally identifying information
was, or is reasonably believed to have been,
accessed or acquired by an unauthorized per-
son exceeds 5,000;

(2) the security breach involves a database,
networked or integrated databases, or other
data systems containing sensitive person-
ally identifiable information of more than
500,000 individuals nationwide;

(3) the security breach involves databases
owned or maintained by the Federal
Securitv

(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) TIMING AND REVIEW OF THRESHOLDS.—Not later than 1 year after the date of the enactment of this Act, the Federal Trade Commission, in consultation with the Attorney General, the Secretary of Homeland Security, and the Secretary of the Treasury, shall promulgate regulations regarding the reports required under subsection (a). The Federal Trade Commission shall consult with the Attorney General and the Secretary of Homeland Security, after notice and the opportunity for public comment, and in a manner consistent with section 553 of title 5, United States Code, to adjust the thresholds for notice to law enforcement and national security authorities under subsection (a) and to facilitate the purposes of this section.

(d) TIMING.—The notice required under subsection (a) shall be provided as promptly as possible, but such notice must be provided either 72 hours before notice is provided to an individual pursuant to section 201, or not later than the date the business entity or agency discovers the security breach or discovers that the nature of the security breach requires notice to law enforcement or national security authorities, whichever occurs first.

SEC. 207. ENFORCEMENT.

(a) IN GENERAL.—The Attorney General of the United States and the Federal Trade Commission may enforce civil violations of section 201.

(b) CIVIL ACTIONS BY THE ATTORNEY GENERAL OF THE UNITED STATES.—

(1) IN GENERAL.—The Attorney General may bring a civil action in the appropriate United States district court against a business entity that engages in conduct constituting a violation of this title if the Attorney General finds that the conduct in question constitutes a violation of this title.

(2) PENALTY LIMITATION.—Notwithstanding any other provision of law, the total amount of civil penalties assessed against a business entity for all violations of the provisions of this title resulting from the same underlying acts or omissions may not exceed $1,000,000, unless such conduct is found to be willful or intentional.

(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 $1,000,000.

(d) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—If the court determines, in a civil action brought by the Federal Trade Commission under this section, that an individual has or may have been harmed by a violation of section 57a(a)(1)(B) regarding unfair or deceptive acts or practices and shall be subject to enforcement by the Federal Trade Commission under this section, the court may impose an additional penalty in an amount that exceeds $1,000,000.

(f) COORDINATION WITH THE FCC.—If an enforcement action with the Federal Trade Commission is brought under this section, the court shall consult with the Federal Trade Commission to coordinate the enforcement action 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.
(i) IN GENERAL.—Paragraph (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 shall provide notice and a copy of the complaint to the Attorney General at the time the State attorney general files the action.

(b) SERVICE OF PROCESS.—In an action described in such subparagraph, the defendant named in the Federal criminal proceeding or action shall—

(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); 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 any provision of this title, except as provided in section 204(b). Nothing in this title shall be construed to modify, except as provided in section 204(b), any regulations thereunder, any other provision of Federal law, or any provisions of the law of any State, relative to laws of the United States; which was ordered to lie under subsection (a) or any provisions of the law of any State to—

(1) conduct investigations;

(2) administer oaths or affirmations; or

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

(e) VENUE: SERVICE OF PROCESS.—

(i) 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.

(ii) 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 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) subpoena witnesses or the production of documentary and other evidence.

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 notice sent under subsection (a), including any risk assessment or any regulations thereunder, any other provision of Federal law, or any provisions of the law of any State, relative to laws of the United States; which was ordered to lie under subsection (a) or any provisions of the law of any State to—

(1) conduct investigations;

(2) administer oaths or affirmations; or

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

(b) LAW ENFORCEMENT REPORT.—

(1) IN GENERAL.—Not later than 18 months after the date of enactment of this Act, and upon the request by Congress thereafter, the United States Secret Service and Federal Bureau of Investigation shall submit a report to Congress on the number and nature of security breaches subject to the national security or law enforcement exemptions under section 202(a).

(2) REQUIREMENT.—The report required under paragraph (1) shall not 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. 201. 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 the Congressional Budget Office, in the ad-

SEC. 202. ORGANIZED CRIMINAL ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030 of title 18, United States Code, is amended by inserting “section 1030 relating to fraud and related activity in connection with computers” after “section 1030 relating to fraud and related activity in connection with computers” and inserting the following:

SEC. 203. PENALTIES FOR FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.

Section 1030 of title 18, United States Code, is amended to read as follows:

SEC. 301. BUDGET COMPLIANCE.

SEC. 302. ORGANIZED CRIMINAL ACTIVITY IN CONNECTION WITH COMPUTERS.

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

SEC. 304. TRAFFICKING IN PASSWORDS.

SEC. 305. CONSPIRACY AND ATTEMPTED COMPUTER FRAUD OFFENSES.

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

SEC. 307. CONGRESSIONAL RECORD — SENATE
SEC. 1030A. AGGRAVATED DAMAGE TO A CRITICAL INFRASTRUCTURE COMPUTER.

(a) I N GENERAL.—Chapter 47 of title 18, United States Code, is amended by striking "alter;" and inserting the following:

"(a) Any person who violates this section;

(b) Any person, real or personal, constituting or derived from any gross proceeds obtained directly or indirectly, or any property traceable to such property, that such person obtained, directly or indirectly, as a result of any violation of this section, or a conspiracy to violate this section;

(c) PENALTY.—Any person who violates subsection (b) shall be fined under this title, except as otherwise provided in section 1030(e)(6) of title 18, United States Code, or a conspiracy to violate this section.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—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. 80. LIMITATION ON ACTIONS INVOLVING UNAUTHORIZED USE.

Section 1030(e)(6) of title 18, United States Code, is amended by inserting after "alters, removes," and inserting the following:

"(6) 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 section 1030(e)(6); and

"(d) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law—

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

"(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section 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;

"(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 section 1030(e)(6); and

"(e) NO POST-SENTENCE REMEDIES.—(1) In any proceeding against the United States involving any other provision of law, 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, 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 section 1030(e)(6); and

"(f) 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 section 1030(e)(6).

SA 2580. 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:

TITLE VIII—PRIVACY PROTECTIONS

Subtitle A—Video Privacy Protection

SEC. 801. SHIELD PROTECTION.

This subtitle may be cited as the "Video Privacy Protection Act Amendments Act of 2012."
SEC. 844. DELAYED NOTICE.

(a) IN GENERAL.—A governmental entity that is obtaining the contents of a communication service, or remote computing service named in the process or request was supplied to, or requested by, the governmental entity;

(B) notice that informs the customer or subscriber—

(i) that information maintained for the customer or subscriber by the provider of electronic communication service, or remote computing service named in the process or request was supplied to, or requested by, the governmental entity;

(ii) that notification of the warrant was served on the provider and the date on which the information was provided by the provider to the governmental entity;

(iii) that notification of the customer or subscriber was delayed;

(iv) the identity of the court authorizing the delay; and

(v) the provision of this chapter under which the delay was authorized.

(b) PRECLUSION OF NOTICE SUBJECT TO GOVERNMENTAL ACCESS.—

(1) IN GENERAL.—A governmental entity that is obtaining the contents of a communication information or records under section 2703 may apply for a court for an order directing a provider of electronic communication service, or remote computing service, to which a warrant, order, subpoena, or other directive under section 2703 is directed to provide notice to a governmental entity; and

(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, order, subpoena, or other directive 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;

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

(F) endangering national security.

(3) EXTENSION.—Upon request by a governmental entity, a court may grant 1 or more extensions of an order granted under paragraph (2) of not more than 90 days.

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 ‘‘CCDBG Reauthorization: Helping American Families.’’

For further information regarding this meeting, please contact Jessica McNice of the committee staff at (202) 224–9243.

Mr. BINGAMAN. Mr. President, I would like to announce for the information of the Senate and the public that a hearing has been scheduled before the Senate Committee on Energy and Natural Resources to examine gasoline price and margin dynamics within the state of Vermont.

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

For further information, please contact Hannah Breul at (202) 224–4756 or Symone Green at (202) 224–1219, or Abigail Campbell at (202) 224–4905.

AUTHORITY FOR COMMITTEES TO MEET

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

Mr. BEGICH. Mr. President, I ask unanimous consent that the Committee on Commerce, Science, and Transportation be authorized to meet during the session of the Senate on July 25, 2012, at 10 a.m., in room 253 of the Russell Senate Office Building.

The Committee will hold a hearing entitled, ‘‘The International Space Station: a Platform for Research, Collaboration, and Discovery.’’

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

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

Mr. BEGICH. Mr. President, I ask unanimous consent that the Committee on Commerce, Science, and Transportation be authorized to meet during the session of the Senate on July 25, 2012, at 2:30 p.m., in room 253 of the Russell 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 ENVIRONMENT AND PUBLIC WORKS

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–306 of the Dirksen Senate Office Building.

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 10 a.m. in room SD–406 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...